Отчет:
«Укрепление доверия и безопасности при использовании ИКТ в странах СНГ»

Декабрь 2016

ФГБОУ ВО ордена Трудового Красного Знамени «Московский технический университет связи и информатики» (Российская Федерация)

Международный Союз Электросвязи,
Бюро Развития Электросвязи

Отчет «Укрепление доверия и безопасности при использовании ИКТ в странах СНГ» подготовлен Бюро развития электросвязи МСЭ при поддержке ФГБОУ ВО ордена Трудового Красного Знамени «Московский технический университет связи и информатики» (Российская Федерация) в рамках реализации региональной инициативы Администрации связи Российской Федерации «Укрепление доверия и безопасности при использовании ИКТ», утвержденной Всемирной конференцией по развитию электросвязи 2014 года (г. Дубай, ОАЭ, 30 марта-10 апреля 2014 года).

Исполнитель: Докучаев Владимир Анатольевич, д.т.н., профессор, заведующий кафедрой МСиУС ФГБОУ ВО ордена Трудового Красного Знамени «Московский технический университет связи и информатики» (Российская Федерация)

Информация об исполнителе:

Год рождения: 1958 (г. Москва)
Образование: Московский электротехнический институт связи (специальность – инженер-электросвязи); Telecommunications Executive Management Institute of Canada (специальность – Strategic Management in Telecommunications Program).

Имеет более чем 25-летний опыт в области разработки, проектирования, создания и эксплуатации современных информационно-коммуникационных систем; научно-педагогический стаж свыше 30 лет, автор свыше 150 научных, учебно-методических и публицистических работ, генеральный директор некоммерческой организации «Ассоциация производителей оборудования связи» (НО АПОС), член Группы по развитию человеческого потенциала МСЭ (GCBI ITU-D), член Комиссии по телекоммуникациям и информационным технологиям Совета Российского Союза Промышленников и Предпринимателей по конкурентоспособности и отраслевым стандартам, член Экспертного совета Комитета Государственной Думы РФ по информационной политике, информационным технологиям и связи.

Отчёт выполнен сотрудниками ФГБОУ ВО МТУСИ и сети научно-образовательных центров «Инфокоммуникации и информационные технологии». Существенную помощь при подготовке и редактировании отчета оказали:

Владимир Владимиров – руководитель договорно-правового департамента НО АПОС - в части поиска, анализа и систематизации информации о законодательстве стран СНГ в области обеспечения доверия и безопасноси при использовании ИКТ.

Денис Гадасин - к.т.н., доцент кафедры МСиУС МТУСИ - в части поиска, анализа и систематизации информации о технологическом состоянии телекоммуникаций/ИКТ стран СНГ и Грузии.

Олег Иевлев – к.т.н., доцент, проректор по международным связям МТУСИ – в части в части поиска, анализа и систематизации информации об экосистеме ИКТ.

Виктория Маклачкова – заместитель генерального директора ООО Фирма «ТЕЛЕСОФТ» - в части поиска, анализа и систематизации информации о государственных услугах и подготовке кадров стран СНГ и Грузии.

Виктор Малочинский – главный специалист по информационной безопасности ФГБОУ ВО МТУСИ - в части поиска, анализа и систематизации информации о законодательстве стран СНГ и Грузии в области обеспечения доверия и безопасности при использовании ИКТ и подготовке кадров.

Сергей Мытенков – Вице-Президент Российского союза промышленников и предпринимателей (РСПП) в части сбора, подготовки, классификации, и систематизации о технологическом состоянии телекоммуникаций/ИКТ стран СНГ и данных по интернет-торговле (e-commerce).

Андрей Шведов (www.telesoft.com.ru) – технический директор ООО Фирма «ТЕЛЕСОФТ» - в части сбора, подготовки, классификации, и систематизации данных о технологическом состоянии телекоммуникаций/ИКТ стран СНГ и подготовке кадров.

Иван Крупнов – студент магистратуры МТУСИ - в части поиска, анализа и систематизации информации о технологическом состоянии телекоммуникаций/ИКТ стран СНГ и Грузии.

Оглавление

Введение

Информационно-коммуникационные технологии с каждым днем все прочнее входят в нашу жизнь: используются в быту, на работе, в обучении, в медицине, в торговле, облегчают взаимодействие с государственными органами и т.д. Мы живем в эпоху «виртуальной реальности».

Однако существующие в реальной действительности негативные элементы, такие как мошенничество, преступность, проявления насилия, неотвратимо проецируются в «виртуальный мир» – спам, вирусы, хакерство, распространение детской порнографии, киберпреступность, кибертерроризм и др. Киберпространство не имеет пределов и границ, киберугрозы могут возникнуть где угодно и нанести огромный ущерб за считаные минуты. Поэтому повышение доверия и безопасности при использовании информационно-коммуникационных технологий (ИКТ) является одной из самых актуальных проблем для мирового сообщества.

Впервые проблема обеспечения информационной безопасности в глобальном масштабе была обозначена в «Окинавской хартии глобального информационного общества», принятой в 2002 году лидерами стран G8 («Большой восьмерки»). Следующим этапом стала Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО). Для стран СНГ важное значение имеет встреча на высшем уровне «Соединим СНГ» (ноябрь 2009 года). В итоговых документах саммитов отражена необходимость принятия реальных мер по обеспечению безопасности при использовании ИКТ на глобальном, региональном и национальном уровнях.

Реализация решений ВВУИО в части обеспечения информационной безопасности осуществляется в рамках направления деятельности ВВУИО «Укрепление доверия и безопасности при использовании ИКТ». В этом процессе активная роль отводится Международному союзу электросвязи (МСЭ). Направления деятельности МСЭ в данной сфере определены соответствующими резолюциями ООН, актами и решениями полномочных конференций МСЭ 2010 года, Хайдарабадским планом действий по развитию электросвязи, Глобальной программой кибербезопасности, начатой по инициативе генерального секретаря МСЭ Х. Туре, а также другими документами МСЭ. Вопросы укрепления доверия и безопасности, управления определением идентичности, защиты детей от онлайновой эксплуатации, неприкосновенности частной жизни и защиты данных, кибербезопасность и т.д. были отражены в отчете генерального секретаря МСЭ и активно обсуждались на Всемирном форуме по политике электросвязи МСЭ.

Большое внимание вопросам укрепления доверия и безопасности при использовании ИКТ уделяет Региональное содружество в области связи (РСС), образованное в 1991 году министрами связи вновь созданных независимых государств на постсоветском пространстве с целью сохранения и гармоничного развития сетей почтовой и электрической связи. РСС является открытой международной региональной организацией в области связи, в состав которой наряду с полноправными членами – странами СНГ – входят наблюдатели – администрации министерств связи Болгарии, Латвии, Словении, операторы связи Эстонской Республики и Международная организация космической связи «Интерспутник». Стратегические задачи РСС в вопросах обеспечения информационной безопасности четко отражены в проекте стратегии сотрудничества государств – участников СНГ в построении и развитии информационного общества и плане действий по ее реализации на период до 2015 года, в разделе «Информационная безопасность». Для расширения взаимодействия по вопросам обеспечения информационной безопасности и

выработки общих подходов к их решению в конце 2004 года при Координационном совете была создана Комиссия по информационной безопасности.

В декабре 2011 года в целях расширения состава участников решением Совета глав АС РСС Комиссия была преобразована в Комиссию РСС по информационной безопасности (далее – Комиссия). Учитывая специфику тематики, в состав Комиссии наряду с представителями администраций связи РСС входят работники компетентных органов в данной сфере из стран Содружества. Также в целях привлечения научных кругов к деятельности Координационного совета и Комиссии была определена головная организация по научному обеспечению вопросов информационной безопасности – ФГУП ВНИИПВТИ (Российская Федерация). При Комиссии действует общественный консультативный совет по научно-технологическим вопросам информационной безопасности, который оказывает помощь в подготовке и экспертизе документов, организации семинаров и др.

Вопросу обеспечения защиты информации и безопасности информационных ресурсов уделяется большое внимание на самом высоком уровне. Признавая, что актуальность и обеспечение технологической независимости и информационной безопасности государства является стратегической задачей, главы государств СНГ в октябре 2008 года утвердили Концепцию сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности и Комплексный план мероприятий по ее реализации. Принятие этих документов способствовало дальнейшему формированию и совершенствованию правовой основы межгосударственного сотрудничества в данной сфере и созданию защищенной информационной среды на пространстве СНГ.

Отметим, что Координационный совет определен основным исполнителем мероприятий Комплексного плана. В целях реализации ряда мероприятий, предусмотренных Комплексным планом, в рамках РСС была организована и проведена ФГУП ВНИИПВТИ соответствующая научно-исследовательская работа. В ходе НИР проанализировано текущее состояние, проблемы и первоочередные задачи обеспечения информационной безопасности в СНГ, включая анализ законодательств государств – участников СНГ, регламентирующих обеспечение информационной безопасности. Подготовленный анализ использован при подготовке аналитического доклада Совету глав правительств СНГ. Комиссией по информационной безопасности подготовлены проекты Соглашения о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности и Положения о базовой организации государств – участников СНГ, осуществляющей методологическое и организационно-техническое обеспечение работ в области информационной безопасности и подготовку специалистов в этой сфере.

В соответствии с появлением возможности использования широкополосного доступа к сети Интернет существенно увеличилось количество пользователей. Часть этих пользователей – дети, для которых существует множество угроз и рисков, связанных с использованием сети Интернет, отсюда и возможные негативные последствия. Кроме того, дети являются наиболее уязвимыми пользователями сети Интернет.

Большую роль в борьбе с негативными проявлениями сети Интернет в отношении несовершеннолетних играют международные организации, а также национальные и государственные структуры. Как пример, в России было создано общественное объединение «Лига безопасного Интернета», куда вошли представители общественных организаций, независимого гражданского общества, крупнейших операторов связи, контент-провайдеров,

правоохранительных органов, Федерального Собрания, с тем чтобы не только начать обсуждать эти проблемы, но и предпринимать конкретные меры именно по линии гражданского общества.

В соответствии с решением Всемирной конференции по развитию электросвязи (ВКРЭ-2014) Международного союза электросвязи (Дубай, ОАЭ, 30 марта - 10 апреля 2014 года) на Российскую Федерацию возложена реализация региональной инициативы 5 «Укрепление доверия и безопасности при использовании ИКТ».

Министерство связи и массовых коммуникаций Российской Федерации закрепило за ФГБОУ ВО ордена Трудового Красного Знамени «Московский технический университет связи и информатики» (МТУСИ) реализацию указанной выше региональной инициативы.

На протяжении 2015 года в рамках проведения работ по реализации РИ5 «Укрепление доверия и безопасности при использовании ИКТ» по материалам открытых источников на русском и английском языках был проведён экспресс-анализ по следующим направлениям для стран СНГ и Грузии (за исключением Республики Туркменистан):

- Правовое состояние дел в вопросах обеспечения доверия и безопасности при использовании ИКТ, включая национальные и международные инициативы;
- Текущее технологическое состояние в области информационно-коммуникационных технологий;
- Развитие государственных услуг в электронном виде;
- Защита детей в «online» среде;
- Доступная среда. Организация доступа лиц с ограниченными возможностями к ИКТ;
- Межоператорское взаимодействие в части обеспечения доверия и безопасности при использовании ИКТ;
- Проблемы доверия и безопасности при Интернет-торговле (e-commerce);
- Развитие человеческого капитала;
- Деятельность МСЭ и РСС по укреплению доверия и безопасности при использовании ИКТ.

По каждому из направлений подготовлены краткие рекомендации и представлены обощённые индикаторы, позволяющие оценить уровень доверия и безопасности при использовании ИКТ. Определённая неоднородность материалов определяется сложность доступа к официальным материалам по отдельным из перечисленных выше направлений.

В ходе выполнения Региональной инициативы были разработаны «Типовые требования к видам профессиональной деятельности», базирующиеся на основе профессиональных стандартов: «Системный администратор информационно-коммуникационных систем»; «Специалист по администрированию сетевых устройств информационно-коммуникационных систем»; «Системный программист»; «Специалист по дизайну графических и пользовательских интерфейсов»; «Специалист по технической поддержке информационно-коммуникационных систем»; «Менеджер по продажам информационно-коммуникационных систем» (утверждены в Министерстве труда и социальной защиты Российской Федерации). Также подготовлены типовые требования к профессиональной деятельности по информационной безопасности и защите информации в информационно-коммуникационных системах на основе проекта

профессионального стандарта «Специалист по информационной безопасности информационно-коммуникационных систем», который признан Назиональным советом при Президенте Российской Федерации по профессиональным квалификациям соответствующим предъявляемым требованиям к профессиональным стандартам. Перечисленные типовые требования к видам профессиональной деятельности могут быть использованы при разработке аналогичных профессиональных и образовательных стандартов в странах СНГ. Указанные профессиональные стандарты находятся в свободном доступе в сети Интернет и могут быть скачены всеми желающими по адресу - http://АСИКТ.РФ.

Создана сеть Научно-образовательных центров (в ФГБОУ ВО МТУСИ и в НИУ ВШЭ) «Инфокоммуникации и информационные технологии», призванных способствовать развитию человеческого потенциала стран региона в области укрепления доверия и безопасности при использовании ИКТ.

Приведённые в отчте материалы могут послужить структурированной основой для дальнейших углублённых исследований в области укрепления доверия и безопасности при использовании ИКТ в каждой из стран СНГ и Грузии.

1. Правовое состояние дел в вопросах обеспечения доверия и безопасности при использовании ИКТ, включая национальные и международные инициативы

Республика Азербайджан

Сфера информационно-коммуникационных технологий (ИКТ) объявлена приоритетной сферой экономики в Азербайджане. Широкое применение информационно-коммуникационных технологий служит всестороннему развитию страны и имеет особое значение с точки зрения обеспечения национальной безопасности в информационной сфере. Последние десять лет в Азербайджане наблюдается динамичное развитие в секторе ИКТ. Эта тенденция позволяет предположить, что в недалеком будущем эта отрасль наряду с энергетикой может стать одним из ведущих направлений экономики страны. Национальная стратегия развития ИКТ, принятая в 2003 году, определила на ближайшие годы главную цель деятельности - переход к информационному обществу.

Учитывая сказанное выше, очевидно, что всё более актуальным становится вопрос об информационной безопасности (ИБ). В существующих нормативно-правовых актах (НПА), угрозы в связи с ИБ, носят несколько общий характер и не затрагивают конкретную информационную безопасность в политической, экономической, оборонной и других сферах страны. Опыт развитых стран показывает, что в Азербайджане так же, как и в других странах возникает необходимость в разработке отдельной Национальной концепции информационной безопасности. В таком документе следует определить правовую базу информационной деятельности и безопасности. Должны быть изучены и классифицированы угрозы ИБ, наиболее характерные для данной страны, а также спрогнозированы конкретные последствия возможных угроз. Своевременное выявление угроз ИБ и предупреждение их в каждой стране имеет большое значение.

Правовое регулирование обеспечения информационной безопасности Республики Азербайджан осуществялестя на основании Закона Азербайджанской Республики «Об информации, информатизации и защите информации». Основным документом, обеспечивающим применение данного Закона, является Указ призидента Азербайджанской Республики «О применении Закона Азербайджанской Республики «Об инфомрации, информатизации и защиет информации».

В указанном документе особое внимание уделяется следующим аспектам.

- Подготовка предложений о приведении действующих законодательных актов в соответствие с Законом Азербайджанской Республики «Об информации, информатизации и защите информации»;
- обеспечение приведения нормативно-правовых актов Кабинета министров и соответствующих центральных органов исполнительной власти в соответствие указанному Закону;
- подготовкаа предложений о порядке идентификации и использования электронной подписи в автоматизированной информационной системе, предусмотренной частью четвертой статьи 5 указанного Закона;

- подготовка предложений об органе исполнительной власти, уполномоченном выдавать специальное разрешение (лицензию) на деятельность специализированных организаций в области формирования государственных информационных ресурсов и оказании услуг с учетом положений части четвертой статьи 7 данного Закона;
- подготовка предложений об информационных ресурсах или их определенной части, подлежащих отнесению к национальным информационным ресурсам и их охране как национальное достояние, предусмотренное статьей 9 данного Закона;
- подготовка предложений о порядке сертификации информационных систем, в том числе, сертификации средств защиты этих систем, и об органах исполнительной власти, осуществляющих сертификацию, с учетом положений части первой статьи 16 данного Закона;
- подготовка предложений об органе исполнительной власти, уполномоченном выдавать специальное разрешение (лицензию) на деятельность в области проектирования и производства средств защиты информации с учетом положений части второй статьи 16 указанного Закона;
- разработка и утверждение соответствующих НПА, отнесенных к компетенции Кабинета министров Азербайджанской.

Полномочия «соответствующих органов исполнительной власти», предусмотренные частью первой статьи 5, частью первой статьи 10 и частью первой статьи 11 Закона Азербайджанской Республики «Об информации, информатизации и защите информации», осуществляет Межведомственная комиссия по охране государственной тайны при Президенте Азербайджанской Республики, аолномочия «соответствующего органа исполнительной власти», предусмотренные частью первой статьи 8, частью четвертой статьи 11 и частью третьей статьи 14 данного Закона, осуществляет Кабинет министров Азербайджанской Республики.

Перечислим основные программы и законы по развитию ИКТ в Республике Азербайджан:

- «Национальная стратегия по информационно-коммуникационным технологиям, направленная на благо развития Азербайджанской Республики (2003-2012 гг.)»
- «Электронный Азербайджан (2003-2008 гг.)»;
- закон «Об обеспечении прав интеллектуальной собственности и борьбе с пиратством»;
- Закон Азербайджанской Республики «О персональных данных»;
- Закон «Об авторском праве и смежных правах»;
- Закон «Об электронной торговле» способствует осуществлению операций купли-продажи, оказанию разного типа торговых услуг, заключению договоров электронным способом в сети, а также развитию экономических отношений между странами в глобальном мире;
- Закон «О телекоммуникации» регулирует отношения в телекоммуникационных сетях и операторов, а также механизм управления в этой области;
- Закон «О приобретении информации» – это нормативный акт, который регулирует право гражданина в приобретении информации на основе реализации принципов демократического правового государства;
- Закон Азербайджанской Республики «О коммерческой тайне». Под коммерческой тайной согласно закону понимаются сведения, связанные с производственной, технологи- ческой, управленческой, финансовой и другой деятельностью юридических и физических лиц,

разглашение которых без согласия владельца может причинить ущерб их законным интересам;

- Закон Азербайджанской Республики «Об информации, информатизации и защите информации». Этот закон регулирует отношения, возникающие при формировании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения информации, при создании и использовании информационных систем, технологий и средств их обеспечения, защите информации, и устанавливает права субъектов, участвующих в информационных процессах.

Республика Армения

В Республике Армения осуществляются меры, направленные на дальнейшую модернизацию информационно-коммуникационной инфраструктуры государства, раскрытие потенциала индустрии информационных и инновационных технологий. Совершенствуется государственная политика в области развития ИКТ, доступности Интернета, обеспечения информационной безопасности.

Правительство Республики Армения 28 августа 2008 года одобрило Концепцию развития сферы информационных технологий. Основной целью Концепции является определение перспектив и направлений развития информационных технологий и информационного общества. В Концепции проанализированы основные вызовы и проблемы на этом пути и предложены стратегические подходы для их преодоления, определены основные этапы развития информационной сферы.

В документе приведен ряд целевых показателей, предусматривающих их достижение к 2018 году. В частности, планируется довести объем доходов сферы информационных технологий до 1 млрд долларов США в 2018 году, увеличить объемы экспорта до 700 млн долларов США, увеличить количество ИТ-компаний до 1000, в том числе с иностранным капиталом – до 200, а число рабочих мест – до 20000.

Предусмотрено довести оснащенность компьютерной техникой государственных органов и образовательных учреждений до 100 %, а домашних хозяйств – до 50–70 %. Доступность Интернета для населения увеличить до 90 %, инвестирование венчурного капитала планируется довести до 700 млн долларов США, а количество технопарков и инкубаторов увеличить до 10–30 ед.

Государственным органом, определяющим государственную политику в области информационной безопасности, является Совет национальной безопасности Республики Армения, который возглавляет Президент Республики Армения.

Служба национальной безопасности при Правительстве Республики Армения определена уполномоченным и национальным координирующим органом в сфере обеспечения информационной безопасности Решением Правительства Республики Армения от 03 марта 2011 года № 185-А.

При Премьер-министре Республики Армения действует Совет по содействию развитию информационных технологий.

Органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий является Министерство экономики Республики Армения.

Общественной организацией, координирующей деятельность компаний сферы информационных технологий, является Союз предприятий информационных технологий, целью которого является защита экономических интересов компаний данной отрасли, стимулирование развития бизнеса, поощрение исследований в сфере ИКТ.

По решению Правительства Республики Армения в апреле 2009 года при Службе национальной безопасности создан специальный узел, который посредством серверов подключен к основным национальным провайдерам. Благодаря этому отслеживаются и предотвращаются не только попытки хакерских взломов, но и проникновения разного рода вирусов и нежелательных программ.

С развитием Интернета и повышением уровня информатизации органов государственной власти, региональных и местных органов, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан приобретают все большую актуальность вопросы обеспечения информационной безопасности.

26 декабря 2013 года Правительством Республики Армения было утверждено «Решение об утверждении стандартных требований к официальным страницам органов государственного управления в сети Интернет», которая содержит следующие основные положения.

Официальные сайты размещаются на серверах государственных органов или интернет-провайдеров в зоне безопасности с помощью специальных защищенных узлов или на серверах службы национальной безопасности.

Официальные сайты начинают действовать только после проверок на безопасность и разрешения Службы национальной безопасности.

На серверах, где размещены официальные сайты государственных органов, не должны быть размещены сайты иных организаций или физических лиц, или других систем электронных услуг.

14 августа 2014 года протокольным решением Правительства Республики Армения были утверждены «Принципы управления Интернетом», при помощи которых будут реализованы следующие основные задачи:

- разработка основных принципов управления Интернетом;
- формирование политики управления Интернетом;
- государственная поддержка вопросов развития надежности и безопасности сетей;
- содействие сотрудничеству в области управления Интернетом межгосударственных, международных, региональных и других организаций.

13 апреля 2015 г. на форуме «Медиа и информационная безопасность», было отмечено, что Армения по уровню информационной безопасности занимает в мире довольно низкое место, и для ее улучшения надо проводить серьезную работу. В последние годы количество атак на армянские ресурсы усиливается. На сегодняшний день хакерские атаки стали одним из главных проблем «всемирной паутины»: публикуются секретные данные крупных компаний, со взломанных аккаунтов политиков и известных деятелей начинают рассылать вирусы, многим компаниям

приходится тратить миллионы за восстановление своих сайтов, баз данных и иной важной информации.

Учитывая опасность хакерских атак в Армении, особенно в сфере обороны и безопасности, Вооруженные силы и Министерство обороны республики также делают все возможное, чтобы защитить свои официальные сайты от взломов.

Укрепление доверия и безопасности при использовании ИКТ — одно из важнейших условий успешного развития информационного общества в Армении. Приоритетными направлениями деятельности в области обеспечения ИБ являются:

- развитие правового обеспечения информационной безопасности и совершенствование правоохранительной деятельности в этой сфере;
- разработка и внедрение эффективных программных и программно-аппаратных средств защиты информационных ресурсов, информационных и телекоммуникационных систем;
- создание централизованно управляемой ИКИ, необходимой для обеспечения деятельности государственных органов, включая соответствующий уровень защиты информации;
- увеличение набора в высшие учебные заведения на специальности в области защиты информации, совершенствование системы повышения квалификации и создание системы переподготовки кадров в этой области;
- формирование системы мониторинга информационной безопасности Республики Армения в наиболее важных сферах жизнедеятельности общества и государства.

В рамках сотрудничества государств Содружества в области обеспечения информационной безопасности со стороны Республики Армения (письмо директора Службы национальной безопасности Республики Армении Г.Г. Акопяна № 2/4/3-844 от 21.08.14) предлагается:

- обеспечить сближение законодательных баз государств – участников СНГ в сфере информационной безопасности;

- изучить опыт государств – участников СНГ по созданию и функционированию Национальных групп быстрого реагирования на компьютерные инциденты;

- обеспечить переподготовку специалистов, работающих в сфере информационной безопасности, а также оперативных сотрудников подразделений по борьбе с киберпреступностью.

Одной из центральных международных инициатив в сфере Информационного общества, проходящей под патронажем Организации объединенных наций и Международного союза электросвязи, стало проведение Всемирной встречи на высшем уровне по информационному обществу(2003-2005г.).

Целью проведения Саммита была определена «выработка общего видения и понимания информационного общества, а также принятие декларации и плана действий для правительств, международных учреждений и всех секторов гражданского общества.

Информация о проектах, реализуемая Арменией, в рамках выполнения решений Всемирной встречи на высшем уровне по вопросам информационного общества:

1. Создание соответствующей международным стандартам национальной широкополосной телекоммуникационной сети, направленной на удовлетворение потребностей регионов, городских и сельских общин, государственных органов и органов местного самоуправления, а также частного сектора Республики Армения (2009 – 2018 годы).

2. Создание общественных телекоммуникационных центров для обслуживания жителей регионов, городских и сельских общин Республики Армения (2009 – 2013 годы).

3. Осуществление пилотных проектов электронного управления:

- реестр административного бизнеса;
- система электронной пенсии;
- система электронного налогообложения;
- система электронного здравоохранения;
- система электронного банковского дела;
- система электронного образования (23% школ Армении обеспечены компьютерными центрами с Интернет доступом).

Срок реализации пилотных проектов: 2008 – 2011 годы.

4. Разработка и рассмотрение Правительством Республики Армения проекта закона «Об информационных технологиях, информатизации и информационной безопасности» (2009 год).

5. С целью внедрения оптиковолоконных систем во всех сельских селениях Республики Армения, предусмотрена подготовка концепции совершенствования и удерживания инфраструктуры в области электронного сообщения (2009 год).

6. Подготовка и представление на рассмотрение Правительства Республики Армения проекта Решения Правительства Республики Армения «Об утверждении концепции о расширении географии предоставления услуг Интернет доступа, обеспечения доступа для широких слоев населения, а также направленной на обеспечение здоровой рыночной конкуренции» (2009 год).

Перечислим основные программы и законы по развитию ИКТ в Республике Армения.

- Закон Республики Армения «О Государственной и служебной тайне»;
- Закон Республики Армения «О свободе информации»;
- акон Республики Армения «О персональных данных»;
- Закон Республики Армения «Об электронном документе и электронной цифровой подписи» ;
- Закон Республики Армения «Об электронной связи»;
- Закон Республики Армения «Об органах национальной безопасности»;
- Закон Республики Армения «Об актах гражданского состояния»;
- Закон Республики Армения «Об архивном деле»;
- Уголовный кодекс Республики Армения;
- Гражданский кодекс Республики Армения;
- Указание Президента Республики Армения от 26 июня 2009 года №НК-97 об утверждении Концепции «Информационной безопасности Республики Армения»;
- Решение Национального собрания Республики Армения от 27 февраля 2012 года о ратификации «Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера»;
- Решение Национального собрания Республики Армения от 21 марта 2006 года о ратификации «Конвенции по борьбе с киберпреступностью Европейского союза».

Республика Беларусь

В настоящее время в Республике Беларусь завершается формирование основ информационного общества. Заложена правовая основа информатизации. Успешно развивается национальная информационно-коммуникационная инфраструктура (далее - ИКИ), позволяющая оказывать новые информационные услуги и услуги электросвязи на основе технологий широкополосного доступа. На протяжении последних 10 лет в результате выполнения государственных программ разработан ряд общегосударственных и ведомственных информационных систем. Республиканские органы государственного управления, большинство местных исполнительных и распорядительных органов представлены в глобальной компьютерной сети Интернет. Республика обладает достаточно развитой собственной информационной индустрией, что является одним из необходимых условий конкурентоспособности экономики. Национальная информационная индустрия, не ограничиваясь только прямым вкладом в валовой внутренний продукт, обеспечивает эффективное использование ИКТ в государственном управлении, социальной сфере, во всех отраслях экономики, повседневной жизни населения

За последние годы в Республике Беларусь реализуется комплекс мер по совершенствованию обеспечения информационной безопасности. Вместе с тем анализ состояния безопасности информационно-вычислительных систем различных государственных органов, организаций и предприятий республики показывает, что ее уровень не в полной мере соответствует современным потребностям. Отставание отечественных информационных технологий вынуждает государственные органы при создании информационно-вычислительных систем идти по пути закупок средств вычислительной техники, а также программного обеспечения импортного производства, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации.

В связи с расширением сфер применения систем обработки и распространения информации наблюдается рост количества случаев несанкционированного использования, модификации и уничтожения информации. Угрозы вычислительному и информационному ресурсам не могут быть выявлены, локализованы и ликвидированы внедрением в информационные системы отдельных аппаратных, программных средств и организационных мероприятий. Все средства и мероприятия должны быть объединены в систему защиты. Защиту информации следует рассматривать как регулярный процесс, осуществляемый путем комплексного использования технических, программных средств и организационных мероприятий на всех этапах разработки, испытаний и эксплуатации информационных систем. Требования по защите, предъявляемые к информационной системе, должны рассматриваться как часть общих функциональных требований к ней.

В настоящее время остро назрела необходимость обеспечения функционирования государственной системы защиты информации. Созданные в последние годы организационные структуры, принятые национальные законодательные акты, действующая нормативная, методологическая и материально-техническая базы еще не в полной мере решают основополагающую задачу в данной области – обеспечение безопасности Республики Беларусь в информационной сфере, являющейся составной частью национальной безопасности.

Разработка и реализация систем информационной защиты информации в республике осуществялется согласно подпрограмме «Безопасность ИКТ и цифровое доверие», (Заказчики: Департамент информатизации Минестерства связи РБ, оперативно-аналитический центр при Президенте Республики Беларусь), являющейся частью Национальной программы ускоренного

развития услуг в сфере информационно-коммуникационных технологий на 2011 - 2015 годы, утвержденной Постановлением Совета Министров Республики Беларусь от 28.03.2011 №384

Основными мероприятиями подпрограммы являются:

- развитие правового обеспечения информационной безопасности;
- разработка и внедрение эффективных программных и программно-аппаратных средств защиты информационных ресурсов, информационных и телекоммуникационных систем;
- создание информационных систем, необходимых для обеспечения деятельности государственных органов, включая соответствующий уровень защиты информации;
- формирование системы мониторинга информационной безопасности Республики Беларусь в наиболее важных сферах деятельности общества и государства;
- разработка типовых политик безопасности для государственных информационных систем.

Цель и задачи подпрограммы.

Основной целью подпрограммы является развитие системы информационной безопасности, обеспечивающей правовое и безопасное использование ИКТ, укрепление доверия, обеспечение условий для безопасного оказания и получения электронных услуг.

Поставленная цель достигается решением следующих задач:

- разработка методологии аудита безопасности информационных систем;
- разработка комплекта типовых документов политики безопасности для государственных информационных систем;
- создание системы оценки соответствия профессиональной компетентности персонала в выполнении работ, услуг в области защиты информации;
- обеспечение государственных органов информационно-аналитической системой для поддержки принятия решений.

Ожидаемые результаты

Выполнение данных задач позволит свести к минимуму возможность злоупотребления персональной и иной конфиденциальной информацией, расширить сферу использования электронного документооборота, обеспечить возможность ведения электронной торговли, предоставления электронных услуг, широкомасштабного внедрения систем электронных платежей.

Грузия

Грузия, как и другие страны СНГ, относится к региону стран с развивающейся экономикой, и активно реализует свои национальные планы социально-экономического развития. Одним из важнейших критериев роста, является укрепление доверия и безопасности при использовании ИКТ, что соответствует одному из важнейших направления деятельности ВВУИО «Укрепление доверия и безопасности при использовании ИКТ». В этом процессе активная роль отводится Международному союзу электросвязи (МСЭ). В Грузии осуществляется План действий по реализации Стратегии сотрудничества государств - участников СНГ в построении и развитии информационного общества на период до 2015 года (утвержден Решением Совета глав правительств СНГ от 28 сентября 2012 года). Актуальность проблемы укрепления доверия и безопасности при использовании ИКТ также отмечено в Решении № 1106 «Первоначальный

перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» (ОБСЕ, Постоянный совет PC.DEC/1106 3 декабря 2013).

Следует отметить тот факт, что Грузия не брала на себя инициативу в разработке мер обеспечения доверия и безопасности при использовании ИКТ, однако являясь членом района СНГ, страна перенимала нормативную базу и идеи от своих соседей. Так, например, в Санкт-Петербургской Декларации по ИКТ (Форум АТЭС 7-8 августа 2012 года) отмечена необходимость укрепление доверия и безопасности при использовании ИКТ для стимулирования экономического роста и процветания. По итогам встречи принята декларация «Укрепление доверия и безопасности при использовании ИКТ в целях содействия экономическому росту и процветанию» («Building Confidenceand Security in the Use of ICT to Promot e Economic Growth and Prosperity»).

Республика Казахстан

Основополагающими документами, определяющими подходы к обеспечению безопасности при использовании информационно-коммуникационных технологий в республике Казахстан, являются:

- Концепция информационной безопасности Республики Казахстан до 2016 г. (утверждена Указом Президента Республики Казахстан от 14 ноября 2011 г. № 174);
- О дальнейших мерах по реализации Стратегии развития Казахстана до 2030 года от 15 августа 2003 года N 1165;
- Закон Республики Казахстан от 15 марта 1999 года № 349-I «О государственных секретах»;.
- Закон Республики Казахстан от 13 июля 1999 года № 416-I «О противодействии терроризму»
- Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи»;
- Закон Республики Казахстан от 11 января 2007 года № 217-III «Об информатизации»;
- Закон Республики Казахстан от 9 ноября 2004 года № 603-II «О техническом регулировании»;
- Закон Республики Казахстан от 11 января 2007 года № 214-III «О лицензировании»;
- Закон Республики Казахстан от 23 июля 1999 года № 451-I «О средствах массовой информации»;
- Закон Республики Казахстан от 5 июля 2004 года № 567-II «О связи»;
- Закон Республики Казахстан от 1 июня 2010 года № 286-IV «О ратификации Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности».

Ниже приведены основные действующие национальные и международные стандарты по обеспечению доверия и безопасности при использовании ИКТ в республике Казахстан.

- СТ РК 34.020-2006 Защита информации. Технические средства защиты информации. Имитаторы излучения. Общие технические требования - Введен впервые

- СТ РК 34.021-2006 Защита информации. Технические средства защиты информации. Генераторы пространственного зашумления. Общие технические требования - Введен впервые
- СТ РК ГОСТ Р 50739-2006 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования - Введен впервые
- СТ РК ГОСТ Р 51275-2006 (ГОСТ Р 51275-99, IDT) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
- СТ РК 34.024-2006 Защита информации. Автоматизированные системы в защищенном исполнении. Общие технические требования - Введен впервые
- СТ РК 34.025-2006 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения - Введен впервые
- СТ РК 1073-2007 Средства криптографической защиты информации. Общие технические требования. Веден взамен СТ РК 1073-2002
- СТ РК 1694-2007 Средства защиты телефонных аппаратов от утечки информации за счет акустоэлектрических преобразований и высокочастотного навязывания
- СТ РК 1697-2007 Защита информации. Средства защиты технических средства от утечки информации по цепям электропитания
- СТ РК 14516-2007 Технологии информационные. Методы обеспечения защиты. Использование и управление услугами доверенной третьей стороной. Общие требования
- СТ РК 1700-2007 Техническая защита информации в служебных помещениях
- СТ РК 1701-2007 Техническая защита информации в средствах вычислительной техники, автоматизированных информационных системах и сетях от утечки посредством побочных электромагнитных излучений и наводок. Общие технические требования
- СТ РК ГОСТ Р 51188-2007 Защита информации. Испытания программных средств на наличие компьютерных вирусов
- СТ РК 1178-2003 Защита информационной системы Государственного фонда стандартов от несанкционированного доступа. Общие технические требования - Введен впервые
- СТ РК 34.022-2006 Защита информации. Требования к проектированию, установке, наладке, эксплуатации и обеспечению безопасности информационных систем
- СТ РК 1698-2007 Защита информации. Защита информации от технических разведок и от ее утечки по техническим каналам на объекте средств вычислительной техники
- СТ РК ИСО МЭК 27001-2007 Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасности. Требования - Введен впервые
- СТ РК ГОСТ Р МЭК 60950-2005 Безопасность оборудования информационных технологий - Введен впервые
- СТ РК 34.023-2006 Информационная технология. Методика оценки соответствия информационных систем требованиям безопасности - Введен впервые
- СТ РК ГОСТ Р ИСО/МЭК 15408-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель - Введен впервые

- СТ РК ГОСТ Р ИСО/МЭК 15408-2-2006 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности - Введен впервые
- СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности - Введен впервые
- СТ РК 1695-2007 Информационная безопасность. Аттестация объектов информатизации и средств вычислительной техники. Общие требования – Введен впервые
- СТ РК 34.022-2006 Защита информации. Требования к проектированию, установке, наладке, эксплуатации и обеспечению безопасности информационных систем.

Кыргызская Республика

Национальная Стратегия Устойчивого Развития (НСУР) Кыргызской Республики ставит задачу восстановить доверие граждан к государственным органам исполнительной власти путем коренной модернизации работы государственного аппарата. Предполагается усилить его профессионализм и ответственность, повысить качество оказания государственных услуг гражданам и бизнес - сообществу Кыргызстана, преодолеть коррупцию в государственном управлении за счет обеспечения полноценной прозрачности органов государственного управления, включая укрепление взаимодействия власти с гражданским обществом. Предусматривается активно использовать ИКТ для достижения этих целей. В частности, НСУР призывает к проведению единой государственной политики в области связи и ИКТ, эффективного использования ИКТ - инфраструктуры и информационных активов.

Республика Молдова

Республика Молдова (РМ) осуществила ряд мер по укреплению информационной безопасности. В результате ратификации Факультативного протокола к Конвенции ООН о правах ребенка, касающегося торговли детьми, детской проституции и порнографии 22 февраля 2007 года, Конвенции Совета Европы об информационной преступности 2 февраля 2009 года и Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия 19 декабря 2011 года Республика Молдова стала активным участником процесса применения общей уголовной политики в области борьбы с информационной преступностью, в том числе преступлениями по сексуальной онлайн-эксплуатации детей.

Разработан и утвержден Закон № 20 от 3 февраля 2009 года о предупреждении и борьбе с преступностью в сфере компьютерной информации, который конкретно устанавливает функции государственных органов и учреждений, компетентных в области предупреждения и борьбы с информационной преступностью, а также осуществлены разработки предложений по обеспечению ИБ. Следует также отметить Закон № 91 от 29 мая 2014 года об электронной подписи и электронном документе, разработанный с целью повышения уровня безопасности электронных подписей, а также приведения в соответствие с международными стандартами и рекомендациями в области инфраструктуры открытых ключей. Для обеспечения соответствия молдавского законодательства европейскому в этой области был принят еще ряд законодательных актов.

Этот вопрос рассматривался и на заседании Высшего Совета Безопасности Молдовы 7 октября 2014 г. Было решено, в частности, создать Национальный центр реагирования на инциденты в области безопасности. обеспечить дальнейшее развитие специальной правительственной телекоммуникационной системы государственного управления, разработать Концепцию информационной безопасности РМ и Стратегию информационной безопасности РМ и активизировать действия, направленные на уменьшение воздействия потенциальных рисков в отношении информационной безопасности.

Приведём основные программы и НПА, направленные на укрепление доверия и безопасности при использовании ИКТ.

- «Национальная стратегия создания информационного общества – «Электронная Молдова»», утвержденная Постановлением Правительства Республики Молдова № 46-50/336 от 25 марта 2005 года;
- Закон Республики Молдова «О доступе к информации» № 982-XIV от 11.05.2000;
- Закон Республики Молдова «Об информатизации и государственных информационных ресурсах» № 467-XV от 21.11.2003;
- Закон Республики Молдова «Об электронном документе и цифровой подписи» № 264-XV от 15.07.2004;
- Закон Республики Молдова «Об электронной торговле» № 284-XV от 22.07.2004;
- Закон Республики Молдова «О техническом регулировании» № 420–XVI от 22.12.2006;
- Закон Республики Молдова «О защите персональных данных» № 17-XVI от 15.02.2007;
- Закон Республики Молдова «О государственной тайне» № 245 от 27.11.2008;
- Указ «О создании информационного общества в РМ», 2004.

Российская Федерация

Как следует из Стратегии развития информационного общества в Российской Федерации, утвержденной Президентом РФ 7 февраля 2008 г., совершенствование правового обеспечения информационной безопасности является одним из приоритетов при построении глобального информационного общества, провозглашенного в Окинавской хартии глобального информационного общества, подписанной Президентом РФ 22 июля 2000 г.

В Российской Федерации одним из основополагающих документов по кибербезопасности, несущих рекомендационный характер, является «Рекомендация МСЭ-Т X.1500 -Методы обмена информацией о кибербезопасности».

К числу основных НПА, направленных на укрепление доверия и безопасности при использовании ИКТ следует отнести.

- № 126 -ФЗ «О связи»
- № 152-ФЗ «О персональных данных»;
- № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- № 612-ПП «Об утверждении Правил продажи товаров дистанционным способом»;
- № 584-ПП «Об утверждении Положения о защите информации в платежной системе»;
- Указ Президента РФ от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;
- «Доктрина информационной безопасности Российской Федерации»;
- Методический документ ФСТЭК от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах».

Также дейстует ряд стандартов, таких как «ГОСТ Р 54582-2011 -Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий», стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».

Совершенствование механизмов правового регулирования общественных отношений, возникающих в области обеспечения информационной безопасности, должно стать одним из приоритетных направлений государственной политики в рассматриваемой сфере. Развитие законодательства в области обеспечения информационной безопасности Российской Федерации должно базироваться на соблюдении не только общеправовых принципов (законности, справедливости, юридического равенства граждан, гуманизма, демократизма, единства прав и обязанностей, федерализма), межотраслевых (неотвратимости ответственности и др.), но и таких принципах правового обеспечения информационной безопасности, как единство информационного пространства, соблюдение баланса интересов личности, общества и государства и их взаимной ответственности, интеграции в рамках системы международной информационной безопасности.

На Расширенной коллегии Минестерства связи и массовых коммуникаций Российской Федерации в 2015 году рассматривались отдельные вопросы повышения качества государственного управления.

Первый блок — это то, что связано с экспертизой документов по информатизации. Работа год за годом становится более предметной, четкой и конкретной. Целый ряд регионов РФ перенимают этот опыт, где-то удалось вообще централизовать расходы на ИТ, где-то внедряется принцип координации информатизации.

За три года — с 2013 по 2015 — суммарно на предпроектной стадии Минкомсвязи России рассмотрело около 1000 проектов по информатизации в различных отраслях и от самых разных федеральных органов власти. Общая сумма представленных проектов превысила 300 млрд. рублей, лишь четверть проектов получила отрицательное заключение. При этом стоимость реализации проектов в процессе прохождения экспертизы снижалась в среднем на 20–30% от первоначально заявленной.

В 2015 году завершилась реорганизации подведомственного Минкомсвязи России ФГУП «ВНИИПВТИ», на его базе образован Центр экспертизы и координации информатизации.

В среднем на ИКТ госорганов в России ежегодно выделяется порядка 100 млрд. рублей. 70% — это традиционно эксплуатационные расходы. Бюджет развития — около 30 млрд. рублей, ежегодная дополнительная потребность составляет около 20 млрд. рублей. Большая часть этих средств — это потребность в развитии инфраструктуры. Из-за того, что это недофинансируется, в том числе, в связи с бюджетными ограничениями, нарастает растущее цифровое неравенство уже среди органов власти. Для устранения этого необходимо использовать единую инфокоммуникационную инфраструктуру. В настоящее время реализуется проект по так называемой Единой сети передачи данных (ЕСПД). Проект опирается на опыт компании ПАО «Ростелеком». Этот проект начинался с Федеральной миграционной службы. В 2016 году еще 14 федеральных органов государственной власти также приняли решение об использовании ЕСПД. Это основа для того, чтобы оказывать дополнительные сервисы. Не только каналы передачи данных, но и вычислительные мощности и, самое главное, сервисы, когда базовые сервисы, типовые, которые не связаны с ведомственными прикладными задачами, могут оказываться без дополнительных затрат по принципу унифицированных подходов.

Минкомсвязи России продолжает разработку необходимой нормативно-правовой базы, старается ликвидировать возникающие барьеры для перехода федеральных органов власти на электронный межведомственный документооборот. Переход должен быть осуществлен до конца 2016 года. Ведомства сейчас обеспечивают доработку и интеграцию ведомственных систем. Соответствующие правила были утверждены на Правительственной комиссии по ИТ.

Республика Таджикистан

Государственная программа развития и внедрения информационно-коммуникационных технологий в Республике Таджикистан разработана в целях реализации Государственной стратегии «Информационно-коммуникационные технологии для развития Республики Таджикистан», утвержденной Указом Президента Республики Таджикистан от 5 ноября 2003 года № 1174. Программа направлена на координацию действий государственных органов власти всех уровней на территории республики в области развития и массового распространения информационно-коммуникационных технологий в экономике, государственном управлении и общественной жизни путем реализации ведомственных программ.

В Таджикистане принят ряд законодательных и иных нормативных правовых актов по вопросам информации, информатизации и развития информационно-коммуникационных технологий.

Несмотря на это, ощущается большой дефицит грамотного и упрощенного информационного взаимодействия не только между государственными органами, но и внутри каждого государственного органа, в частности по следующим причинам:

- отсутствует единый стандарт в разработке и применении информационных систем в государственных органах;
- государственные структуры не интегрированы между собой, вследствие чего применение информационно-коммуникационных технологий значительно теряет свою эффективность;
- отсутствуют стандарты и требования по внедряемым программным обеспечениям в государственных органах;
- не проведена оптимизация ведомственных и межведомственных функций и процедур государственных органов, обеспечивающая перевод информации на бумажных носителях в электронный вид;
- отсутствуют соответствующие задачам оптимизации административных процедур единые стандарты создания и эксплуатации ведомственных и межведомственных методы и способы и протоколы ведомственного и межведомственного электронного взаимодействия;
- отсутствует единая инфраструктура обеспечения юридически значимого электронного взаимодействия на основе применения электронной цифровой подписи;
- не разработаны механизмы управления ведомственными и межведомственными программами информатизации органов государственной власти, учитывающие вопросы оптимизации административных процедур;
- разрыв по уровню автоматизации процессов, развитию информационной инфраструктуры и качеству реализованных программных решений между министерствами и ведомствами;
- отсутствие общих требований по обеспечению совместимости и интеграции государственных информационных ресурсов;
- неполноценное наполнение или полное отсутствие ведомственных информационных систем, ограниченность или отсутствие электронных государственных реестров;
- отсутствие механизмов взаимодействия государственных органов по исполнению государственных задач, что приводит к повторному запросу у граждан и организаций информации, которая уже имеется в базах данных других государственных органов;
- дублирование затрат государственных органов на разработку и сопровождение однотипных электронных реестров данных; - отсутствие единых требований на разработку типового и закупку коробочного программного обеспечения;

- отсутствие в министерствах и ведомствах технической информационной инфраструктуры и каналов доступа;
- отсутствие взаимодействия по обмену данными между государственными органами, основанного на единых правилах;
- локальный, преимущественно ведомственный характер внедрения средств информационно-коммуникационных технологий;
- отсутствие согласованных планов обновления и развития технического аппарата информационно-коммуникационных технологий;
- во многих государственных органах не имеются специализированных подразделений информационно-коммуникационных технологий, сохраняются трудности в связи с привлечением высококвалифицированных кадров для разработки и внедрения информационно-коммуникационных технологий.

За последние годы в Республике Таджикистан реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности. Начато и продолжается формирование и совершенствование базы правового обеспечения информационной безопасности.

Действующими нормативными документами в сфере информационной безопасности в Республики Таджикистан являются следующие основные законы Республики Таджикистан

- Об электронном документе от 10 мая 2002 года № 51 (в редакции Законов Республики Таджикистан от 26.12.2005 г. №122, 28.12.2012 г. №908, 22.07.2013 г. №995, 31.12.2014 г. №1074);
- Об информации от 10 мая 2002 года (в редакции Законов Республики Таджикистан от 03.07.2012 г. №848, 27.11.2014 г. №1164);
- Об электронной цифровой подписи от 30 июля 2007 года № 320;
- О праве на доступ к информации от 18 июня 2008 года № 411;
- Об экологической информации от 25 марта 2011 года № 705; О периодической печати и других средствах массовой информации от 19 марта 2013 года №961;
- О телевидении и радиовещании от 14 декабря 1996 года №382 (в редакции Законов Республики Таджикистан от 02.05.1998 г. №580, 30.06.1999 г. №814, 29.11.2000 г. №12, 06.08.2001 г. №35, 28.02.2004 г. №7, 29.04.2006 г. №184, 22.07.2013 г. №1014);
- Об издательском деле от 27 декабря 1993 года №897 (в редакции Законов РТ от 1.02.1996 г., 15.05.1997 г., 11.12.1999 г., 2.12.2002 г., 17.05.2004 г., 28.12.2005 г. №144);
- Об электрической связи от 10 мая 2002 года №56 (в редакции Законов Республики Таджикистан от 03.03.2006 г. №166, 20.03.2008 г. №379, 31 декабря 2008 года №462, 28.12.2013 г. №1047);
- О фельдъегерской связи от 2 декабря 2002 года №74;
- Об авторском праве и смежных правах от 13 ноября 1998 года №726 (в редакции Законов Республики Таджикистан от 01.08.2003 г. №27, 03.03.2006 г. №162, 03.12.2009 г. №573, 31.12.2014 г. №1172);
- Об информатизации от 6 августа 2001 года №40 (в редакции Закона РТ от 26 декабря 2005 г. №124); [17]
- О защите информации от 2 декабря 2002 года №71 (в редакции Закона РТ от 26 декабря 2005 г. №132);

- О Национальном архивном фонде и архивных учреждениях от 13 ноября 1998 года №704 (в редакции Законов РТ от 31.12.2008 г. №484, от 02.08.2011 г. №763); О рекламе от 1 августа 2003 года №34 (в редакции Законов Республики Таджикистан от 13.06.2007 г. №276, 06.10.2008 г. №445, 26.12.2011 г. №779, 16.04.2012 г. №812, 27.11.2014 г. №1163, 05.03.2015 г. №1202);
- О лицензировании отдельных видов деятельности от 17 мая 2004 года №37 (в редакции Законов Республики Таджикистан от 01.03.2005 г. №81, 28.07.2006 г. №195, 13.06.2007 г. №277, 05.01.2008 г. №349, 18.06.2008 г. №399, 06.10.2008 г. №435, 26.03.2009 г. №485, 19.05.2009 г. №519, 05.10.2009 г. №551, 29.12.2010 г. №662, 28.12.2012 г. №911, 19.03.2013 г. №950, 12.11.2013 г. №1030, 26.07.2014 г. №1110, 27.11.2014 г. №1157, 18.03.2015 г. №1184, 18.03.2015 г. №1191);
- О государственных секретах от 26 июля 2014 года №1095 (в редакции Закона Республики Таджикистан от 18.03.2015 г. №1185);

Также в республике действует ряд государственных программ таких, как:

- Программа обеспечения информационной безопасности Республики Таджикистан, утвержденная постановлением Правительства Республики Таджикистан от 30 июня 2004 года № 290 (в редакции Постановления Правительства Республики Таджикистан от 01.07.2011 г. №337);
- Программа реализации Концепции государственной информационной политики Республики Таджикистан, утвержденная постановлением Правительства Республики Таджикистан от 28 мая 2009 года № 307;
- Государственная Стратегия «Информационно-коммуникационные технологии для развития Республики Таджикистан», утвержденная Указом Президента Республики Таджикистан от 5 ноября 2003 года под № 1174;
- Концепция информационной безопасности Республики Таджикистан, утвержденная Указом Президента Республики Таджикистан от 7 ноября 2003 года под № 1175;
- Концепция формирования электронного правительства в Республике Таджикистан, утвержденная постановлением Правительства Республики Таджикистан от 30 декабря 2011года № 643 (в редакции Постановления Правительства Республики Таджикистан от 15.11.2012 г. №655);
- План дальнейших мероприятий Правительства Республики Таджикистан по внедрению информационно-коммуникационных технологий в целях совершенствования государственного управления, утвержденный постановлением Правительства Республики Таджикистан от 3 декабря 2010 года № 629 (в редакции Постановления Правительства РТ от 01.08.2011г. № 384);
- Государственная программа развития и внедрения информационно-коммуникационных технологий в Республике Таджикистан на 2014-2017 годы, утвержденная постановлением Правительства Республики Таджикистан от 3 июля 2014 года №428;
- Положение о требованиях, условиях и правилах защиты информации от иностранной технической разведки, утвержденное постановлением Правительства Республики Таджикистан от 2 апреля 2015 года №190;
- Положение о сертификации средств защиты информации по требованиям безопасности информации, аттестации объектов информатизации, порядка их государственной

регистрации, утвержденное постановлением Правительства Республики Таджикистан от 1 октября 2004 года №404;

В 2014-2015 годах осуществлялись следующие основные задачи государственной программы развития и внедрения информационно-коммуникационных технологий в Республике Таджикистан: уточнение функций и задач органов государственного управления, установленных нормативными правовыми актами;

- проведение анализа и оптимизации внутриведомственных бизнес процессов (бизнес-функций);
- определение и реализация приоритетных задач, требующих автоматизации;
- определение потребности в техническом оснащении для соответствия современным базовым техническим требованиям;
- определение государственного органа, уполномоченного на ведение реестра государственных информационных ресурсов, и утверждение положения о нем;
- проведение анализа и оптимизации межведомственных бизнес процессов (бизнес-функций); - разработка модели обмена информацией для информационных систем;
- поэтапная организация межведомственного обмена электронной информации.

На последующих этапах реализации программы в 2016-2017 годы предполагается выполнить следующие задачи, в том числе:

- закупка современной компьютерной техники и строительство ведомственных локально-вычислительных сетей; проектирование ведомственных информационных систем и определение требований для их разработки или закупки;
- разработка или закупка ведомственных информационных систем, в том числе предусматривающей межведомственный обмен данными;
- организация межведомственного обмена данными между всеми государственными органами; - замена используемого режима межбанковских платежей на современный автоматический режим межбанковского перевода средств - для осуществления крупных и срочных платежей;
- осуществление работ по распространению автоматического режима межбанковского перевода средств на все платежи.

Координацию деятельности по исполнению государственной программы развития и внедрения информационно-коммуникационных технологий в Республике Таджикистан на 2014-2017 годы осуществляет Совет по информационно-коммуникационным технологиям при Президенте Республики Таджикистан, образованный Указом Президента Республики Таджикистан от 27 февраля 2006 года №1707.

Центр информационных и коммуникационных технологий Исполнительного аппарата Президента Республики Таджикистан, Налоговый комитет при Правительстве Республики Таджикистан и Служба связи при Правительстве Республики Таджикистан на основании сведений министерств и ведомств каждые три месяца рассматривают ход исполнения мероприятий данной Программы.

Для мониторинга выполнения Программы приняты следующие отслеживаемые показатели:

а) Количество сотрудников центрального аппарата органов государственного управления, обеспеченных компьютерами, %;

б) Количество сотрудников центрального аппарата и местных подразделений органов государственного управления, обеспеченных компьютерами, %;

в) Количество центральных исполнительных органов, в которых внедрен электронный документооборот внутри аппарата, ед.;

г) Количество центральных исполнительных органов, во всей системе которых внедрен электронный документооборот, ед.;

д) Доля используемых компьютеров органов государственного управления, подключенных к единой внутренней сети, %;

е) Количество государственных органов, подключенных к единой сети и обеспечивающих электронный обмен информации между собой, ед.;

ж) Количество электронных баз данных центральных исполнительных органов, доступных для других государственных органов, ед.

В Таджикистане состояние информационной безопасности и защиты информации характеризуется следующими параметрами:

- не сформирована инфраструктура, обеспечивающая информационную безопасность при взаимодействии государственных органов между собой, а также с населением и организациями;
- отсутствуют эффективные механизмы контроля и использования информации о гражданах и организациях, содержащиеся в государственных информационных системах;
- законодательными актами не обеспечено полное регламентирование доступа к информации: каждый государственный орган в своих информационных системах самостоятельно определяет степень доступа сотрудников. Зачастую такое ограничение носит хаотичный характер и недостаточно администрируется;
- наблюдается низкий уровень применения электронной цифровой подписи при обмене информацией;
- по защите информации отсутствуют правила и нормы создания резервных хранилищ данных;
- отсутствуют правила и планы восстановления информационных систем после сбоев или катастроф;
- зачастую резервирование баз данных либо не осуществляется, либо осуществляется с применением уязвимых методов, что в случае возникновения крупных аварий может привести к полной потере данных;
- отсутствует практика использования специальных офицеров по информационной безопасности.

Для достижения целей государственной программы развития и внедрения информационно-коммуникационных технологий в Республике Таджикистан на 2014-2017 годы необходимо обеспечить решение приоритетных задач по следующим направлениям:

а) совершенствование нормативно-правовой базы развития информационно-коммуникационных технологий, в том числе:

- проведение анализа действующего законодательства на предмет соответствия современным требованиям информационно-коммуникационных технологий;
- приведение национальных стандартов по информационно-коммуникационных технологий в соответствие с передовыми международными стандартами;
- разработка и принятие нормативного правового акта, предусматривающего использование мобильной цифровой подписи:
- разработка порядка межведомственного обмена информацией;
- определение государственного органа, уполномоченного на ведение реестра государственных информационных ресурсов, и утверждение положения о нем;
- формирование единых стандартов по разработке и применению информационно-коммуникационных технологий систем в государственных органах;

б) разработка и внедрение информационно-коммуникационных технологий в органах государственного управления, в том числе:

- разработка и применение общих требований по обеспечению совместимости и интеграции государственных информационных ресурсов;
- внедрение и развитие технической инфраструктуры информационно-коммуникационных технологий и каналов передачи данных;
- разработка согласованных планов обновления и развития технического парка информационно-коммуникационных технологий;

в) укрепление технического потенциала информационно-коммуникационных технологий органов государственного управления, в том числе:

- обеспечение сотрудников органов государственного управления современной компьютерной техникой и (или) обновление имеющихся;
- оснащение специализированными серверными помещениями или размещение информационных ресурсов на базе центров обработки данных иных государственных органов;
- создание и развитие локально-вычислительных сетей с использованием современного сетевого оборудования;
- разработка требований к Интернет-провайдерам по предоставлению Интернет-услуг органам государственного управления;

г) формирование эффективной системы обмена информацией, в том числе:

- разработка правил обмена данными, исключающих дублирование функций и затрат;
- обеспечение совместимости программно-технических решений при обмене информацией;
- обеспечение условий выравнивания степени актуальности и достоверности данных при осуществлении обмена данными;

д) обеспечение защищенности информационных систем от случайного или преднамеренного вмешательства, в том числе:

- разработка общих требований по обеспечению информационной безопасности и защите информации;
- разработка и внедрение каждым органом государственного управления плана восстановления информационных систем после аварии с целью восстановления и сохранения работоспособности информационных систем;
- применение электронной цифровой подписи при обмене информацией, носящей персонализированный характер;
- создание эффективных схем резервирования баз данных каждым органом государственного управления;
- обеспечение органами государственного управления государственной закупки средств информационной защиты.

В результате реализации мероприятий государственной программы в Республике Таджикистан на 2014-2017 годы ожидается эффект по следующим направлениям:

- повышение результативности исполнения функций государственных органов за счет обеспечения доступности и достоверности используемых информационных материалов, применения единых баз данных;
- снижение затрат органов государственной власти на организацию обмена информацией на межведомственном уровне, а также за счет развития межведомственной системы электронного документооборота;
- повышение оперативности и качества принимаемых решений, сокращение издержек на управление за счет создания соответствующих информационных систем, улучшения технической инфраструктуры информационно-коммуникационных технологий;
- формирования информационно-коммуникационного потенциала государственных органов для последующего оказания электронных услуг населению и организациям и создания на этой базе «электронного правительства».

Республика Узбекистан

Развитие сферы связи, информатизации и телекоммуникационных технологий как важного фактора повышения благосостояния народа и экономического роста страны является одним из основных приоритетов государственной политики Узбекистана. Это еще раз подтверждается принятием Постановлением Президента страны от 27 июня 2013 года Комплексной программы развития Национальной информационно-коммуникационной системы Республики Узбекистан на период 2013-2020 годы.

Основными целями принятия программы является дальнейшее развитие и широкое внедрение во всех отраслях экономики и сферах жизни современных информационно-коммуникационных технологий, обеспечение ускоренного развития информационных ресурсов, систем и сетей, а также стимулирование расширения спектра и улучшения оказываемых интерактивных государственных услуг субъектам предпринимательства и населению.

Комплексная программа развития Национальной информационно-коммуникационной системы Республики Узбекистан на период 2013-2020 годы условно разделена на две программы. Первая программа развития телекоммуникационных технологий, сетей и инфраструктуры связи в Узбекистане, а вторая программа по созданию комплексов информационных систем и баз данных системы «Электронное правительство».

Программа развития телекоммуникационных технологий, сетей и инфраструктуры связи направлена на расширение сетей фиксированного и мобильного широкополосного доступа, центров коммутации передачи данных и голосового трафика, модернизации и расширение магистральных телекоммуникационных сетей, создание необходимой инфраструктуры для развития мультимедийных услуг.

До 2020 года планируются работы по расширению оптических сетей широкополосного доступа и строительства волоконно-оптических линий связи, дальнейшей установке по всей стране базовых станций EDVO, 3G и 4G LTE. Предусматривается создание студий для оказания мультимедийных услуг корпоративному сектору, центров информационно-справочных услуг, хранения и обработки данных, а также хранения часто используемых данных.

Основным законом Республики Узбекистан является Конституция, принятая 8 декабря 1992 года. В соответствии со статьей 29 Конституции, каждый имеет право на свободу мысли, слова и убеждений. Каждый имеет право искать, получать и распространять любую информацию, за исключением информации направленной против существующего конституционного строя и других ограничений, предусмотренных Законом. Статья 27 Конституции гарантирует гражданину право на защиту от посягательств на его честь и достоинство, вмешательства в частную жизнь, на неприкосновенность его жилища. Никто не вправе войти в жилище, производить обыск или осмотр, нарушать тайну переписки и телефонных разговоров иначе как в случае и порядке, предусмотренных законом.

В Гражданском кодексе Республики Узбекистан находят отражение такие понятия, как банковская, коммерческая и служебная тайна, а также определяются меры, необходимые для их защиты.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Республики Узбекистан. Уголовное законодательство устанавливает ответственность по шести составам, относящимся к преступлениям в сфере информационных технологий (Глава XX-1 «Преступления в сфере информационных технологий»).

Кодексом об административной ответственности Республики Узбекистан также предусмотрена ответственность за нарушение правил пользования информацией (статья 155) и нарушение правил эксплуатации компьютерной системы (статья 155-1).

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе «О защите государственных секретов».

Основополагающим среди законов Республики Узбекистан, посвященных вопросам информационной безопасности, следует считать Закон Республики Узбекистан «Об информатизации». В нем даются основные определения, намечаются направления, в которых должно развиваться законодательство в данной области, регулируются отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации.

Статья 11 закона устанавливает категории доступа к информационным ресурсам, разделяет их на общедоступные информационные ресурсы и информационные ресурсы с ограниченным доступом. В законе также появилось определение блогера, а также нормы устанавливающие обязанность блогеров и других владельцев веб-сайтов не допускать размещение на них информации, распространение которой запрещено, а также недостоверной информации. Статьи 19 и 20 данного закона целиком посвящены вопросам защиты информационных ресурсов и информационных систем.

11 декабря 2003 года Президентом Республики Узбекистан был подписан Закон Республики Узбекистан «Об электронной цифровой подписи». Согласно этому закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при соблюдении определенных требований.

Закон Республики Узбекистан «О принципах и гарантиях свободы информации» от 12 декабря2002 года является важным документом для формирования и развития информационной инфраструктуры и системы противодействия информационным угрозам. В закон вошли 5 статей, определяющих основные принципы информационной безопасности в стране.

Закон установил общее определение понятия «информационная безопасность» (статья 3), согласно которому «информационная безопасность — состояние защищенности интересов личности, общества и государства в информационной сфере»

По формированию государственных информационных ресурсов и систем, постановлением Кабинета Министров Республики Узбекистан «О совершенствовании нормативно-правовой базы в сфере информатизации» от 22 ноября 2005 года № 256 утверждены Положение о порядке формирования государственных информационных ресурсов и Положение о порядке создания информационных систем государственных органов.

В соответствии с Законом «О принципах и гарантиях свободы доступа к информации» и Положением «О порядке подготовки и распространения информационных ресурсов Республики Узбекистан на сети передачи данных, включая интернет» (утверждено Постановлением Кабинета Министров Республики Узбекистан от 26.03.1999 №137) определено, что – документированная информация, не содержащая информацию, отнесенную к государственным секретам, доступ к которой ограничивается в соответствии с законодательством. Кроме того, постановлением Кабинета Министров Республики Узбекистан от 07.11.2011 г. №296 утвержден Перечень сведений, отнесенных к конфиденциальной информации (Приложение №2).

Регулирование вопроса, касательно криптографической защиты информации, отражено в постановлении Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан», согласно которому уполномоченным органом в данной сфере является Служба национальной безопасности РУз. Постановлением утверждены Положение о криптографической защите информации в Республике Узбекистан и Положение о сертификации средств криптографической защиты информации в Республике Узбекистан.

Важным организационным шагом в решении вопросов информационной безопасности стало принятие Постановления Президента Республики Узбекистан от 27 июня 2013 года № ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан». Во исполнение данного постановления Президента РУз Кабинетом Министров РУз принято Постановление от 16 сентября 2013 года №250 «О мерах по

организации деятельности Центра развития системы «Электронное правительство» и Центра обеспечения информационной безопасности при Министерстве по развитию информационных технологий и коммуникаций Республики Узбекистан».

В настоящее время, в республике нет единого концептуального документа в области информационной безопасности. Такой документ позволил бы обозначить направления работы по совершенствованию нормативно-правовой базы, деятельности по разработке и широкому внедрению единых стандартов и других нормативных документов, а также определить необходимые меры по развитию кадровой политики в сфере информационной безопасности.

Также отметим распоряжение от 25 июня 2014 г. «О программе законотворческих работ по реализации поправок к Конституции Республики Узбекистан» и инициативу Президента Узбекистана о необходимости разработки и принятия Закона Республики Узбекистан «Об электронном правительстве».

Целью принятого Законодательной палатой Республики Узбекистан закона «Об электронном правительстве» является повышение эффективности деятельности государственных органов на основе широкого использования информационно-коммуникационных технологий, оптимизация порядка оказания электронных государственных услуг, повышение качества и доступности электронных государственных услуг, упрощение процедур и сокращение сроков их оказания, а также снижение административных издержек, связанных с получением государственных услуг, формирование информационных баз данных государственных органов, внедрение в системе государственного управления принципа «одно окно», использование субъектами предпринимательства систем электронной коммерции. Это позволитзначительно повысить эффективность деятельности государственных органов, улучшить предоставление электронных государственных услуг юридическим и физическим лицам; расширить использование информационно-коммуникационных технологий в различных сферах жизни общества (здравоохранение, образование, занятость и социальная защита населения, жилищно-коммунальное хозяйство, торговля и др.); повысить оперативность и качество принимаемых решений, сократить издержки на государственное управление за счет создания и функционирования соответствующих информационно-аналитических систем; исключить дублирование разработок информационных систем и ресурсов на уровне отдельных государственных органов и другое.

Украина

С намерением развивать ИКТ-сектор, украинское правительство реформировало структуры его управления и активно развивает стратегии продвижения проникновения ИКТ. Основные программы и нормативные документы, относящиеся к ИКТ, включают следующие основные НПА:

- закон «Об основных принципах развития информационного общества в Украине на 2007 — 2015 годы»;
- Стратегия инновационного развития Украины на 2010–2020 гг.;
- Концепция электронного правительства в Украине, действующая до 2015 года.

15 мая 2013 Кабинет министров Украины одобрил проект постановления «О стратегии развития информационного общества в Украине». Указанный документ нацелен на внедрение ИКТ во все сферы жизни и для продвижения электронного правительства, электронной демократии и экономики.

В 2014 году Кабинет Министров одобрил проект закона «Об основных мерах кибербезопасности». Предполагается, что реализация этого документа позволит внедрить комплексный подход в определении основных мер формирования государственной политики в сфере кибербезопасности, а также создать условия для обеспечения защиты информационной инфраструктуры государства.

Государственная служба специальной связи и защиты информации Украины была сформирована в 2006 году. Основными задачами службы являются:

- обеспечение формирования и реализации государственной политики в сфере защиты государственных информационных, телекоммуникационных и информационно-телекоммуникационных систем, использования и защиты государственных электронных информационных ресурсов, телекоммуникаций, пользования радиочастотным ресурсом Украины и т.д.;
- осуществление государственного контроля за состоянием криптографической и технической защиты информации, являющейся собственностью государства;
- разработка и осуществление мероприятий по развитию телекоммуникационных сетей, улучшение их качества, обеспечение доступности и устойчивого функционирования.

Начиная с 2007 года Украина наращивает технологическое отставание в области ИКТ по сравнению с другими странами.

До принятия Закона Украины «О защите персональных данных» вопросами информационной безопасности в глобальном смысле этого термина занимались две категории организаций: государственные учреждения и банки. У большинства других предприятий информационная безопасность ассоциировалась в большей степени со средствами охранной и пожарной сигнализации, а также видеонаблюдения. После принятия Закона Украины «О защите персональных данных», основными специалистами в области защиты информации в силу возложенных на них функциональных обязанностей стали представители кадровых служб предприятий. Именно они отвечают за выполнение требований законодательства относительно вопросов защиты персональных данных.

Согласно Закону Украины «Об информации» выделяется два вида информации: открытая и информация с ограниченным доступом. Информация с ограниченным доступом, в свою очередь, делится на:

- конфиденциальную;
- служебную;
- составляющую государственную тайну.

В законе делается особый акцент на понятии конфиденциальной информации в отношении данных о физическом лице. Так, например, пункт 2 статьи 21 этого же закона говорит о том, что конфиденциальной является информация о физическом лице, а в статье 11 дается более четкое определение, какие именно данные о физическом лице являются конфиденциальными: «К конфиденциальной информации о физическом лице относятся, в частности, данные о

национальности, об образовании, о семейном положении, религиозных убеждениях, состоянии здоровья, а также адрес, дата и место рождения».

Отметим и такой документ, как «Правила обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах», утвержденные постановлением Кабинета министров Украины от 29.03.2006 № 373. Правила дают четкий ответ на вопросы относительно того, какая же информация, по мнению государства, подлежит защите и что подразумевается под словом «защита». Защите подлежит:

1. Открытая информация, которая является собственностью государства и в определении Закона Украины «Об информации» принадлежит к статистической, правовой, социологической информации, информации справочно-энциклопедического характера и используется для обеспечения деятельности государственных органов или органов местного самоуправления, а также информация о деятельности указанных органов, если она публикуется в Интернете, других глобальных информационных сетях и системах или передается телекоммуникационными сетями (далее – открытая информация).
2. Конфиденциальная информация, которая является собственностью государства или требование относительно защиты которой установлено законом, в том числе конфиденциальная информация о физическом лице (далее – конфиденциальная информация).
3. Информация, составляющая государственную или другую предусмотренную законом тайну (далее – секретная информация).

В этом документе отмечается, что для обеспечения защиты информации в системе должна создаваться комплексная система защиты информации, которая предназначается для защиты информации от утечки по техническим каналам, от несанкционированных действий с информацией, в том числе с использованием компьютерных вирусов, от специального воздействия на средства обработки информации.

Данная часть документа перекликается со статьей 8 Закона Украины «О защите информации в информационно-телекоммуникационных системах», в которой говорится о том, что информация, которая является собственностью государства, или информация с ограниченным доступом (конфиденциальная), требование относительно защиты которой установлено законом, должна обрабатываться в системе с применением комплексной системы защиты информации, подтвержденной соответствием. Подтверждение соответствия осуществляется по результатам государственной экспертизы в порядке, установленном законодательством.

Комплексная система защиты информации (КСЗИ) представляет собой взаимосвязанную совокупность организационных и инженернотехнических мероприятий, средств и методов защиты информации. Для создания комплексной системы защиты информации используются средства защиты информации, которые имеют сертификат соответствия или положительное экспертное заключение по результатам государственной экспертизы в сфере технической и/или криптографической защиты информации.

Еще одним важным моментом является то, что согласно Правилам передача конфиденциальной информации из одной системы в другую должна осуществляться в зашифрованном виде или по защищенным каналам связи в соответствии с требованиями законодательства по вопросам технической и криптографической защиты информации.

В основе всех сертифицированных в Украине средств криптографической защиты информации лежит алгоритм симметричного шифрования, ГОСТ 28147-89 (советский и российский стандарт симметричного шифрования, введённый в 1990 году, также является стандартом СНГ).

Порядок проведения работ по созданию КСЗИ описан в одноименном документе: НД ТЗИ 3.7-003-05 «Порядок проведения работ по созданию комплексной системы защиты информации в информационно-телекоммуникационной системе». Согласно этому документу создание комплекса средств защиты от несанкционированного доступа осуществляется во всех информационно-телекоммуникационных системах (ИТС), где обрабатывается информация, являющаяся собственностью государства, относится к отдельным видам информации, необходимость защиты которой определена законодательством, а также в ИТС, где такая необходимость определена собственником информации. Порядок создания КСЗИ в ИТС является единым независимо от того, создается КСЗИ в ИТС, которая проектируется, или в действующей ИТС, если возникла необходимость обеспечения защиты информации либо модернизации уже созданной КСЗИ.

2. Текущее технологическое состояние стран в области ИКТ

Республика Азербайджан

Интенсивное развитие информационно-коммуникационных технологий (ИКТ) имеет огромное влияние на все сферы человеческой деятельности. В этой связи политика развития ИКТ потенциала относится к числу приоритетных во многих странах мира и, в том числе, в Азербайджане.

Национальная стратегия по информационно-коммуникационным технологиям Республики Азербайджан (2003-2012 годы) придала мощный импульс динамичному развитию этой сферы в стране.

В результате проделанной в области ИКТ работы, как составной части государственной политики по общему социально-экономическому развитию Азербайджана, за последние года темпы роста доходов по отрасли, превысили общемировые темпы развития в 4,4 раза, составили в среднем по 30-35 процентов на каждый год. Это способствовало развитию в секторе ИКТ, расширению перечня услуг связи и информационных услуг, повышению их качества.

По состоянию на конец 2015 года состояние сектора таково: ИКТ является вторым по объему и потенциалу сектором после энергетической сферы. По динамичности и стабильности развития этот сектор несомненный лидер. Отрасль с 2003 года показывает среднегодовые темпы роста на уровне 30—32%, за исключением кризисного 2009 года, когда динамика снизилась до 13—14% годовых. При этом среднемировые темпы роста ИКТ составляют примерно 10%. За последние несколько лет объем сектора ИКТ в Азербайджане вырос в пять раз и составляет около 1,5 млрд. долл., что примерно равно 3,5% от ВВП страны.

В 2010 году было достигнуто 100-процентное проникновение уровня сотовой связи. В 2008 году объявлено, что на всей территории республики есть фиксированная телефонная связь, то есть впервые на постсоветском пространстве практически все населенные пункты были обеспечены стационарной телефонной связью. По последним данным, около 50% жителей республики стали пользователями Интернета, при этом доступ в Интернет есть в каждом населенном пункте. На 1 октября 2010 года уровень проникновения широкополосного доступа в Интернет составил 12%.

Покрытие государственных и общественных теле- и радиоканалов по республике — 100%, а у частных масс-медиа чуть поменьше — 80—85%.

В начале 2013 года вклад сектора ИКТ в национальный ВВП составил 1,8 процента. Ожидается, что к 2020 году он вырастет примерно в пять раз.

Данный сектор продолжает развиваться, и следует плану «Национальной стратегии по развитию информационного общества в Азербайджане на 2014-2020 годы».

В январе-августе 2015 года населению и организациям в Азербайджане были оказаны информационные услуги и услуги связи на сумму 1,077 млрд манатов, что на 10,8% превышает показатель аналогичного периода 2014 года.

Порядка 81% доходов, полученных по сектору, пришлось на долю негосударственных предприятий. Из общего объема информационных услуг и услуг связи порядка 72% пришлось на долю услуг, оказанных населению. При этом 54% из общего объема полученных доходов пришлось на долю услуг мобильной связи, что следует из отчета Государственного комитета по статистике Азербайджана по итогам восьми месяцев 2015 года.

Объем доходов, полученных от услуг мобильной связи в Азербайджане в январе-августе 2015 года, составил 581,7 млн манатов, что на 2,2% меньше показателя аналогичного периода 2014 года.

По сообщению Fineko/abc.az в Азербайджане созданы все необходимые условия для перехода с протокола IPv4 на протокол IPv6. Как сообщил Fineko/abc.az технический директор компании Delta Telecom Раид Алекперли, инфраструктура IPv6 полностью готова с начала 2011 года: «На сегодня в стране практически иссякли резервы IP-адресов, основанных на протоколе IPv4, и число IP-адресов провайдеров, работающих в этом протоколе, намного ниже спроса на них. Но провайдеры не могут перейти сразу на протокол IPv6, так как этот процесс должен продвигаться синхронно с мировыми тенденциями технологического развития. Немаловажно также наличие контента, работающего на этом протоколе, в частности, необходимо перевести на новый протокол крупные популярные социальные сети и поисковые системы, работающие в настоящее время на основе протокола IPv4. В этом процессе важно активное участие как провайдеров, так и конечных пользователей и владельцев контента, а также поддержание данного протокола мобильными устройствами и т.д.».

Компанией Delta Telecom произведены необходимые работы в Национальном дата-центре, но среди провайдеров и владельцев контента не наблюдается особого интереса к приобретению и распределению IP-адресов IPv6, в результате чего использование этих адресов мизерно.

На сегодняшний момент средняя скорость соединения в Азербайджане равна 3.3Мбит/сек. Согласно сайту https://www.stateoftheinternet.com Азербайджан находится на 77-ом месте по количеству произведенных DDoS атак.

В Республике Азербайджан активно развивается проект Трансевразийская высокоскоростная информационная магистраль (Trans-Eurasian Information Super Highway - TASIM), который является регионально значимым проектом. Цель проекта - прокладка транснациональной волоконно-оптической линии, охватывающий евразийские страны от западной Европы до восточной Азии.

Проект предусматривает создание основной транзитной линии связи от Франкфурта (Германия) до Гонконга. Сеть объединит крупнейшие центры обмена информации Европы и Азии. Транзитная линия протянется по территории Китая, Казахстана, Азербайджана, Грузии, Турции до Германии. Запасная (Северная) транзитная линия связи пройдет по территории России, Украины и

Польши. 21 декабря 2012 года Генеральная ассамблея ООН приняла очередную резолюцию по проекту. Предложенная Азербайджаном с целью оказания поддержки реализации проекта TASIM резолюция предусматривает развитие соответствующей телекоммуникационной инфраструктуры, необходимой для предотвращения «цифровой пропасти» в широком евразийском регионе и укрепление сотрудничества между частным и государственным секторами.

Республика Азербайджан является инициатором и активным исполнителем многих региональных проектов. Реализация проекта «Транс-Евразийской суперинформационной магистрали» (TASIM), поддерживаемой резолюциями Генеральной Ассамблеи ООН (в 2009, 2012 и 2013 годах), а также использование возможностей «Европейско-Ближневосточной информационной магистрали» (Europe-Persia Express Gateway — EPEG), участником которой является наша страна, будут способствовать значительному повышению потенциала страны для выхода в Интернет. Планируется, что проект будет реализован в два этапа. На первом создается необходимая инфраструктура, а второй предполагает обеспечение недорогим доступом в интернет жителей стран, удаленных от моря.

В целях развития в стране конкурентоспособной инновативной ИКТ-промышленности с высоким экспортным потенциалом соответствующими указами Президента Республики Азербайджан в подчинении Министерства связи и высоких технологий Республики Азербайджан были созданы Государственный фонд развития информационных технологий и «Парк высоких технологий». Эти новые структуры обеспечат финансовую и организационную поддержку усилению экономики Республики Азербайджан, привлечению иностранных инвестиций и расширению производства ИКТ-продукции в стране, организации деятельности новых компаний и инновативным инициативам.

Республика Армения

В настоящее времят большая часть сельского населения Республики Армения живет в условиях ограниченного информационного поля, т.к. для операторов связи строительство сетей фиксированной связи в сельской местности и труднодоступных районах является весьма затратным делом. В городах республики более 87% семей имеют домашние телефоны, в тоже время в сельской местности в телефонизированных населенных пунктах таких семей менее 30%.

Наиболее весомым сегментом сферы электронных коммуникаций в Армении являются услуги мобильной связи – 60,5% . К концу 2011 года уровень проникновения мобильной связи в Армении превысил 108.2%, а количество абонентов, увеличилось за 5 лет более чем в пять раз. В Республике 98% домохозяйств имеют мобильные телефоны. Как и в других странах СНГ, такие высокие показатели отражают тот факт, что многие жители Армении, особенно молодые, используют несколько SIM-карт, чтобы получать преимущества от пользования услугами разных провайдеров мобильной связи.

На рынке мобильной связи Армении существуют три крупнейших лицензированных оператора мобильной связи: ЗАО «АрменТел» (торговая марка Beeline), «К-Телеком» (торговая марка Vivacell - MTS) и France Telecom Армении (торговая марка Orange).

Начиная с 2013, все операторы в стране имеют покрытие GSM, которое поддерживает сотовую передачу голосовых сообщений и данных 2G. Однако, полного покрытия всей страны сервисами 3G и 4G нет.

Большое влияние на развитие сектора ИКТ оказывает внедрение технологии беспроводного интернета Использование мобильного интернета, находится на уровне 15% населения страны, и

продолжает активно расти благодаря большому количеству пользователей мобильных телефонов и развитию беспроводных технологий.

В Армении Интернет-услуги предоставляют около 15 крупных и средних Интернет-провайдеров и операторов сетей WiMax. По данным Международного Союза Электросвязи, число пользователей Интернета в Армении уже 5 лет назад составляло более 1400 тыс. человек, что соответствовало 44% населения республики.

Интернет пользователям предлагается во всех видах технологий доступа, в том числе 3G мобильных сетей, WiMAX, ADSL, включая ADSL2+, FTTB в комбинации с коммуникациями линии электропередачи для распределения в пределах зданий, практикуется также FTTH стандарта GPON Услуга «Hi-Line», основанной на ADSL технологии доступна в г.Ереване и в 9 больших городах Армении. «CDMA Internet» услуга доступна для пользователей беспроводной сети CDMA в основном в сельской местности.

Покрытие 2G услуг составляет около 99% («Билайн», «ВиваСелл-МТС»), у «Оранж Армения» составляет около 99,8% населения: 3G-услуги (в том числе широкополосная передача данных и доступ к Интернет). На начало 2012 года обеспечивалось покрытие со стороны всех трех операторов порядка 85-90% населения. Все три компании продолжают расширять покрытие своих 3G услуг. Проникновение интернета в Армении достигло 52 процентов в 2012 году. Каждый год появляется примерно 900 новых хорошо оплачиваемых рабочих мест в сфере информационно-коммуникационных технологий.

В Республике Армения есть несколько локальных платформ социального взаимодействия. Наиболее популярный локальный вариант - Hayland, насчитывающий 156 тыс. зарегистрированных пользователей. По данным рейтинговой компании, оценивающей армянские веб ресурсы, ежедневный трафик портала в мае 2013 составлял около 52 тыс. просмотров, 48 процентов из которых внутри страны.

В 2007 году сектор информационно-коммуникационных технологий Республики Армения получил значимый стимул к развитию, когда Комиссия по регулированию общественных услуг Армении отменила спорную монополию «АрменТел» на международный интернет-доступ к передаче речи и данных. Наблюдатели отрасли на местах заметили, что это стало первым шагом к либерализации телекоммуникационного сектора. Это способствовало развитию местных провайдеров. В настоящее время у трех операторов остаются международные каналы: ЗАО «АрменТел» (Билайн), ЗАО «ДЖИЭНСИ-АЛЬФА» и ООО «Fibernet Communications».

«АрменТел» использует три международных канала. Первый из них, «Trans Armenia Optical System» (TAOS), с мощностью 7 Гбит/с, подсоединяется к Грузинской оптической магистрали, а затем к российским и европейским каналам. TAOS включает в себя северное «кольцо» (Ереван-Армавир – Гюмри – Ванадзор – Севан - Ереван) и южный «отросток», идущий от Еревана до Мегри на границе с Ираном. От Ванадзора опорная сеть расширяется до Грузии, а затем до России и подводной кабельной системы связи Черного моря. TAOS - один из основных путей, обеспечивающих связь внутри страны и с остальными странами, проходит через 30 крупнейших городов Армении и обслуживает примерно 60% всего населения страны. Дополнительным компонентом TAOS является столичная магистральная оптоволоконная сеть ArmenTel в г.Ереване, включающая логическое кольцо и расширения, присоединяющие основные АТС.

Вторая широкополосная сеть передачи данных, купленная у дочерней копании «Вымпелком» - «Совинтел», начала функционировать в сентябре 2008. Она проходит через Иран и имеет пропускную способность 155 Мбит/с. В качестве резервного маршрута «АрменТел»

использует спутниковое подключение «Teleglobe», производительность которого ограничена 2 Мбит/с. Согласно неофициальным источникам, также ведутся переговоры с турецкими компаниями о строительстве четвертого оптоволоконного канала (4 STU).

Сеть «ДЖИЭНСИ-АЛЬФА» проходит через Иран и Грузию. Южный сегмент, соединяющий г.Ереван и Иран, работает с сентября 2009 года. Два северных сегмента сети «ДЖИЭНСИ-АЛЬФА» между г.Ереваном и Грузией используются с марта 2010 года и соединяются с тремя оптоволоконными кабельными системами в Грузии при помощи двух независимых маршрутов.

ООО «Fibernet Communications», третий оператор, обладающий международным каналом, использует оптоволоконный кабель TRASEKA, принадлежащий государству и предоставляемый компании в рамках 25-летнего договора об аренде. «Fibernet Communications» обеспечивает покрытие всей страны с производительностью магистральной линии 1 Гбит/с и международными подключениями между г.Ереваном и г.Тбилиси, г.Москвой, г.Франкфуртом-на-Майне, г.Будапештом, г.Лондоном и г.Парижем. «Fibernet Communications» соединяет основные бизнес-центры Армении с партнерами в России и Европейских странах. В планах компании реализация крупномасштабных транзитных проектов в Иран и Турцию, которые соединят их с сетевыми операторами в Западной Европе и на Среднем Востоке.

Услуги спутниковой связи, сравнительно хорошо развитой в Армении, дороги. Спутниковая связь обеспечивается двумя наземными станциями, Intelsat и Express. Спутниковый доступ обычно используется провайдерами интернет-услуг с небольшим количеством конечных пользователей.

Республика Беларусь

Национальная стратегия устойчивого социально-экономического развития Республики Беларусь на период до 2020 года, одобренная протоколом Национальной комиссии по устойчивому развитию Республики Беларусь от 6 мая 2004 г. № 11/15ПР (Национальная стратегия), предусматривает, что развитие информационного общества является одним из национальных приоритетов Республики Беларусь и рассматривается как общенациональная задача, требующая координации и объединения усилий государства, бизнеса и гражданского общества. При этом информационно-коммуникационным технологиям отводится роль необходимого инструмента социально-экономического прогресса, одного из ключевых факторов инновационного развития экономики.

Система национальных приоритетов, сформулированная в проекте Основных положений Программы социально-экономического развития Республики Беларусь на 2011–2015 годы, предполагает создание благоприятных условий для интеллектуального и физического развития населения, инновационно-структурное обновление экономики, повышение уровня конкурентоспособности продукции на основе структурной перестройки, технико-технологического переоснащения и реструктуризации производства.

Для успешного выполнения намеченных планов социально-экономического развития страны необходимо эффективное использование современных факторов инновационного развития, к которым относятся ИКТ. Внедрение передовых информационных технологий в государственных органах, реальном секторе экономики, торговле, здравоохранении, образовании и других сферах жизни позволит значительно повысить производительность труда и качество жизни населения.

Развитие услуг в области информационных технологий является важнейшим фактором в обеспечении функционирования экономики и удовлетворения потребностей населения. Приоритетное развитие таких услуг позволило многим государствам Центральной и Восточной Европы преодолеть разрыв в уровнях социально-экономического развития по сравнению с лидирующими (развитыми) странами.

Формирование информационного общества обеспечивается наличием развитого человеческого капитала, высокого научного потенциала, системы государственной поддержки разработки ИКТ.

В настоящее время в республике завершилось формирование основ информационного общества. Заложена правовая основа информатизации. Успешно развивается национальная информационно-коммуникационная инфраструктура (ИКИ), позволяющая оказывать новые информационные услуги и услуги электросвязи на основе технологий широкополосного доступа. На протяжении последних 10 лет в результате выполнения государственных программ разработан ряд общегосударственных и ведомственных информационных систем. Республиканские органы государственного управления, большинство местных исполнительных и распорядительных органов представлены в глобальной компьютерной сети Интернет. Республика обладает достаточно развитой собственной информационной индустрией, что является одним из необходимых условий конкурентоспособности экономики. Национальная информационная индустрия, не ограничиваясь только прямым вкладом в валовой внутренний продукт, обеспечивает эффективное использование ИКТ в государственном управлении, социальной сфере, во всех отраслях экономики, повседневной жизни населения.

Вместе с тем успешное развитие информационного общества сдерживается рядом факторов. Для их устранения необходимо:

- ускорить создание инфраструктуры для предоставления государственными органами электронных услуг с использованием средств электронной цифровой подписи (ЭЦП);
- развивать экспортно-ориентированную отрасль услуг в области информационных технологий (ИТ-индустрия);
- расширить представительство государства, бизнеса, общественных организаций в глобальной компьютерной сети Интернет;
- принять меры по повышению уровня компьютерной грамотности государственных служащих и населения в целом;
- обеспечить эффективное применение современных возможностей ИКТ при решении задач в сфере занятости населения;
- совершенствовать систему взаимодействия государства и бизнеса в сфере информатизации.

Цель и основные задачи Национальной программы соответствуют стратегической цели устойчивого развития страны, которая определена Национальной стратегией как динамичное повышение уровня благосостояния, обогащение культуры, нравственности народа на основе интеллектуально-инновационного развития экономической, социальной и духовной сфер, сохранение окружающей среды для нынешних и будущих поколений, а также Стратегии.

По состоянию на май 2014 года сеть 2G Life (Лайф) охватывала свыше 93% территории страны, на которой проживает около 99,74% населения страны. Сеть 3G Лайф охватывала 29,6% территории страны, на которой проживает около 82,10% населения. Сеть Лайф в Беларуси обслуживается около 4 тыс. базовыми станциями стандарта GSM900/DCS1800/NODEB2100.

Клиенты компании могут пользоваться услугой международного роуминга в 105 странах мира. Лайф (Беларусь) имеет 15 собственных центров обслуживания по всей Беларуси. Дилерская сеть на территории Республики Беларусь насчитывает 132 эксклюзивных пунктов продаж, около 277 официальных представителей компании (дилеров), 170 магазинов партнеров «Евросеть» и «Связной», предлагающих услуги Лайф (Беларусь). Салоны Лайф присутствуют в 120 городах страны. Также по всей Беларуси работает до 100 активных продавцов (промоутеров) компании на 50 местах.

На 1 января 2014 года услугами компании «Велком» (Velcom) пользовались более 4950 тыс. абонентов. По результатам третьего квартала 2009 года доля компании на рынке мобильной связи составила 43,5%. Мобильной связью охвачено 96,6% территории страны, на которой проживает 99,3% населения (100% городских жителей).

Выручка компании (согласно данным международной финансовой отчётности) по результатам третьего квартала 2009 года составила 311,4 млрд рублей, показатель EBITDA (прибыль до вычета расходов по процентам, уплаты налогов и амортизационных отчислений) — 146,1 млрд рублей. За девять месяцев 2009 года сумма выручки составила 863,2 млрд рублей, EBITDA — 426,9 млрд рублей.

Связь GSM-оператора доступна жителям всех районных центров, городов и крупных населённых пунктов с численностью населения более 3 тысяч человек. По состоянию на декабрь 2009 в сети работали 3232, (ранее – 3125…3078) базовые станции и 28193 (ранее - 27223) приёмопередатчика в 1341 (ранее - в 1296) населённом пункте страны, а также 8 коммутаторов: 3 в г.Минске и по одному в каждом областном центре.

Клиенты компании могут пользоваться услугой международного роуминга в 161 стране мира в сетях 376 операторов. Унитарное предприятие «Велком» располагает собственной сетью фирменных центров продаж и обслуживания, состоящей из 61 офисов в 29 городах Беларуси. Дилерская сеть насчитывает 645 салонов в 154 населённых пунктах.

На конец 2014 года число активных абонентов компании «Мобильные ТелеСистемы» (МТС) составляло более 5,41 млн. и доля на рынке около 46%. Покрытие МТС охватывает 99% территории страны, на которой проживает 99,8% населения Республики Белорусь. Техническая инфраструктура сети МТС включает 6,2 тыс. базовых станций. Ежедневно она обрабатывает свыше 35,5 млн. звонков в почти 22 тыс. населенных пунктов Белоруси. В соответствии с ранее заявленными планами по развитию сети, 3G компания МТС обеспечила связью «третьего поколения» 91% территории Белоруси. Услуга международного роуминга предоставляется в 184 странах мира в сетях 512 GSM-операторов.

Интенсивно развивается сеть собственных центров обслуживания абонентов МТС. На конец 2015 года она включает более 1600 салонов (в том числе, более 70 собственных салонов связи МТС), центров обслуживания абонентов и пунктов продаж коммерческих представителей в 721 населенном пункте Белоруси.

Анализ опросов экспертов в области ИКТ показал, что состояние национально-инорфмационной инфраструктуры всеми экспертами оценивается скорее как высокое. Общий балл – 4,34. Оценка проводилась по следующим параметрам.

Качество и стоимость услуг мобильных операторов. В целом качество услуг двух ведущих операторов «Велком» и МТС оценивается как хорошее («Велком» немного впереди). По стоимости услуг предпочтение отдано МТС. Эксперты не смогли оценить третьего оператора – «Лайф».

Качество и стоимость услуг широкополосного доступа оцениваются как скорее удовлетворительные (более 4 баллов).

Качество контента ниже среднего (3,5 балла), *степень доступности контента* – удовлетворительная (более 4 баллов).

Степень использования социальных сетей близка к удовлетворительной – более 3,5 баллов.

Отмечается, что основной проблемой является качество белорусского контента в Интернет.

Грузия

Информационно-коммуникационные технологии в Грузии все больше интегрируются в экономику, общественную жизнь и политику страны. Сведения о контроле и надзоре немногочисленны, правительственные меры блокирования онлайн-контента отсутствуют. При этом даже в таких условиях все-таки отмечается серьезный недостаток прозрачности телекоммуникационной сферы. Состав собственников компаний намеренно скрыт за фиктивными фирмами и компаниями в оффшорных зонах.

Киберпространство Грузии отличается от того же пространства соседних государств Южного Кавказа. Интернет стал новой, цифровой версией общественной площадки, где люди встречаются и участвуют в разнообразных проявлениях политического диалога, дискурса и взаимодействия с политиками. Интернет Грузии также выделяется уровнем кибершпионажа и целевых вредоносных атак на высшем уровне государственной власти.

Правительство Грузии признает зависимость страны от киберпространства. Последствия военного конфликта 2008 года, в ходе которого было отмечено одно из первых киберстолкновений в условиях межгосударственного конфликта, показали уязвимость Тбилиси в киберпространстве. Правительством Грузии были предприняты дополнительные меры по обеспечению безопасности в интернет-пространстве.

На рынке фиксированных каналов связи Грузии можно отметить двух основных операторов: «Silknet» и «Caucasus Online».

В 2010 году произошло объединение бывшего государственного телефонного оператора «United Telecom» с «Ванекс» и «Электросвязь Аджарии», и образована компания «Silknet», которая, как утверждается, владеет половиной общей абонентской базы и удерживает высший показатель абонентов DSL - 76%. Это объясняется историей образования компании, поскольку компании «United Telecom» ранее принадлежала проводная сеть телекоммуникаций всей страны.

«Caucasus Online», второй крупнейший интернет-провайдер, организован путем слияния «Sanet», «Georgia Online» и «Caucasus Telecom». Компания удерживает порядка 30% рынка интернет-услуг, что значительно меньше ее практически монополистической позиции 2007 года, когда ей принадлежала доля 90%. Несмотря на то, что компания больше не доминирует на рынке, «Caucasus Online» по-прежнему обслуживает около трёх четвертей оптоволоконного сегмента. В реестре юридических лиц Грузии нет данных о структуре владения компанией, поскольку она зарегистрирована за рубежом.

Рынок провайдеров Грузии полностью приватизирован и насчитывает около 20 компаний. В числе менее крупных компаний отмети «Ахали Кселеби» («New Net»), интернет-провайдер и

оператор телефонной связи, охватывающий города Тбилиси, Кутаиси, Гори, Зестафони, Терджола, Зугдиди и Поти. Это третий по размеру провайдер, которому принадлежит порядка 7% рынка.

«Центральная корпорация связи Грузии» (Central Georgian Communications Ltd, CGC) действует как оператор местной и междугородней телефонной связи с 1995 года, обслуживая г. Рустави и прилегающие территории. Весной 2009 года компания также начала предлагать услуги высокоскоростного интернета на базе технологий DSL.

В Грузии работают три основных оператора мобильной связи: «Geocell», «Magticom» и «Mobitel» (Билайн). «Magticom» была первой компанией, которая получила лицензию на предоставление услуг мобильной связи в Грузии (в 1995 году). В 1998 к ней присоединилась компания «Geocell». Третий оператор Грузии, «Билайн» пришел на рынок лишь в 2007 году.

Компания «Geocell» обогнала «Magticom» и заняла лидирующую позицию на рынке в 2012 году, охватив 41% абонентов. «Geocell» принадлежит шведской телекоммуникационной компании «TeliaSonera». «Geocell» предлагает мобильный интернет по технологии 2G и 3G.

Компания «Magticom» - вторая крупнейшая телекоммуникационная компания с долей рынка приблизительно 30%, предлагающая широкополосный доступ по различным стандартам 2G и 3G.

Компании «Mobitel» принадлежит примерно четверть рынка, предлагает широкополосный доступ по GPRS в силу ограниченности частотного ресурса. Такой доступ относится к стандарту 2G, поддерживающий обмен данными по мобильной сети.

Компания «Silknet» начала предлагать услуги мобильного доступа в конце 2012 года, и ее доля составляет лишь 0,01%. Доля остальных провайдеров вместе составляет примерно 6% рынка.

Рынок WiFi насчитывает порядка 4500 абонентов, которые сосредоточены в основном в сельской местности, где нет оптоволоконных сетей. WiFi-сети способствуют проникновению интернета за пределами городов, но т.к. они обслуживаются мелкими провайдерами, их общее влияние невелико. Число абонентов в 2011 году выросло лишь на 3 тысячи. Тем не менее, рынок WiFi отличается довольно высокой конкурентоспособностью, здесь представлены 33 небольшие компании и явные лидеры отсутствуют.

Отметим, что в Грузии мало международных подключений к опорной сети интернета. Возможности международного сетевого взаимодействия ограниченны отсутствием внешних каналов связи. Согласно исследованию «Freedom on the Net», в результате этого недостаточного количества внешних каналов связи интернет-пользователь в Грузии может быть отсоединен от международного интернета 2-3 раза в месяц. Инфраструктура опорной сети Грузии проходит с востока на запад и соединяется по наземным путям с Арменией и Азербайджаном. Но она особенно зависит от Турции и России, как напрямую, так и по нисходящим каналам. Среди основных провайдеров - «Deltacom» в Азербайджане с дальнейшей маршрутизацией на Россию через «TransTelecom», а также посредством турецкого оператора «TTNet».

Грузинская телекоммуникационная компания «Fiber-Optic Telecommunications Network» (FOPTNET) совместно с ПАО «Ростелеком» (Россия) и «DanTelcom» (Дания) построила подводную волоконно-оптическую кабельную систему в Черном Море, которая, проходя через Сочи, связывает систему «Грузинская оптическая магистраль» с крупным телекоммуникационным узлом в г.Новороссийске. Второй международной подводной волоконно-оптической кабельной системой управляет «Caucasus Online», и она через Черное Море связывает Грузию с Болгарией и далее с европейскими сетями.

Линия «Грузия-Россия» также обеспечивает доступ к Кавказу, Центральной Азии и Восточной Азии посредством волоконно-оптической кабельной сети Транс-Азия-Европа (TAE). Через территорию Грузии также проходит Трансевразийская высокоскоростная информационная магистраль (TASIM), которая по плану должна обеспечить прокладку транснациональной волоконно-оптической линии, охватывающей страны от Западной Европы до Азии.

Спрос на высокоскоростной интернет создал важный рынок для провайдеров. Были проведены значительные инвестиции в развитие сектора информационно-коммуникационных технологий.

Показатели проникновения интернета в Грузии составили 45,5% в 2012 году по сравнению с 10% в 2008. Число пользователей мобильного интернета выросло на 50%, достигнув 1,2 миллиона в конце 2012 года. Число абонентов мобильной связи достигли 4,4 миллионов или 100% проникновения, что ниже среднего показателя по региону в 135%. За этот же период объем национального интернет-трафика увеличился более чем вдвое, от 180 до 370 ТВ.

С 2010 года количество абонентов широкополосного доступа в Интернет выросло на 35%, достигнув почти 400 тысяч, но в 2012 году темпы снизились до 5% (Georgian National Communications commission, GNCC Annual Report 2011 and statistical database). Число пользователей оптоволоконных линий связи выросло приблизительно на 50%, а линий DSL — на 23 процента. Связь по телефонной линии через модем практически вышла из употребления, и спутниковый интернет идет за ней следом (Georgian National Communications commission, GNCC Annual Report 2010).

Снижение тарифов также сыграло важную роль в привлечении новых клиентов. Доступ в интернет по оптоволоконному соединению со скоростью 50 Мбит стоит приблизительно 30 долларов США в месяц, тогда как стоимость линии 22 мб/с составляет порядка 18 долларов США в месяц. Провайдеры, обладая технической оснащенностью и предлагая конкурентоспособные цены, начали продвигать дополнительные услуги, такие как VoIP (онлайн-телефония) и IPTV (онлайн-телевидение).

Регистрация доменных имен в Грузии осуществляется исключительно одним коммерческим интернет-провайдером — «Caucasus Online». На сегодня в зоне .ge зарегистрировано порядка 30 тысяч доменных имен. При этом, лишь около 20 тысяч из них активны. Доменные имена нельзя зарегистрировать онлайн. Для этого необходимо распечатать бланк и подать его в офис «Caucasus Online» в г.Тбилиси вместе с удостоверением личности или, в случае регистрации корпоративного домена, вместе с ИНН компании. Имена и электронные адреса владельцев зарегистрированных доменов доступны на сайте registration.ge.

В Грузии действует более 320 лицензированных провайдеров и сетевых операторов. Согласно годовому отчету за 2011 год, Национальной комиссии Грузии по коммуникациям (GNCC), доля телекоммуникационного сектора в ВВП составляет 0,5%.

Отдельные точки обмена интернет-трафиком в Грузии отсутствуют. Техническое взаимодействие между телекоммуникационными компаниями основано на отдельных соглашениях. Впервые пиринг был регламентирован Директивой GNCC относительно пиринга (№6, 10.06.2001), которую позднее заменил Закон об электронных коммуникациях. Услуги VoIP регулируются как обычные услуги телефонии Законом об электронных коммуникациях.

Большинство интернет-пользователей Грузии — частные лица и более половины из них, 55%, женщины. У двух третей всех интернет-пользователей есть профиль в социальной сети, то есть 30% населения Грузии пользуются социальными сетями.

Интернет занял второе по важности место среди источников новостей и информации после телевидения. Результаты опроса показали, что 6% респондентов узнают новости политики онлайн, а еще 12% считают Интернет в целом важным источником информации. К онлайн-источникам новостей не предъявляются требования лицензирования, выход на этот рынок отличается минимальными препятствиями и низкой себестоимостью.

Республика Казахстан

Развитие информационно-коммуникационных технологий является одним из важнейших факторов повышения конкурентоспособности казахстанской экономики. Процесс глобализации, конвергенции и диффузии экономик различных стран требует от Казахстана перехода к качественно новому уровню развития, без которого невозможно занять достойное место в мировой экономической системе. Современная телекоммуникационная отрасль занимает особое положение в экономике страны, поскольку наиболее приближена к мировым стандартам по таким критериям, как темпы роста, конкурентоспособность представляемых услуг, уровень развития научно-технической базы, профессионализм менеджмента.

Сфера ИКТ Республики Казахстан стала самостоятельным сектором экономики. Она состоит из отрасли телекоммуникаций, почтовых услуг, отрасли информационных технологий и распространения телерадиосигнала. Данный подход обусловлен взаимным проникновением технологий связи, распространения телерадиовещания и информационных технологий, который наблюдается в последние десятилетия по всему миру. Значительный прогресс в использовании информационных технологий правительствами стран Центральной Азии зарегистрирован Всемирным банком за последние четыре года. Об этом говорится в обзоре «Использование информационных и коммуникационных технологий в повышении гражданской активности в Центральной Азии», презентованный Всемирным банком в г.Бишкеке в 2014 году.

В Казахстане значительный прогресс получили такие проекты как, «электронное правительство», получение государственных услуг через интернет, блоги чиновников, связь через интернет-сайт с муниципальными властями, а также открытые государственные данные. «В 2012 году Казахстан улучшил свои позиции в мировом рейтинге стран, внедривших систему электронного правительства, заняв второе место среди развивающихся стран. Электронные услуги являются приоритетным направлением в области электронного правительства. Государственный портал обеспечивает единую точку входа ко всем услугам электронного правительства», — отмечают эксперты Всемирного банка.

В отчете Агентства по статистике Республики Казахстан об использовании информационно-коммуникационных технологий в Казахстане в 2013 году отмечается, что число интернет-пользователей в возрасте 6–74 лет (с учетом пользователей мобильного интернета) в 2013 году составило 63,3% от общего числа населения, а количество пользователей компьютером - 63,2%. Наибольший процент пользователей Интернета среди городского населения зафиксирован в Атырауской (88,6 %), Мангистауской (87,8%) и Актюбинской (85,3%) областях. Среди сельского населения - в Костанайской (71%), Кызылординской (64%) и Акмолинской (62,8%) областях. Наибольшее число пользователей компьютером среди городского населения - в Атырауской (84,2%), Кызылординской (83,1%) и Актюбинской (80%) областях. Среди сельского - в Атырауской (67,3%), Кызылординской (66,4%) и Костанайской (63,5%) областях. В г.Астане

число интернет-пользователей составляет 64,5%, ПК-пользователей - 62,2% от общего числа населения. В г.Алматы -71% и 68,5%, соответственно .

Согласно рейтингу Международного союза электросвязи за 2007–2008 гг. Казахстан лидирует среди стран Центральной Азии, опережая такие страны как Кыргызстан, Туркменистан, Таджикистан, Узбекистан и занимает 69 место.

Задача сделать Казахстан развитой страной автоматически подразумевает под собой увеличение доли высокотехнологичной продукции в валовом продукте страны, то есть такой продукции, в цене которой большую долю составляет не сырьевая составляющая и физический труд, а интеллектуальная часть. Международный опыт разделения труда показывает устойчивую тенденцию переноса производств в такие страны, в которых можно добиться снижения себестоимости продукции за счёт климатических условий, удобностей транспортировки и избытку рабочей силы. В то же время, где бы реально не производилась продукция, большая часть дохода от её реализации оседает в тех странах, в которых эти изделия были разработаны.

Рост экономики Казахстана позволяет направлять часть бюджетных средств на развитие перспективных высокотехнологичных производств и обучение специалистов, необходимых для этих производств. В то же время, учитывая мировой опыт, приоритет должен отдаваться не столько созданию самих производств, сколько развитию предпосылок для появления большего числа предприятий, занимающихся разработкой новой, высокотехнологичной продукции, востребованной в первую очередь на мировом рынке. Это подразумевает организацию массовой подготовки инженерно-технических и научных кадров, ориентированных не на эксплуатацию технических средств, а на их разработку.

В настоящее время производство Республики Казахстан ориентировано на строительство постиндустриального общества, характеризующегося опережающим развитием и ростом доли сферы информационно-коммуникационных товаров и услуг. Концепция постиндустриального общества ориентирована на развитие цивилизации, в которой главными продуктами производства являются информация и знания.

Её отличительная особенность создание глобального информационного пространства, обеспечивающего эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам и удовлетворение потребностей в информационных продуктах и услугах.

В Казахстане ИКТ является видом экономической деятельности (ВЭД), который включает 4 области профессиональной деятельности:

1. Информационные технологии - разработка и внедрение программного обеспечения, монтаж, сопровождение и обслуживание информационно-коммуникационного оборудования;

2. Электроника, микропроцессорная техника - создание, производство микропроцессорной техники, сопровождение и обслуживание электронной части информационно-коммуникационного оборудования, дискретного и процессного производств;

3. Автоматизация, робототехника - создание систем автоматизации, робототизации их сопровождение и обслуживание в дискретных и процессных производствах**;**

4. Связь - обеспечение передачи, приема, обработки и хранения информации.

В Индексе развития информационно-коммуникационных технологий 2012 года Казахстан занимает 49 место среди 155 стран, на 7 позиций выше предыдущего рейтинга.

В начале 2013 года в Казахстане была принята Государственная программа «Информационный Казахстан – 2020». Данная программа определяет роль и место ИКТ в современном развитии Казахстана. В документе отмечается, что в «период реализации Стратегического плана – 2020 будет ускорена диверсификация экономики путем форсированной индустриализации», которая нацелена на комплексное повышение производительности экономики, по таким направлениям отраслей как: нефтегазовый, горно-металлургический, атомной, химической и других. Получат развитие такие сектора экономики как: машиностроение, стройиндустрия, оборонная промышленность, фармацевтика; агропромышленный комплекс, легкая промышленность, туризм. Большое внимание уделяется в Стратегическом плане развитию секторов «экономики будущего», которые будут играть доминирующую роль в мировой экономике в последующие 15-20 лет: ИКТ, биотехнологии, альтернативная энергетика.

Сущность и структура рынка ИКТ сферы Республики Казахстан - это «создание конкурентоспособного отечественного рынка ИКТ через развитие инфокоммуникационной и инновационной инфраструктуры и научно-исследовательской деятельности». ИКТ охватывает все отрасли экономики и направления деятельности государства и призвано стимулировать ИКТ рынок, обеспечивать эффективность системы государственного управления, доступности информационно-коммуникационной инфраструктуры, создание информационной среды для социально-экономического и культурного развития общества.

Большое внимание уделено развитию ИКТ инфраструктуры промышленных предприятий, роботизации всех производственных процессов с высоким уровнем опасности для здоровья и жизни человека, внедрению автоматизированных систем управления технологическими и внутренними процессами предприятия промышленности, развитие инновационной деятельности предприятиями промышленности путем тесного взаимодействия с отечественными научно-исследовательскими организациями и высшими учебными заведениями. С учетом мировых тенденций уделено внимание и стимулированию промышленных предприятий к внедрению энерго-, ресурсосберегающих, «зеленых» ИКТ в производственном процессе путем использования инструментов поддержки в рамках Закона Республики Казахстан «О государственной поддержке индустриально-инновационной деятельности» и совершенствования налогового и земельного законодательства.

Должна получить развитие электроника, использование телеметрических датчиков и геоинформационных систем для мониторинга за состоянием агрегатов и узлов объектов промышленных предприятий для предупреждения и предотвращения аварийных и иных чрезвычайных ситуаций. Без развития электроники не возможно развитие промышленными предприятиями своей логистической и складской инфраструктуры для оптимизации процесса учета складских запасов, контроля перемещения грузов с применением технологии радиочастотной идентификации (RFID), геоинформационных систем и ERP систем.

Рынок телекоммуникационных услуг в Казахстане динамично развивается, конкуренция в этом сегменте растет, так же как и спрос на подобные услуги. Компьютер заменяет огромное количество рабочей силы, на которую в свое время тратились огромные средства, но теперь эти расходы могут значительно сократиться за счет использования современных систем. В сферу этих

услуг традиционно входят услуги сотовой связи, услуги фиксированной телефонной линия связи и услуги доступа к сети интернет, услуги и средства почтовой и курьерской деятельности и связи.

В этом направлении в целом идет последовательный динамичный рост, кроме показателей доставки газет, писем и телеграмм.

Успешно развивается на рынке Казахстана мобильная связь, объемы которой с каждым годом растут. Удельный вес этого вида связи в общей сумме доходов за 2011 г. составлял свыше 50%. Число абонентов сотовой связи в 2011 г. превысило 25 млн. За год количество абонентов сотовой связи увеличилось на 30%.

Банк Развития Казахстана опубликовал обзор по информационно-коммуникационным технологиям, на основе мировых тенденций отрасли, а также анализа отечественного сектора ИКТ вкотором отмечается следующее.

По итогам 1 квартала 2014 года, большую часть услуг в области ИКТ в Казахстане, составляет мобильная связь (42,44%), которая, по сравнению с соответствующим периодом 2013 году, сократилась на 1,79%. Затем идут услуги связи через Интернет, выросшие на 23,67%, что составляет 13,56 млрд. тенге или 25,21% среди всех услуг связи.

В 2014 году рынок смартфонов в Казахстане вырос более чем на 100%, но вырасти также в денежном выражении, ему не удалось. С одной стороны, основные игроки рынка телекоммуникаций не проиндексировали цены по курсу и покупатели стали активнее покупать смартфоны. С другой стороны, произошло снижение доли дорогих устройств. Основная часть премиальных смартфонов продавалась с рассрочкой платежа.

Услуги мобильной связи представляют собой наиболее динамично развивающийся сектор, значительно опережающий по темпам роста остальные секторы. Объем выручки в 2013 году составил 307 млрд. тенге, это представляет собой 48% от совокупного объема выручки на рынке.

Объем выручки в сегменте услуг предоставления доступа в Интернет и передачи данных в мобильных сетях в 2013 году составил 47,4 млрд. тенге, что более чем на 40% выше по сравнению с 2012г., тогда как объем рынка широкополосного доступа в сетях фиксированной связи в 2013 году составил 72,7 млрд тенге, увеличившись всего лишь на 18%.

По данным аналитического агентства «IKS-Consulting», число активных устройств с доступом в Интернет и передачей данных в мобильных сетях в 2013 году составило около 2,8 млн. единиц.

Более 90% всего телекоммуникационного рынка Республики Казахстан сконцентрировано в рамках «первой десятки операторов»:

АО «Кселл» - ведущий оператор мобильной связи в Казахстане, использующий два бренда: Kcell и Activ, суммарная абонентская база которых в Казахстане составляет 14,3 млн. пользователей. Контролирующий акционер Компании – TeliaSonera, один из крупнейших телекоммуникационных холдингов в Европе и на мировом рынке.

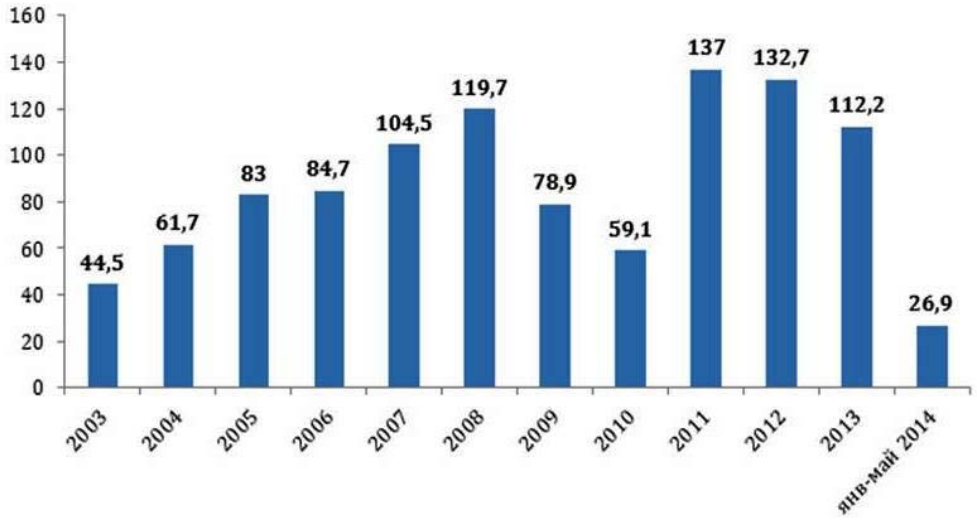
ТОО «Мобайл Телеком-Сервис» - европейский оператор связи с торговой маркой Tele2, обслуживающий более 15 млн. абонентов в 10 странах мира. В РК Tele2 появилась в 2010г., вызвав ажиотаж на рынке благодаря низким ценам.

ТОО "КаР-Тел" занимает 34,2% рынка, тогда как в I квартале 2013г. речь шла о 31,5%-ной доле. Это свидетельствует о закреплении позиции компании на рынке: стремительном увеличении клиентской базы, а вместе с ним и доходов.

АО «Казахтелеком» - крупнейший оператор связи в Республике Казахстан, предоставляющий широкий спектр инфокоммуникационных услуг. В конце 2012 года АО «Казахтелеком» под торговой маркой Altel 4G запустил первую в Казахстане коммерческую сеть стандарта LTE 4G в г.Астане и г.Алматы, и приступил к строительству сети мобильной связи и передачи данных стандарта LTE в других регионах страны, что объясняет изменение чистой прибыли (-93,59%).

В 2013 году совокупный объем мирового рынка в сфере инновационных облачных технологий составил порядка 40 млрд долл. По некоторым оценкам, к 2020 году этот показатель достигнет 240 млрд долл. При этом объем рынка облачных технологий в Республике Казахстан можно оценить в 2% от общего рынка ИТ-услуг, который в 2013 году составил 36 млрд. тенге. Уровень проникновения пользования облачными услугами в Казахстане на сегодня крайне низок - 0,4% от общего числа населения страны.

После мирового кризиса отмечается резкий рост объема прямых инвестиций в сектор информации и связи. Однако за последние 2 года наблюдается незначительное снижение доли инвестиций в сектор информации и связи в общем объеме инвестиций.



Объем инвестиций в секторе информации и связи в Республике Казахстан (млрд. тенге)

Планируется формирование венчурного фонда «Фонд развития ИКТ» за счет частного капитала, а также капитала международных компаний. Фонд будет инвестировать в проекты от 100 тыс. до 3 млн. долл. США ежегодно.

В 2013 году отмечается увеличение кредитования банками второго уровня сектора связи на 15,7% или 89,93 млрд. тенге по сравнению с 77,73 млрд. тенге в 2012 году.

АО «Банк Развития Казахстана» профинансировал 3 крупных проекта республиканского значения в области ИКТ:

- строительство волоконно-оптической линии связи (ВОЛС) на участке Астана-Алматы с предоставлением услуг 155 каналов связи;
- строительство магистральной ВОЛС на участках ШУ-Кандыагаш, Астана-Павлодар-Семей-Актогай, Кокшетау-Костанай (общей протяженностью 3950 км.);
- создание сети передачи данных G-Net (услуги Интернет и кабельного телевидения) до 5 тыс. абонентов в каждом регионе (города Павлодар, Актобе, Караганда,Усть-Каменогорск, Актау, Атырау, Уральск, Шымкент). Также, ожидается финансирование проекта по строительству аппаратно-программного комплекса и платформы связи вдоль железнодорожных линий.

В отчёте Агентства Республики Казахстан по статистике об использовании информационно-коммуникационных технологий в Казахстане в 2013 году на основании данных по 21 тысяче домохозяйств представлены следующие показатели наличия и использования тех или иных средств ИКТ: 98,9% — телевизоры; 96,8% — мобильные телефоны; 87,7% — фиксированную телефонную линию; 66,6% — настольный компьютер; 44,9% — кабельное телевидение; 39,7% — спутниковое телевидение; 18,5% — портативный компьютер; 12,3% — планшетный компьютер; 12% — радиоприемники; 2,8% — игровые консоли; 0,9% — факсимильный аппарат.

Кыргызская Республика

Кыргызстан пережил значительное улучшение практически во всех областях ИКТ в период с 2010 по 2015 год.

Рост международной пропускной способности интернета был особенно значительным. Строительство новых оптико-волоконных линий связи с Китаем и Казахстаном было завершено в 2013 году. Оптическая линия связи (оператор Элкат – Elcat) с производительностью 2,5 Гбит/с, с возможностью расширения до 40 Гбит/с связала города Нура (Китай) и Карамык (Кыргызстан). Другая оптико-волоконная линия связи была проложена между городамиу Бишкек (Кыргызстан) и Чалдовар (Казахстан) с начальной емкостью 2,5 Гбит/с, с возможностью расширения до 40 Гбит (ЭСКАТО ООН, 2014). В течение 2014 года построены волоконно-оптические линии связи в направлении Таджикистана, Узбекистана и Китая (East Horizon, 2014). Это помогло повысить конкуренцию и снизить цены при одновременном укреплении международной связи.

Правительство Республики Кыргызстан приложила большие усилия для реализации использования в коммерческих целях радиочасто, что позволило расширить доступ в Интернет в школах для сельских районов.

Следует отметить, что уровень фиксированной телефонной связи упал на 14% в период между 2010 и 2015 годами. Также остается ограниченный доступ в стране домохозяйств к Интернету. Жители продолжают использовать точки коллективного доступа к Интернету. По некоторым оценкам около 50% пользователей использую доступ к Интернету в киберкафе (East Horizon, 2014). По данным Всемирного экономического форума (World Economic Forum) Республика Кыргыстан в 2015 году заняла 98 место в Индексе готовности сетей (The Networked Readiness Index 2015) и 102 место в Индексе наличия условий для развития ИКТ (Environment subindex and pillars) из 143 стран мира, что, по сравнению с 2014 годом, улучшило показатель на 20 и 12 пунктов соответственно.

С ростом количества пользователей интернета, социальных сетей, мессенджеров, в республике Кыргызии приходят всевозможные проявления киберпреступности. Чем больше интернет-пользователей, тем больше число людей, которые могут стать жертвами кибермошенников.

Анализ показывает, что в настоящее время в Кыргызстане не достаточно уделяют должного внимания информационной безопасности. Проблемой является отсутствие обязательных для всех государственных органов единых требований к информационной безопасности, включая обучение руководителей подразделений и всего задействованного в оказании государственных и муниципальных услуг в электронном формате персонала принципам и технологиям защиты конфиденциальной информации.

Республика Молдова

В 2014 году Республика Молдова поднялась на четыре позиции в международном рейтинге по уровню развития информационно-коммуникационных технологий, составленном Международным союзом электросвязи с целью мониторинга развития информационного общества во всем мире.

По данным ежегодного доклада Международного союза электросвязи «Measuring the Information Society 2014», Молдова оказалась 61-й из 166 стран, где проводился мониторинг, а в 2013 году она занимала 65-ю позицию в списке. Таким образом, Молдова превзошла на 0,95 пунктов мировой средний показатель.

Также в докладе установлен рейтинг стран по уровню развития, проникновения и доступности для населения информационно-коммуникационного сектора. Молдова находится в группе стран со средним уровнем данного показателя, между Румынией (58-я строка рейтинга) и Украиной (73-я строка). Лидерами этого списка являются Дания, Южная Корея, Швеция, Исландия, Великобритания, Норвегия, Голландия и Финляндия.

На рынке доступа в Интернет в Республике Молдова доминируют такие провайдеры, как: Moldtelecom, StarNet, SunCommunications и Интерднестрком.

Компания SunCommunications предоставляет доступ в интернет через коаксиальный кабель и оптоволкно (в двух городах Кишинев и Бельцы).

Компания StarNet предоставляет доступ в Интернет через оптоволокно. Услуга доступна жителям городов Кишенев, Комрат, Унген и Оргеев, проживающим в многоэтажных домах.

Компания Moldtelecom – основной поставщик услуг через оптоволокно в Молдове. Услуга доступна в большинстве городов.

Компания Интерднестрком предлагает подключение к оптоволокну домашним пользователям и индивидуальным предпринимателям. Как правило, используются технологии ADSL, FTTB, Wi-Fi и Mobile.

Покрытие территории и населения сетями электронных коммуникаций

№	Услуга связи *(по состоянию на начало 2014 г.)*	Наличие доступа		Проникновение	
		(% от населения страны)	**(% от общего числа населенных пунктов)**	**(% домохозяйств)**	**(% от населения страны)**
1.	Фиксированная телефония (включая радиодоступ WLL)	99,89%	98,3%	95%	34,3%
2.	Мобильная телефония 2G (GSM/CDMA)	99,0/99,0/96,82 %	99,0/98,07/97,36 % тер. страны	-	124,5%
3.	Сотовые мобильные сети 3G	99,0/81,2/62,01 %	99,0/80,4/77,71% тер. страны	-	
4.	Сотовые мобильные сети 4G/LTE	28/14	2,15//0,07%	-	0,25%
5.	Фиксированный широкополосный доступ в Интернет	93%	76,77%	38,95%	13,1%
6.	Фиксированный широкополосный доступ в Internet по технологии FTTx	42%	5,17%	19,08%	6,42%

К началу 2014 года на рынке фунционировали: 30 операторов фиксированной связи, 3 оператора мобильной связи, 55 Internet-провайдера, 148 провайдеров ТВ услуг (MMDS, кабельного, спутникового, IPTV).

Конкуренция на рынке фиксированных каналов доступа в интернет растет, но государственный оператор АО «Moldtelecom» продолжает доминировать. На 2014 год в Молдове действовали десять провайдеров первого уровня: «Moldtelecom», «StarNet», «Arax», «Orange», «Интерднестрком», «Moldcell», «SunCommunications», «Relsoft», «Riscom» и «Dynamic Network Technologies». Еще 45 провайдера обеспечивают доступ всем регионам страны.

«Moldtelecom» охватывает приблизительно 69% общего числа интернет-абонентов, за ней следует «Starnet» с 17,5%, «SunCommunications» с 5% и остальные провайдеры, обслуживающие оставшиеся 13,5%. Большинство интернет-провайдеров арендуют объекты инфраструктуры у «Moldtelecom» и используют одну точку обмена интернет-трафиком (IXP), которая также контролируется государственным оператором. Положение «Moldtelecom» вызывает вопросы относительно свободной и справедливой конкуренции рынка фиксированных каналов связи. Примечательное исключение составляет Приднестровье, где основным оператором, предлагающим услуги доступа в интернет в широком масштабе, является «Интерднестрком».

Компания Ookla провела тестирование скорости Интернета по Молдове в 2014 году и предоставила результаты в цифрах. Сравнивалась скорость доступа в Интернет у операторов в разных регионах Молдовы. Согласно полученным данным, средняя скорость, предоставляемая интернет-провайдерами, составляет 36,4 Мбит/с, что намного меньше, чем в соседней Румынии, где скорость в среднем по стране составляет 56,2 Мбит/с. Самую высокую скорость Интернета по республике в 62,95 Мбит/с предлагает компания Starnet, за которой следуют Nordlinks – 61,12 Мбит/с, Inet Techno – 54,25 Мбит/с, Danis – 52,45 Мбит/с и Sun Communications – 48, 95 Мбит/с.

Аж Национальный Оператор Moldtelecom оказался на 12 месте со скоростью Интернета 31,28 Мбит/с. Заключают список мобильные операторы Orange (15,51 Мбит/с) и Moldcell (10,13 Мбит/с)

В Молдове действуют три основных оператора мобильной связи: «Moldcell» (основной акционер — «TeliaSonera»), «Orange Moldova» (принадлежащий «France Telecom Orange») и государственный оператор связи «Moldtelecom». На 31 марта 2012 года компания «Orange Moldova» отличалась самым большим числом абонентов выделенного широкополосного мобильного доступа, составлявшим почти 80 тыс., за ней шла компания «Moldcell» с более чем 38 тыс. абонентами, а затем «Moldtelecom» с порядка 27 тыс. абонентов.

Проникновение мобильного доступа сотовой связи достигло в 2012 году почти 115%, тогда как мобильный широкополосный доступ охватил лишь 5% (Annual Report for 2012, of the National Regulatory Agency for Electronic Communications and Information Technology). В том же году общий объем мобильного интернет-трафика, потребляемого пользователями мобильной голосовой связи, достиг 575,8 тысяч Гб или порядка 36,8 Мб на одного пользователя в месяц. Общий объем интернет-трафика пользователей выделенного широкополосного мобильного доступа составил более 15943,97 тысяч Гб или порядка 8,8 Гб на одного абонента в месяц (Annual Report for 2012, of the National Regulatory Agency for Electronic Communications and Information Technology).

Технологии мобильного доступа в интернет становятся все более сложными. Все основные провайдеры предлагают мобильный доступ в интернет по 3G/HSDPA со скоростью загрузки до 42 Мбит/с. «Orange Moldova» и «Moldcell» предлагают доступ по стандарту LTE со скоростью до 100 Мбит/с. Компания «Orange Moldova» стала первым в мире провайдером, запустившим 11 июля 2010 года испытание сервиса LTE 4G с публичной демонстрацией его возможностей. Однако доступ пользователей стал возможен только в конце 2012 года.

В первом триместре 2015 года рост числа пользователей интернета посредством сети 4G составил 34,7%.

Соответствующие данные содержатся в отчёте Национального агентства по регулированию в области электронных коммуникаций и информационных технологий (НАРЭКИТ).

За отчётный период доступом к интернету через сети 4G воспользовались 35,4 тыс. пользователей мобильной связи. В то же время увеличилось и количество пользователей услуг мобильного широкополосного доступа к Интернету (посредством модемов, карточек или USB). В первом квартале 2015 года было зафиксировано 1 миллион 245,8 тысяч таких пользователей, что на 4,8% больше прошлогодних показателей.

По данным НАРЭКИТ, в январе-марте 2015 года общий объём мобильного интернет-трафика составил более 9,6 миллиона Гб, превысив показатели такого же периода 2014 года на 43%.

Российская Федерация

Несмотря на впечатляющие темпы роста в последние 10 лет, абсолютные объемы рынка ИКТ в России остаются скромными. Доля расходов на ИКТ к ВВП в России составляет лишь 1,2 %, в то время как в развитых странах данный показатель находится на уровне 3-4%.

В 2013 году большую долю рынка ИКТ занял рынок аппаратных средств — 51,3%. На рынок программных средств пришлось 20,3%, на рынок услуг — 28,4%.

В 2014 году в структуре ИКТ-рынка произошли изменения в сторону снижения доли аппаратных средств до 45,8% при росте доли рынка программных средств до 24% и рынка услуг до 30,2%.

Темпы роста секторов ИКТ-рынкав РФ на 2013-2015 гг. (%%)

Рынок информационно-коммуникационных технологий	**Темпы роста в 2013 г.**	**Темпы роста в 2014г.**	**Темпы роста в 2015г.**
Рынок программных средств	10,5	11.2	12,4
Рынок аппаратных средств	4,7	4,3	4,1
Рынок ИТ-услуг	7,1	8,2	9,4

Росту объема ИКТ-рынка способствовало стимулирование внутреннего спроса на информационно-коммуникационные технологии; оказание государственных услуг в электронном виде; распространение в обществе базовых навыков использования информационных технологий; совершенствование налогового и таможенного регулирования.

В настоящее время в области ИТ наблюдается смена технологических эпох. Уходящую эпоху определяли такие продукты, как серверы или корпоративные базы данных, а теперь на первый план выходят новые решения: «облачные» вычисления, инструменты по обработке огромных массивов структурированных и неструктурированных данных (Big Data), модели развития бизнеса в социальных сетях (Social Business), программные продукты для совместной работы (Collaboration Software) и другие.

Рост наблюдается и в сегменте телекоммуникаций. По мнению аналитиков Gartner, мировые расходы на телекоммуникационные услуги в 2014 году выросли на 1% по сравнению с 2013 годом и составляют около1,7 трлн долл. Результаты исследования J’son & Partner Consulting показали, что российский рынок телекоммуникационных услуг растет большими темпами, чем мировой. В 2013-2015 годах рост составил 5%.

Одним из важных показателей технологического состояния развития сектора ИКТ является уровень использования протокола IP. В 2012 году был проведен семинар МСЭ для стран СНГ, на котором обсуждалась возможность перехода с протокола с IPv4 на IPv6 и проблемы, которые могут возникнуть в связи с этим. Был предложен сценарий перех ода на IPv6 в два этапа.

Первый этап: перевод всей сети на протокол IPv6 с сохранением формата адресации IPv4. На устройствах сети разворачивается стек IPv6, адреса устройств берутся не из пула Global Unicast Address, а формируются определенным образом на основе адресов IPv4. При передаче пакета из IPv4 в сеть IPv6 пакет и формат адреса преобразуются согласно алгоритму, без использования таблиц соответствия адресов.

Далее следует второй этап перехода на IPv6. После перевода всей сети на протокол IPv6 возможно использование других форматов адресов. Возможен плавный переход на иерархические адреса IPv6: в формате IPv6 адрес IPv4 позволяет создавать сети на своей основе, добавляя идентификатор интерфейса, благодаря чему адресное пространство значительно расширится. Нет необходимости в новых адресах IPv4.

Таким образом, операторам придется решать следующие проблемы:

- разработка плана миграции на новый протокол;
- полный аудит сетевой инфраструктуры;
- создание опытных зон для отработки новой технологии;
- замена или модернизация оборудования и систем OSS/BSS;
- отдельный бюджет на работу с абонентами:

  - на уведомления о переходе на новый протокол и разъяснения его преимуществ;

  - на разбор претензий и жалоб, а также на качественную техническую поддержку.

Кроме того, оператор может понести дополнительные затраты на стимулирование перехода абонентов на новый протокол и поддержание их лояльности.

По информации Технического центра Интернет, IPv6 в России развивается так же, как и в других странах мира, пока что ни одна из стран не может похвастаться полным переходом на IPv6.

И это вполне объяснимо – для внедрения IPv6 требуется смена оборудования, поэтому основной скачок произойдет в тот момент, когда большая часть используемого на сетях оборудования окажется физически и морально устаревшим и потребует замены.

Основная же российская проблема - малое число пользователей IPv6. И здесь необходимо продвижение этого протокола, решения, позволяющие обычному пользователю перейти на IPv6 практически незаметно для себя. По мнению многих экспертов, в ближайшие три года следует ожидать серьезного роста числа конечных пользователей, подключенных по IPv6: примерно 50% пользователей к 2017 году.

Относительно использования стандарта 4G - по состоянию на первый квартал 2015 года, скорость 4G-сетей в России выше, чем в Японии на 11,1% и на целых 42,9% выше, чем в США.

В апреле 2016 года состоялась Расширенная коллегия Министерства связи и массовых коммуникаций Российской Федерации (http://www.minsvyaz.ru/ru/events/35024/). В выступлении Министра связи и массовых коммуникаций РФ господина Н.А.Никифорова были представлены основные показатели развития отрасли и намечены планы её развития.

В частности, были подробно рассмотрены наиболее приоритетные задачи, которые проистекают из принятых нормативных актов, федеральных законов, отдельных поручений Президента, Правительства, над которыми работает Минкомсвязи России вместе с коллегами в регионах. При этом основным программным документом является государственная программа «Информационное общество». Ответственным исполнителем госпрограммы является инкомсвязи России. Главная цель программы — обеспечить гражданам, организациям такой высокий уровень функционирования информационных и телекоммуникационных технологий, чтобы были созданы условия для эффективного взаимодействия между гражданами, государством и за счет этого обеспечивался необходимый экономический рост и качество жизни.

В 2015 году было продолжено выполнение основных задач по развитию услуг широкополосного доступа в интернет, по реформе универсальных услуг связи, устранению цифрового неравенства и реализации отдельных проектов, связанных с оптимизацией регулирования в этой сфере.

Уровень проникновения мобильного интернета в России на сегодняшний день превышает уровень проникновения проводного широкополосного доступа в интернет. Доступность услуг

проводного ШПД достигла 66,7%. При этом современная технология связи мобильного интернета LTE уже доступна на территории, где проживает 60% населения страны.

В 2015 году была продолжена реформа универсальных услуг связи. Ее цель — устранить цифровое неравенство. Продолжается строительство волоконно-оптических линий связи. Всего предстоит построить 215 тысяч километров, это около 14 тысяч точек доступа в конкретных населенных пунктах. Речь идет о селах с населением 250–500 жителей, где интернета раньше либо не было вообще, либо он предоставлялся по такой технологии, на такой скорости и по такой цене, что фактически делало его недоступным.

Планируется по пути в села с населением от 250 до 500 жителей заходить и в другие населенные пункты. Много населенных пунктов еще не подключено по оптике в диапазоне от 500 до 10 000 жителей. Суммарно потенциальный охват этой программы достигает 37 млн человек.

Рабочая поддержка и реализация программы осуществляются силами компании с государственным участием ПАО «Ростелеком», которая была определена оператором по данной программе отдельным решением Правительства. Эта компания сегодня реализует проект во многом за счет собственных средств. Объективные бюджетные ограничения приводят к тому, что фонд универсального обслуживания недополучает финансирование. Минкомсвязи России продолжает последовательную политику в отношении того, что средства фонда универсального обслуживания должны целевым образом использоваться исключительно на реализацию ранее поставленных задач.

На конец марта 2016 года удалось подключить уже около 2100 населенных пунктов, которые расположены в 65 субъектах РФ. География этой работы охватывает почти всю территорию России.

Минкомсвязи России удалось утвердить, это было прямо предусмотрено нормативной базой, специальный льготный социальный тариф — стоимость доступа в интернет на скорости 10 Мбит/с составляет 45 рублей в месяц.

При развитии связи на Дальнем Востоке компания ПАО «Ростелеком» действует в рамках собственного инвестпроекта и реализует прокладку волоконно-оптической линии связи от Сахалина до Магадана. Эта стройка фактически завершена, идет сдача-приемка данной линии связи.

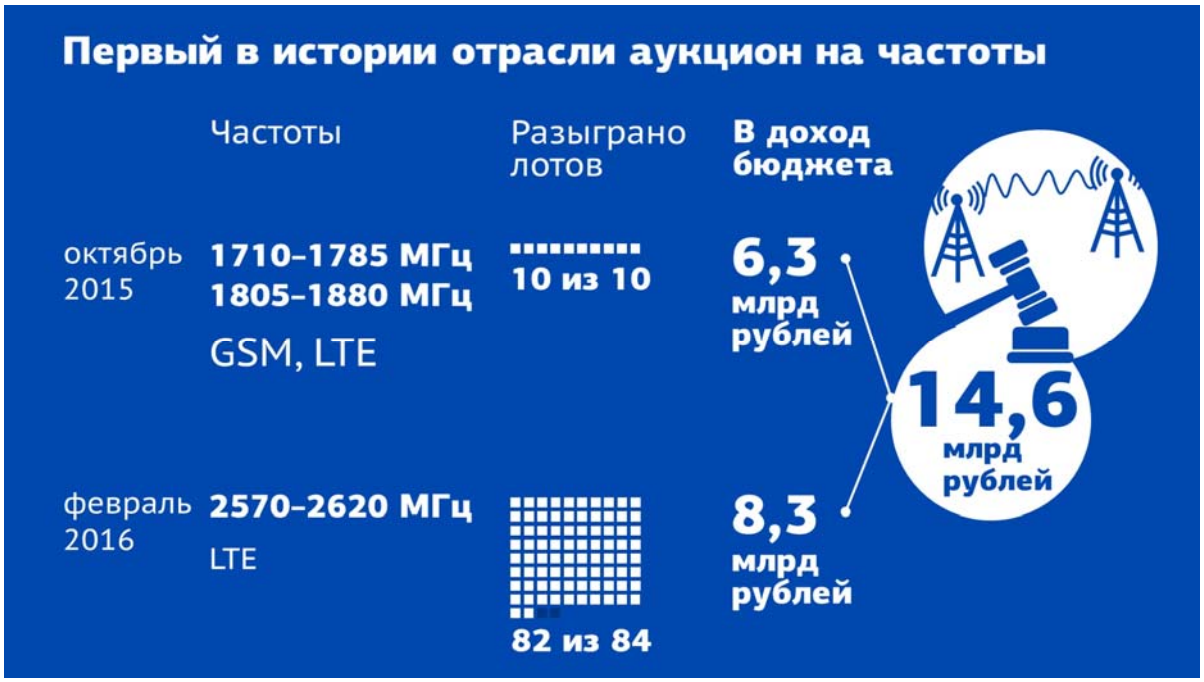
Летом 2016 года планируется осуществить прокладку маршрута ВОЛС до Камчатки. Подписано отдельное соглашение между Минкомсвязью России и Чукоткой.

Очевидно, что территория России обязывает Минкомсвязи России использовать и тот космический потенциал, который есть у нашей страны. Спутники позволяют получить интернет там, куда никогда не дойдет ВОЛС, но подключение крупных городов по оптике высвобождает значительный спутниковый ресурс.

В 2015 году была продолжена программа пусков спутников связи. Суммарно сегодня это 17 аппаратов, из них основная часть находится в ведении ФГУП «Космическая связь», также есть четыре космических аппарата у компании «Газпром космические системы».

Ключевыми новеллами в законодательстве, регулирующими использование радиочастотного спектра являются следующие. Первое и очень важное — это совместное использование радиочастот. В крупных городах существует высокая готовность инфраструктуры, высокий уровень конкуренции, но когда речь заходит о небольших населенных пунктах, о протяженных автодорогах, которые тоже нужно обеспечивать связью, то здесь необходимо операторам объединять свои усилия, в том числе объединять возможности по использованию радиочастот. Такие нововведения в 2015 году вступили в силу. Операторы связи, которым ранее были выделены полосы радиочастот, получили возможность их совместного использования в диапазоне от 800 МГц до 2,5 ГГц.

В конце 2015 года в Российской Федерации впервые состоялся аукцион на право использования радиочастот. Уже прошло два таких аукциона — один из них прошел в 2016 году, суммарно удалось выручить в доход федерального бюджета почти 15 млрд. рублей.

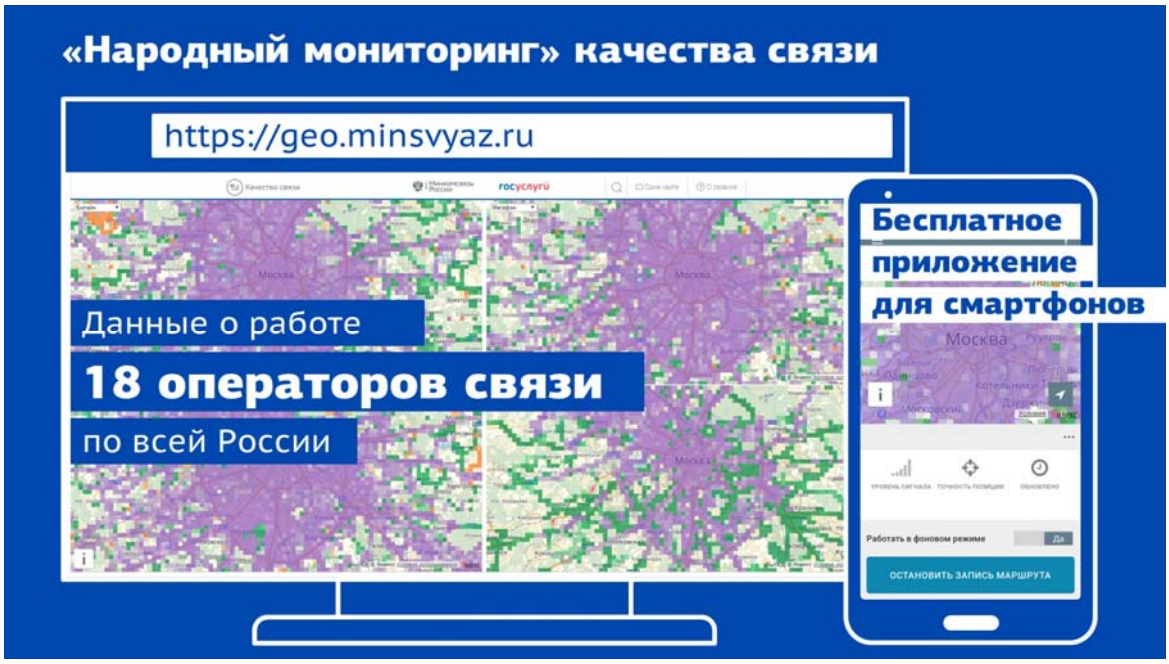


В настоящее время в Российской Федерации активно внедряется технология LTE — связи четвертого поколения. В 2015 году был зафиксирован существенный рост количества базовых станций стандарта LTE — на 77% относительно 2014 года. Количество базовых станций превысило 70 тысяч.

Отрасль связи Российской Федерации занимает достостойное место среди таких отраслей-лидеров по объему оказания платных услуг населению, как, к примеру, сфера ЖКХ или транспорт. Увеличился объем услуг связи до 1,7 трлн. рублей.

В Российской Федерации внедрена услуга переносимости мобильного номера. Более 3 млн. абонентов фактически перешли от одного оператора к другому, сохранив за собой свой мобильный номер.

В настоящее время запущена программа публичный «народный мониторинг» качества связи. Роскомнадзор осуществляет активный мониторинг, публикуется целый ряд отчетов. Упомянутый «народный мониторинг» доступен для всех, это открытые публичные данные по адресу geo.minsvyaz.ru, где любой желающий может принять участие и замерить связь в тех местах, где он живет, перемещается, работает, учится.



Отметим, что средняя скорость соединения в Российской Федерации по широкополосному доступу превысила показатели таки стран как, к примеру, Франция, Италии и целого ряда других государства. Это данные Всемирного Банка. Остается лишь добавить такой любопытный пример, что суммарное количество подключенных в Российской Федерации абонентов оптоволоконных линий связи превысило этот показатель во всех странах ЕС вместе взятых.

В 2014 году Минкомсвязи России утвердило план импортозамещения по программному обеспечению, в нем три направления. Первый блок продуктов, связанных с мерами поддержки в виде преференций при госзакупках — это реестр российского программного обеспечения. Второй блок работы — субсидирование части затрат на поддержку системного ПО. Третий блок работы — отраслевые прикладные программные продукты, где нужно идти по принципу коммерциализации. Минкомсвязи России внесло предложение в план устойчивого развития экономики, который был утвержден 1 марта 2016 года Председателем Правительства РФ, по выделению отдельной строчки, отдельного мероприятия по поддержке разработки, развития и распространения российского программного обеспечения. Сегодня ни для кого не секрет, что конкурентоспособность и информационный суверенитет государства и государств-партнеров Российской Федерации крайне зависим от состояния программного обеспечения и обладания Российской Федерацией всем набором технологий и компетенций в этой сфере.

С 1 января 2016 года вступила эта законодательная инициатива по созданию реестр отечественного ПО. Сегодня в реестр включено свыше 1000 программных продуктов. Продукты включает специальный Экспертный совет по российскому ПО при Минкомсвзяи России.

В 2015 году Российская Федерация была председателем блока БРИКС, что позволило Минкомсвязи России активно продвигать тему вопросов информационной безопасности, информационного суверенитета, диверсификации глобального ИТ-рынка, ухода интернет-монополии. БРИКС - это фактически половина населения нашей планеты, а соответственно, в перспективе, это половина рынка инфокоммуникационных услуг.

Республика Таджикистан

По состоянию на конец 2015 года рейтинг страны по атакам DDoS, зафиксированных компанией Akamai составляет 162 место из 251.

Каждый раз, когда бот используется в атаке DDoS против клиента Akamai, IP-адрес бота и расположение записываются и отслеживаются.

Статистика за 24 часа по данному виду атак для Республики Таджикестан отсутствует. Из этих двух показателей следует, что Таджикистан находится почти в наилучшем положении и не является самой частой мишенью для DDoS-атак.

В настоящее время в Республике Таджикистан полностью отсутствует внедрение протокола IPv6, поскольку нет потребности в его использовании.

Стоимость и доступность услуг остаются решающим фактором в области ИКТ в Таджикистане.

Республика Таджикистан совместно с Республикой Кыргызстан являются единственными странами СНГ, в которых предоплата за мобильный широкополосный доступ (далее МШПД) в Интернет составляет более 5 % ВНД (валовой национальный доход на душу населения).

Цены являются наименее доступными в Таджикистане, который тоже включен в страны СНГ в сравнении с низким уровнем проникновения мобильной широкополосной связи.

По ценам за МШПД, пост-оплата за услуги на мобильной основе за 500 Мб, 2014 г., Таджикистан занимает 144 место. По ценам за МШПД, пред-оплата за услуги на мобильной основе за 500 Мб, 2014 г., Таджикистан занимает 149 место. По ценам за МШПД, пост-оплата за услуги компьютерных сетей за 1 Гб, 2014 г., Таджикистан занимает 134 место. По ценам за МШПД, пред-оплата за услуги компьютерных сетей за 1 Гб, 2014 г., Таджикистан занимает 129 место.

Предварительная инвентаризация информационного потенциала министерств и ведомств Республики Таджикистан, проведенная в 2014 году, выявила, что сотрудники центральных аппаратов следующих министерств и ведомств обеспечены персональной компьютерной, техникой:

- Национальный банк Таджикистана, Министерство финансов Республики Таджикистан, Агентство государственной службы при Президенте Республики Таджикистан, Налоговый комитет при Правительстве Республики Таджикистан, Таможенная служба при Правительстве Республики Таджикистан, Агентство по социальной защите и пенсиям при Правительстве РТ, АОХК «Барки Точик» - на 100%;
- Министерство здравоохранения и социальной защиты населения Республики Таджикистан - на 95%;
- Министерства внутренних дел, транспорта и Государственный комитет по инвестициям и управлению государственным имуществом Республики Таджикистан на 90%;
- другие министерства и ведомства, где проведена инвентаризация, - от 60 до 85%.

Существующая в стране техническая инфраструктура информационно-коммуникационных технологий государственных органов характеризируется следующими параметрами:

- недостаточное обеспечение сотрудников современной компьютерной техникой;
- использование устаревшей компьютерной техники не соответствует требованиям современных информационных систем;
- недостаточное оснащение специализированными серверными помещениями или их полное отсутствие;
- нехватка или отсутствие серверного или сетевого оборудования; - отсутствие локально-вычислительных сетей;
- низкое качество и высокая стоимость Интернет-услуг, предоставляемых Интернет-провайдерами;
- отсутствие инфраструктуры обслуживания специализированного серверного и сетевого оборудования, а также отсутствие технической базы обслуживания информационно-коммуникационных технологий.

На данный момент некоторые министерства и ведомства осуществляют обмен данными, применяя различные, носящие частный характер, методы передачи-обмена данных. Зачастую обмен данными носит асинхронный характер, т.е. ведомства одним методом отправляют данные и совершенно другим методом получает данные из других ведомств.

При этом не имеется общего согласованного правила обмена данными, в связи с чем происходит дублирование функций и затрат при передаче одной и той же информации различным ведомствам.

В целом ситуация по обмену данными между государственными органами Республики Таджикистан требует улучшения.

Отсутствие действующей единой сети, связывающей органы исполнительной власти (созданная в 2010 году техническая инфраструктура в настоящее время не может быть использована для обмена информацией), отсутствие единого центра обработки данных и единого телекоммуникационного данных делает затруднительным консолидацию данных, усложняет процесс обмена информацией.

Наблюдается несовместимость применяемых различными государственными органами программно-технических решений.

Используемые государственные информационные системы формировались отдельными органами государственной власти в условиях отсутствия единой нормативной правовой базы, регламентирующей эти процессы, и общей координации.

Содержащиеся в них базы данных зачастую недоступны для оперативного использования другими органами государственной власти, что на практике приводит к значительным временным задержкам при обмене информацией на межведомственном уровне, ее многократному сбору и дублированию в отдельных системах.

В результате такие информационные системы содержат сведения разной степени актуальности и достоверности. При этом часть информации оперативно не обновляется, что приводит также к несогласованности и противоречивости содержащихся в них данных.

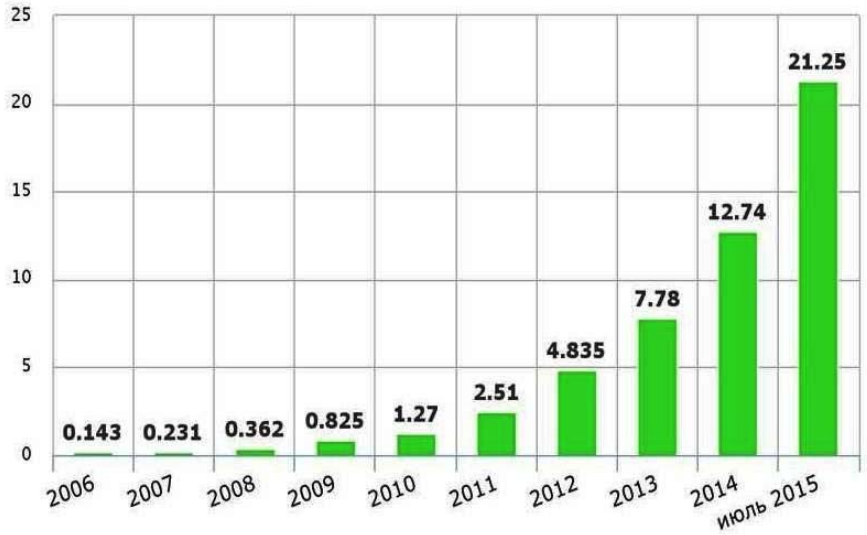
Различные форматы хранения данных ограничивают возможность применения автоматизированных средств поиска и аналитической обработки информации, содержащейся в различных системах.

Все это снижает оперативность и качество управленческих решений, подготавливаемых и принимаемых государственными органами.

Республика Узбекистан

За первые 9 месяцев 2015 года предприятиями сферы связи, информатизации и телекоммуникационных технологий Республики Узбекистан оказано услуг на 85 млрд. рублей (рост по сравнению с аналогичным периодом 2014 года составил 16,4%), в том числе населению оказаны услуги на 59.5 млрд. рублей (рост – 17,5%).

Общая скорость пользования международными информационными сетями возросла на 27,7% по сравнению с началом 2015 года и составила 21,25 Гбит/с.



Скорость доступа к международным информационным сетям (Интернет) (Гбит/с)

Количество портов, установленных для оказания услуг фиксированного широкополосного доступа к сети Интернет, доведено до 716,9 тысяч, а количество используемых портов возросло на 21,5%. Рост этих показателей позволит оказывать широкополосные мультисервисные услуги (IPTV, видеотелефония, высокоскоростной Интернет, передача данных, возможность просмотра каналов HDTV и т.д.) широким слоям населения страны.

В стране осуществляется поэтапный переход на цифровое телевизионное вещание, в настоящее время уровень охвата населения цифровым телевещанием доведен до 54%. До конца 2015 года запланирована установка 19 передатчиков цифрового телевидения и доведение охвата до 70%.

Тариф для операторов и провайдеров сети Интернет, подключаемых к Международному центру пакетной коммутации, снижен до 202,9 долл. США за 1 Мбит/с, что на 21,75 % меньше по сравнению с началом 2015 года, а по сравнению с аналогичным периодом 2014 года на 33,1 %.

Государственная инспекция по надзору в сфере связи, информатизации и телекоммуникационных технологий Республики Узбекистан провела анализ качества оказания услуг операторами мобильной связи Узбекистана: ИП ООО «COSCOM», АК «Узбектелеком», ИП ООО «RWC» и ООО «UNITEL».

Согласно анализу, вышеуказанные операторы мобильной связи допускают нарушения требований Закона Республики Узбекистан «О телекоммуникациях», в частности абзац 3 статьи 22, в частности не обеспечивается качество оказываемых услуг в соответствии с установленными стандартами, правилами и нормами.

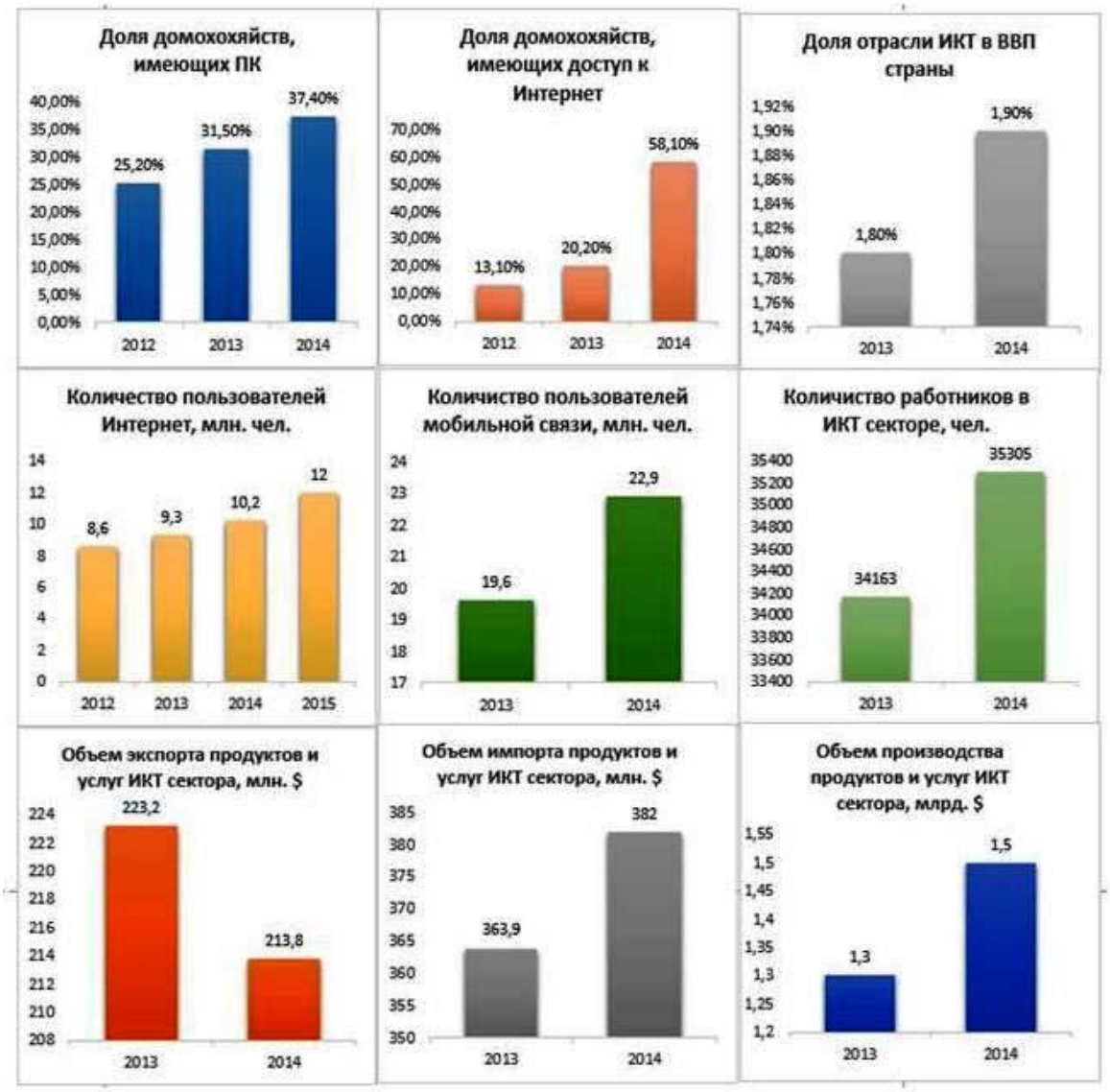
В связи с этим, а также по результатам анализа поступивших жалоб от абонентов мобильной связи, были даны поручения операторам мобильной связи: ИП ООО «COSCOM», АК «Узбектелеком», ИП ООО «RWC», ООО «UNITEL» с требованием выработать план мероприятий по улучшению качества мобильной связи в соответствии с требованиями законодательства.

Руководство страны четко обозначило, что стабильное и полноценное развитие национальной экономики Узбекистана невозможно без внедрения и использования информационно-коммуникационных технологий в различных сферах социально-экономической жизни общества и развития экономики, которые являются одним из основных локомотивов экономических преобразований любой страны мира.

На саммите по информационно-коммуникационным технологиям – ICT SUMMIT 2015 были приведены основные показатели развития ИКТ в республике («О состоянии и перспективах развития ИКТ в Узбекистане»):

- доля домашних хозяйств, имеющих компьютеры, достигла 37,4%;
- доля домашних хозяйств, имеющих доступ к сети Интернет, — 58,1%;
- доля отрасли ИКТ в ВВП страны составила 1,9%;
- количество пользователей Интернета превысило 12 млн., из них число пользователей мобильного Интернета составило 11,2 млн.

Если остановиться на экономических показателях развития отрасли, то можно отметить, что объем производства товаров и услуг в сфере ИКТ превысил $1,5 млрд. долларов США, а экспорт составил более 213 млн. долларов США.



Основные индикаторы ИКТ в Республике Узбекистан

Развитая телекоммуникационная инфраструктура является ключевым фактором масштабного внедрения ИКТ. С 2012 года в этом направлении принят ряд государственных программ, в частности:

- Постановлением Президента Республики Узбекистан от 17.04.2012 г. утверждена Программа по техническому и технологическому переходу на цифровое телевидение в Республике Узбекистан. По результатам реализованных проектов на сегодняшний день эксплуатируются 22 передатчика цифрового телевидения. Охват населения цифровым телевидением составляет 54,3%.
- Постановлением Президента Республики Узбекистан от 27.07.2013 г. утверждена Программа развития телекоммуникационных технологий, сетей и инфраструктуры связи в Республике Узбекистан на 2013–2020 годы. Реализация программы даст возможность увеличению скорости передачи данных и Интернета до областей — в 4 раза, до районов — в 10 раз.
- Постановлением Президента Республики Узбекистан от 06.03.2015 г. утверждена Адресная программа развития информационно-коммуникационных технологий на 2015–2019 годы, предусматривающая построение центров хранения и обработки данных, расширение сетей широкополосного доступа, а также развитие сетей мобильной 4G LTE.

В настоящее время развитие телекоммуникационных технологий, сетей и инфраструктуры связи страны ведется путем расширения сетей фиксированного и мобильного широкополосного доступа, расширение центров коммутации передачи данных и голосового трафика, модернизации и расширения магистральных телекоммуникационных сетей, а также создания инфраструктуры для развития мультимедийных услуг.

На сегодняшний день общая скорость пользования международными информационными сетями возросла на 42,3% по сравнению с началом 2014 года и составила 15,5 Гбит/с.

Тариф для операторов и провайдеров сети Интернет, подключаемых к Международному центру пакетной коммутации, снижен до 276,27 долл. США за 1 Мбит/с, что на 11,6% меньше по сравнению с началом 2014 года.

Осуществлено строительство более 2000 км волоконно-оптических линий связи для широкополосного доступа по современным технологиям на участках «Бузатау–Кунград», «Гузар–Байсун», «Денау–Узун–Шаргун», «Жаслик–Каракалпакстан», «Муйнак–Кибла Устюрт», «Узун–граница Таджикистана» с предоставлением конвергентных услуг, таких как видеотелефония, интернет-телевидение, высокоскоростной Интернет, просмотр HDTV-каналов и другие. Количество портов, установленных для оказания услуг фиксированного широкополосного доступа к сети Интернет, доведено до 640 тыс., а количество используемых портов возросло на 135,1%.

Реализация указанных проектов также способствует развитию беспроводной связи. На сегодняшний день операторы мобильной связи внедряют сети четвертого поколения 4G LTE, что позволит пользователям быстро и эффективно работать с большим объемом информации в Интернете, загружать и просматривать потоковое видео, загружать фотографии высокого качества, а также пользоваться онлайн-приложениями в образовательных целях и для бизнеса. Все эти технологии с точки зрения мобильности позволяют интернет-пользователям Узбекистана расширить свои привычные возможности работы с ИКТ.

Особое значение придается развитию мобильной связи в Узбекистане. Проводится работа по последовательному развитию сетей мобильной связи на основе технологии передачи голоса (2G GSM), данных (3G UMTS) и высокоскоростной передачи данных (4G LTE) в городе Ташкенте, в областных центрах и остальных населенных пунктах Республики.

В целях экстренного реагирования на запросы пользователей по информационно-коммуникационным услугам во всех регионах страны были созданы 13 колл-центров в рамках проекта внедрения Единого центра обслуживания вызовов АК «Узбектелеком», а также для нужд государственных органов и хозяйствующих субъектов. Эти меры служат повышению качества оказываемых телефонных и интернет-услуг на более высокий уровень.

Ведется постепенная модернизация местных телефонных сетей на основе технологий следующего поколения. В течение текущего года по всей Республике были запущены в эксплуатацию 26 единиц современного коммутационного оборудования, что значительно увеличивает емкость телефонных номеров.

Согласно Постановлению главы государства «О мерах по реализации инвестиционных проектов развития и модернизации телекоммуникационной сети Республики Узбекистан с участием Государственного банка развития Китая» от 2 декабря 2014 года осуществляются проекты по развитию телекоммуникационной инфраструктуры на общую сумму 117,6 млн. долларов США, в т. ч. за счет кредитных средств, выделенных Государственным банком развития Китая (КНР) на сумму 100,0 млн. долларов США. Эти проекты нацелены на расширение пропускной способности магистральных сетей передачи данных: по международному направлению — в 10 раз (до 100 Гбит/сек), до областных центров — в 4 раза (до 40 Гбит/сек) и райцентров — в 10 раз (до 10 Гбит/сек).

В рамках выполнения данного постановления также предусмотрено развитие оптических сетей широкополосного доступа по технологии FTTx контрактной стоимостью 6,9 млн. долларов США, направленного на модернизацию абонентских линий связи г. Ташкента с установкой оборудования передачи данных широкополосного доступа на 69 120 портов.

Реализуется программа развития сетей широкополосного доступа по технологии Wi-Fi в Республике Узбекистан на период 2014–2015 годы, направленная на создание возможности определить стратегические направления развития инфраструктуры беспроводных сетей широкополосного доступа по технологии Wi-Fi. Целью этой Программы является создание в каждом регионе Республике, в том числе в аэропортах, вокзалах, в местах частого пребывания туристов, парках, торговых центрах и других общественных местах широкополосного беспроводного доступа по технологии Wi-Fi.

Продолжается работа по внедрению современных телекоммуникационных технологий в сферу телевидения согласно Постановлению Президента страны «О Государственной программе по техническому и технологическому переходу на цифровое телевещание в Республике Узбекистан». В рамках Программы переход на цифровое телевизионное вещание в стране осуществляется в два этапа: первый охватывает 2013–2015 годы, второй — 2016–2017 годы.

В конце первого этапа госпрограммы должны быть установлены 84 передатчика высокой мощности, которые позволят охватить цифровым телевизионным вещанием все крупные населенные пункты страны и 90% населения. На сегодняшний день доступом к цифровому телевидению обеспечены около 54 процентов населения Узбекистана: жители города Ташкента и

большинства районов Ташкентской, Самаркандской, Хорезмской, Бухарской, Андижанской, Наманганской, Ферганской, Навоийской, Кашкадарьинской областей, а также Республики Каракалпакстан. Они имеют возможность смотреть цифровые телепрограммы с высоким качеством изображения.

Параллельно, развивая телекоммуникационную инфраструктуру страны, ведется работа по внедрению современных ИКТ путем создания информационных систем и информационных ресурсов, которые должны действовать в телекоммуникационных сетях.

Индекс развития ИКТ в Узбекистане (ICT Development Index) по состоянию на 2014 год составляет 3,4. В 2015 году Узбекистан не был включен в рейтинг.

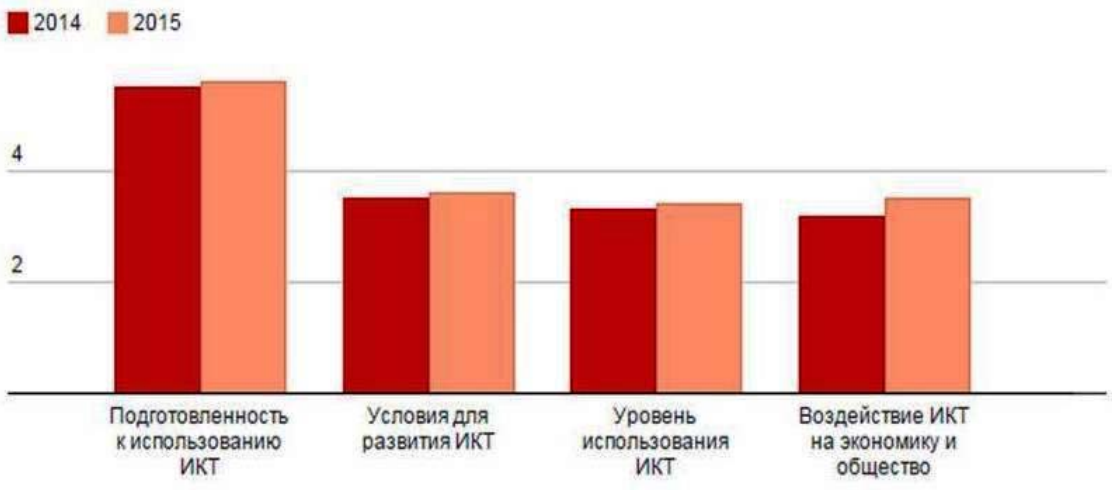
Также Узбекистан занимает 114 место по показателю уровня развития Интернета. Этот показатель характеризует число пользователей Интернета на 100 человек в стране, является одним из базовых в оценке общего уровня развития информационно-коммуникационных технологий.

Украина

По уровню развития информационно-коммуникационных технологий в 2015 году Украина оказалась на 71 месте среди 143 государств. Таким образом, за последний год Украине удалось подняться сразу на десять позиций мирового списка (в 2014 г. – 81 место среди 148 стран). Об этом говорят данные ежегодного отчета «Global Information Technology Report 2015», подготовленного Всемирным экономическим форумом (ВЭФ) совместно с международной бизнес-школой INSEAD и Высшей школой управления имени Сэмюэла Кертиса Джонсона при Корнельском университете. Информацией для анализа послужили данные Всемирного банка, Международного союза электросвязи, ЮНЕСКО и других специальных учреждений ООН.

По сравнению с 2014 г. итоговое значение индекса сетевой готовности Украины выросло на 0,14 балла – до 4,01.

За последний год Украина продемонстрировала рост показателей по всем компонентам индекса, а наибольшего прогресса добилась в сфере вовлеченности ИКТ в экономическую и общественную среду (+0,3 балла).



Изменение значений Украины по компонентам индекса сетевой готовности

Однако уровень развития ИКТ на Украине ещё недостаточно высок. В списке 12 бывших республик СССР, охваченных исследованием, в 2015 г. Украина оставила позади себя только Киргизию (3,54) и Таджикистан (3,20). Лучшей среди постсоветских государств оказалась Эстония (5,34), занявшая 22 место мирового списка.

По оценкам экспертов, самыми сильными сторонами Укпаины в области ИКТ являются их доступность (6,6) и навыки пользования ими (5,6). По этим показателям Украина расположилась на 10 и 46 местах глобального рейтинга соответственно. В то же время она обладает одними из худших значений по уровню благоприятности политической и регуляторной сфер, а также эффективности использования ИКТ государственными структурами (122-я и 124-я позиция соответственно.

На 12-м Всемирном телекоммуникационном симпозиуме (ноябрь 2014 г., Тбилиси, Грузия) был представлен ежегодный отчет Международного союза электросвязи (МСЭ) «Оценка информационного общества 2014» (Measuring the Information Society Report 2014). Ключевой показатель развития как ИКТ, так и информационного общества — интегральный показатель “Индекс развития ИКТ” (ICT Development Index, IDI).

Согласно отчету, Украина в рейтинге занимает 73-ю позицию. За период проведения измерений, начиная с 2007 г., Украина потеряла 15 позиций. Это показывает тотальное техническое и технологическое отставание. Реальной становится угроза выпасть из списка Топ-100 наиболее развитых стран мира.

По состоянию на 2015 год на Украине наиболее распространены следующие мобильные операторы: Киевстар, МТС, Life:), Укртелеком, Интертелеком.

Кратко остановимся на показателях покрытия данных операторов, а также оценке средней скорости передачи данных.

Компания «Киевстар» - наиболее популярный мобильный оператор Украины, на 100% принадлежит компании VimpelCom Ltd. По состоянию на 2013 год оператор имеет 27 миллионов абонентов, что составляет почти половину рынка мобильной связи. 23 февраля 2015 года Киевстар получил лицензию на радиочастоты 3G по технологии UMTS-2100. По условиям договора, в течении 18 месяцев Киевстар должен охватить все районные центры технологией 3G.

В настоящее время национальный мобильный оператор «Киевстар» покрывает сетью GSM (2G) территорию Украины, где проживает 99 % населения Украины. Своей сетью «Киевстар» охватывает все крупные и малые города и свыше 28 тыс. сельских населенных пунктов, все основные национальные и региональные трассы, большинство морских и речных побережий Украины. По данным Ericsson сеть «Киевстар» по большинству параметров входит в 25% лучших мировых сетей. Сеть 3G работает в 365 городах.

Абонентская база компании МТС Украины на конец февраля 2013 составляла 20,601 млн. абонентов. 23 февраля 2015 компания «МТС Украина» получила лицензии на связь в стандарте UMTS (3G) в полосах радиочастот 1950—1965/2140-2155. Сеть МТС покрывает более 98% территории Украины, на которой проживает 99% населения.

Третий по популярности мобильный оператор Украины – компания «*Life*:)» имеет более 8 миллионов абонентов. Компания «Life:)» имеет уверенное 2G покрытие по всей стране(98.6%), однако, 3G распространён лишь в некоторых густонаселённых областях.

Компания «Укртелеком» - одна из крупнейших компаний Украины, предоставляющая полный спектр телекоммуникационных услуг во всех регионах страны. Особенно сильные позиции общество имеет на рынке услуг доступа к сети Интернет и фиксированной телефонии.

Компания «Интертелеком» - национальный 3G оператор, предоставляющий услуги мобильной и фиксированной связи по технологии CDMA, а также безлимитный 3G интернет на скорости до 14,7 Мбит/с. В настоящее время компания «Интертелеком» имеет самое широкое 3G покрытие на Украине.

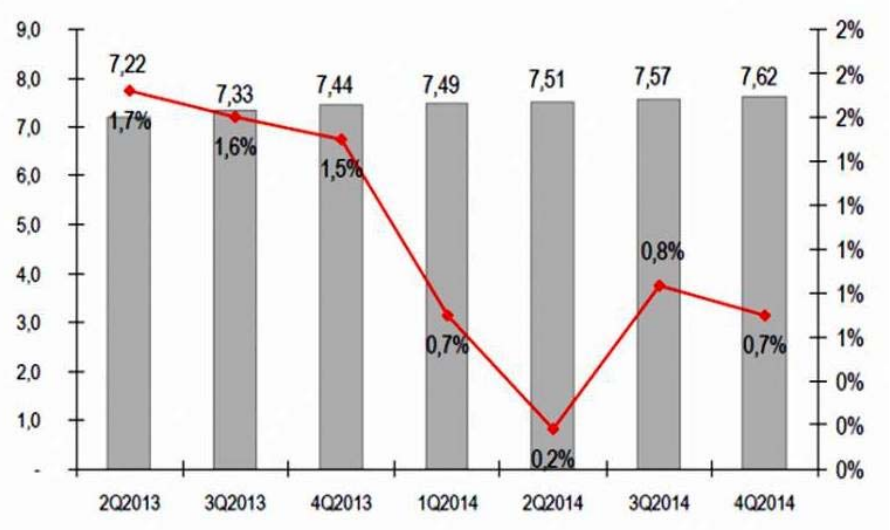
Несмотря на слабое покрытие 3G многих операторов сотовой связи Украины, согласно отчёту компании Akamai мобильная связь Украины в 2014 году имела наивысшую среднюю скорость передачи данных, составляющую 7.3 Мб/с.

Стандарт LTE в настоящее время практически не представлен на Украине. Это объяснимо тем, что с рыночной точки зрения, LTE не даст сразу того возврата инвестиций, на который рассчитывают операторы: маленький процент устройств, поддерживающих эту технологию сейчас у клиентов на руках. А снижение покупательской способности не дает возможности людям сменить текущее устройство на новое, более дорогое, с поддержкой LTE.

Рейтинг интернет-провайдеров Украины (фиксированного широкополосного доступа) по итогам 1-го квартала 2015 года выглядит следующим образом (по количеству абонентов).

Позиция	Оператор	I кв. 2015 (тыс. аб.)
1	ПАО «Укртелеком»	1 622,7
2	ГК «Киевстар»	847,8
3	ГК «Воля»	601,1
4	ГК «Триолан»	285,0
5	ГК «Фрегат»	233,0
6	ЧАО «Датагруп»	221,5
7	ООО «НПП «Тенет»	159,4
8	ГК «Вега»	149,0
9	ГК «Ланет»	128,7
10	ООО «Фринет»	112,5

Источник www.encint.com



Динамика роста числа пользователей и снижения доходов ШПД на Украине

Среди стран СНГ Украина занимает 4-ое место по проникновению ШПД в домашние хозяйства.

3. Развитие государственных услуг в электронном виде

Республика Азербайджан

Все государственные услуги в Республике Азербайджан будут предоставляться в электронном формате до 2020 года. Планируется принять новую государственную программу по развитию сферы информационно-коммуникационных технологий, одним из основных направлений которой станет увеличение числа предоставляемых гражданам электронных услуг. В настоящее время это число составляет примерно 400 услуг от 45 государственных структур.

Программа разработана Минсвязи Азербайджана, рассчитана на период 2015-2016 годов и будет работать в рамках «Национальной стратегии по развитию информационного общества в Азербайджане на 2014-2020 годы».

Часть услуг станет доступной на платформе мобильных устройств, при помощи мобильных приложений. В настоящее время уже оказывается ряд услуг с использованием мобильных платформ. В Минсвязи Азербайджана рассматривают вопрос использования так называемой платформы SmartGov, благодаря которой население сможет выполнять некоторые функции по управлению страной вместе с властями.

В настоящее время Министерство Связи Азербайджана активно работает над проектом «Электронное правительство» («Э-правительство»).

Проект «Э-правительство» разработан на основании «Национальной стратегии по информационно-коммуникационным технологиям во имя развития Азербайджанской Республики (2003-2012 гг.)» и осуществляется в рамках Государственной программы «Электронный Азербайджан». Путем широкого внедрения информационно-коммуникационных технологий, проект предусматривает повышение эффективности деятельности государственных органов, упрощение взаимосвязей между населением, бизнесом и ведомствами, выведение на качественно новый уровень отношений между чиновниками и гражданами, обеспечение прозрачности и полное удовлетворение информационного спроса.

Цели проекта:

- Совершенствование методов и механизмов управления путем расширения использования современных информационно-коммуникационных технологий в государственных органах;
- Повышение рациональности деятельности государственных органов, обеспечение прозрачности;
- Создание условий для участия граждан в принятии общественных решений и осуществление взаимодействия с государственными органами посредством более упрощенных и доступных электронных средств.

Основные направления реализации проекта:

- Формирование нормативно-правовой базы, регулирующей деятельность э-правительства и его граждан;

- Расширение форм применения современных технологий в государственном управлении;
- Создание основных компонентов инфраструктуры э-правительства;
- Внедрение и развитие э-услуг в соответствии с принципом «единого окна»;
- Повышение уровня готовности государственных служащих и специалистов по ИКТ;
- Обеспечение безопасности инфраструктуры э-правительства и деятельности информационных систем, а также защиты персональных данных;
- Повышение уровня компьютерной грамотности групп населения и обеспечение доступа к услугам э-правительства.
- Основные компоненты инфраструктуры э-правительства:
- Единая сетевая инфраструктура государственных органов;
- Портал э-правительства;
- Шлюз э-правительства;
- Государственный реестр информационных ресурсов и систем;
- Национальная инфраструктура э-подписи
- Национальная инфраструктура э-документа (в стадии разработки)
- База данных э-правительства (data-center) (в стадии разработки)

Основные преимущества проекта:

Для правительства:

- Повышение рациональности деятельности государственных органов путем широкого применения современных технологий;
- Сокращение бюджетных расходов, повышение оперативности и эффективности оказания государственных услуг;
- Формирование единого информационного пространства государственных органов и обеспечение ее безопасности;
- Создание эффективного, прозрачного, контролируемого государственного управления и местного самоуправления.

Для граждан:

- Активное участие граждан в государственном управлении;
- Упрощение взаимосвязи между гражданами и государственными органами, осуществление этой связи в более доступной и оперативной форме;
- Удобство в удовлетворении информационной потребности;
- Предоставление доступа к государственным услугам для людей с ограниченными возможностями.

Для бизнес – сектора:

- Рациональное и оперативное налаживание связей с государственными органами, снижение расходов;
- Повышение экономической активности, конкурентоспособности и возможностей доступа к внешним рынкам;
- Выплаты в социальные фонды
- Э-декларация, э-налоговая счет-фактура
- Регистрация новых компаний
- Таможенные декларации
- Э-лицензия
- Э-закупки, э-котировки
- Э-аукцион
- Выдача справок и т.д.

Для граждан:

- Подоходный налог;
- Поиск работы (вакансии в предприятиях);
- Выдача документов (паспорт и водительские права);
- Акты регистрации гражданского состояния (рождение, смерть, заключение брака);
- Регистрация автомобилей;
- «Онлайн» заявление (вступление в вузы, получение разрешения на строительство, пенсия, пособии и др.);
- Регистрация на месте жительства;
- Медицинские услуги (э-консультация) и др.

С января 2013 года подготавливаются ежемесячные бюллетени о ходе проекта. Бюллетень предоставляет информацию об осуществленных и планируемых работах по формированию электронного правительства, данных о проектах электронного правительства, в том числе количестве электронных услуг и их использовании, сравнительной статистики и др.

В ноябре 2015 года был расширен перечень услуг электронного правительства. По данным Информационно-вычислительного центра Министерства связи и высоких технологий Азербайджана (ИВЦ) в портал «Электронное правительство» (e-gov.az) Азербайджана интегрирована новая система идентификации, позволяющая гражданам получать выписки по оплате услуг стационарной связи (голосовые услуги, услуги интернета, фиксированной телефонии и т.д.). Интеграция новой системы стала возможной после усовершенствования подсистемы единого электронного обращения и назначения (VEMTAS) Министерства труда и социальной защиты населения. В будущем одним из критериев оценки нуждающихся в адресной социальной помощи станут их затраты на услуги мобильной и стационарной связи.

Информационный обмен, который налажен между ИВЦ и Минтруда, позволит ведомству получать информацию о текущей и годовой задолженности абонента, проверять его задолженность и расходы по его другим Sim-картам.

Портал «Электронное правительство» является ключевым инструментом, поддерживающим работу с гражданами и предприятиями государственного и частного секторов. Он призван снизить количество запрашиваемых у граждан документов за счет того, что различные органы будут взаимодействовать друг с другом в электронном виде.

Новая платформа не требует наличия картридера. Ее использование не требует замены Sim-карты. Доступ к порталу осуществляется с использованием электронно-цифровой подписи (ЭЦП), идентификационных данных частных предпринимателей и граждан, верификационных данных (логин и пароль), а также мобильной системы аутентификации, которые можно получить в электронной форме после прохождения регистрации на портале. Активация осуществляется по SMS, после чего пользователю отправляется специальный идентификационный номер, который он затем может сменить.

Пользователям будет предложен сервис, позволяющий получить безопасный доступ к разным е-услугам и проводить операции по подписанию е-документов.

Для обслуживания платформы мобильной идентификации e-Gov.Identity будет создан новый сертификационный центр.

Азербайджан усердно развивает предоставление государственных услуг в сфере ИКТ. В настоящее время услуги делятся на интерактивные и информативные

Интерактивные услуги:

- Прием обращений и документов для выдачи разрешения (лицензии) на некоторые виды деятельности;
- Прием обращений и документов для выдачи специального разрешения на оборот предметов, которые могут принадлежать определенным участникам гражданского оборота и пребывание которых в обороте допускается на основе специального разрешения (с ограниченным гражданским оборотом);
- Прием обращений и документов для выдачи специального разрешения на товары (работы, услуги, результаты интеллектуальной собственности), подпадающие под экспортный контроль;
- Прием обращений и документов для выделения и использования номерных ресурсов;
- Прием обращений и документов для выдачи разрешения на распространение на территории Азербайджанской Республики иностранных периодических печатных изданий, редакция либо учредитель которых находится за пределами Азербайджанской Республики;
- Прием обращений и документов для прокладки новой телефонной линии, изменения номера, смены владельца:
  - новой телефонной линии;
  - изменения номера телефона;
  - смены владельца телефонного номера;
- Прием обращений и документов для подключения к телефонным сервисам;

- Прием обращений и документов для подключения к услугам интернета;
- Прием обращений и документов для выдачи сертификатов соответствия телекоммуникационным средствам и устройствам;
- Прием обращений и документов для регистрации средств радиосвязи;
- Оплата услуг связи посредством интернета;
- Получение информации о задолженности за услуги связи и коммунальные услуги по интернету;
- Получение информации о чеках по междугородным и международным телефонным переговорам (с детализацией звонков);
- Интернет-подписка на периодические печатные издания;
- Отслеживание почтовых отправлений;
- Прием обращений и документов для выдачи электронной подписи.

Информативные услуги:

- Выдача разрешений (лицензий) на некоторые виды деятельности;
- Выдача специального разрешения на оборот предметов, которые могут принадлежать определенным участникам гражданского оборота и пребывание которых в обороте допускается на основе специального разрешения (с ограниченным гражданским оборотом);
- Выдача специального разрешения на товары (работы, услуги, результаты интеллектуальной собственности), подпадающие под экспортный контроль;
- Выделение и использование номерных ресурсов;
- Выдача разрешения на распространение на территории Азербайджанской Республики иностранных периодических печатных изданий, редакция либо учредитель которых находится за пределами Азербайджанской Республики;
- Выдача сертификатов соответствия телекоммуникационным средствам и устройствам;
- Регистрация средств радиосвязи;
- Выдача электронной подписи.

В рамках проекта Dilmanc осуществляются работы по созданию и внедрению формальных лингвистических технологий для азербай-д-жан-ского языка. Основные научно-исследовательские направления в рамках проекта следующие:

- Разработка систем машинного перевода с других языков на азербайджанский и наоборот;
- Разработка систем распознавания речи на азербайджанском языке;
- Разработка системы озвучивания текста на азербайджанского языка;
- Разработка систем машинного перевода телефонных разговоров с других языков на азербайджанский и наоборот;
- В числе приоритетных направлений также и разработка программного обеспечения для практического пользования этими технологиями.

Достижения проекта:

В настоящее время достигнуты практические результаты по каждому из научно-исследовательских направлений и работа над улучшением их качества продолжается. В рамках проекта для азербайджанского языка созданы следующие технологии:

- Система машинного перевода с азербайджанского на английский, с английского и турецкого на азербайджанский. Работы по улучшению качества продолжаются;
- Система машинного перевода с азербайджанского на русский и наоборот;
- Система распознавания речи азербайджанского языка, работы по улучшению качества продолжаются;
- Система озвучивания текста, способная вслух зачитать текст на азербайджанском языке.

Продолжается работа по повышению качества систем машинного перевода телефонных разговоров с других языков на азербайджанский и наоборот.

Технологии, разработанные в рамках проекта, успешно представлены на многих международных выставках. Во время выставок ITU Telecom World (Швейцария), CeBIT (Германия) , CeBIT Bilishim (Турция), Связьэкспокомм (Россия), Bakutel (Баку) и др. с разработками проекта ознакомились многие влиятельные лица, представители международных организаций, руководители компаний. В их числе также президент Азербайджана Ильхам Алиев, генеральный секретарь ООН Пан Ги Мун, генеральный секретарь Международного союза электросвязи Хамадун Туре и другие.

В январе-августе 2015 года населению и организациям в Азербайджане были оказаны информационные услуги и услуги связи на сумму 1,077 млрд. манатов, что на 10,8% превышает показатель аналогичного периода 2014 года. 81,1% доходов, полученных по сектору, пришлось на долю негосударственных предприятий. Из общего объема информационных услуг и услуг связи 72,6% пришлось на долю услуг, оказанных населению. При этом 54% из общего объема полученных доходов пришлось на долю услуг мобильной связи, отмечается в отчете Государственного комитета по статистике Азербайджана по итогам восьми месяцев 2015 года.

Объем доходов, полученных от услуг мобильной связи в Азербайджане в январе-августе 2015 года, составил 581,7 млн манатов, что на 2,2% меньше показателя аналогичного периода 2014 года.

Республика Азербайджан и Катар заключили меморандум о сотрудничестве в области информационно-коммуникационных технологий (в рамках всемирной выставки-конференции Международного телекоммуникационного союза ITU Telecom World-2014, которая проходила в Дохе (Катар) 7-10 декабря 2014 года). Меморандум предусматривает сотрудничество в сферах телекоммуникаций, поддержки IT-предпринимательства. Кроме того, в качестве одного из приоритетов рассматривается область нанотехнологий.

Республика Армения

На форуме «Электронная Армения» (2015) было заявлено, что уровень доступности Интернета в Армении достиг 82%, им пользуется подавляющее большинство (67%) населения страны. По этому показателю Армения сравнима со странами ЕС. Благодаря вложениям Евросоюза, с 2010 года Армения приступила к внедрению программы электронного

правительства, что повысило качество предоставляемых госуслуг и сократило коррупционные риски, говорится в сообщении форума.

Республика Армения в 2014 году заняла 61 место среди 193 стран в мировом рейтинге ООН по уровню развития электронного правительства, в то время как в 2012 году находилась на 94 месте. Для сравнения, (данные D-Russia.ru), в рейтинге ООН электронных правительств-2014 Россия осталась, как и в прошлом году, на 27-м месте, Казахстан поднялся на 10 пунктов, с 38-го на 28-е место.

В условиях стремительно развивающегося рынка электронных услуг и электронной торговли актуальными являются вопросы цифрового доверия. Первоочередные задачи для республики:

- создание государственной системы управления открытыми ключами;
- широкомасштабное внедрение средств электронной цифровой подписи;
- разработка типовых политик безопасности для государственных информационных систем;
- создание системы идентификации для физических и юридических лиц.

Выполнение данных задач позволит свести к минимуму возможность злоупотребления персональной и иной конфиденциальной информацией. Для юридических и физических лиц должны быть созданы доступные в ценовом и техническом аспекте механизмы и средства, обеспечивающие идентификацию и аутентификацию пользователей, конфиденциальность и целостность сообщений в системах и сетях общего пользования. Это позволит расширить сферу использования электронного документооборота, обеспечит возможность ведения электронной торговли, предоставления электронных услуг, широкомасштабного внедрения систем электронных платежей.

Республика Беларусь

Министерство торговли Республики Беларусь в сотрудничестве с Ассоциацией «Инфопарк» проводит исследование по использованию информационных систем и технологий, электронных услуг в торговле, транспорте и логистике. Результаты исследования послужили основой для формирования программы третьей конференции-выставки на тему: «Электронные услуги и информационные системы для торговли, логистики и транспорта» - «IT2TLT-2015», которая состоялась 16 апреля 2015 г. в Минске (Международный образовательный центр имени Йоханеса Рау (IBB), пр-т Газеты Правда, 11).

На указанном мероприятии был приставлен проект на внедрение электронных услуг в государственные органы. Ниже приведены подпрограммы проекта:

Подпрограмма «Электронное правительство» (заказчик –Департамент информатизации Минсвязи);

Подпрограмма «Электронное здравоохранение» (заказчик – Минздрав);

Подпрограмма «Электронная занятость и социальная защита населения» (заказчик – Минтруда и соцзащиты);

Подпрограмма «Электронное обучение и развитие человеческого капитала» (заказчик – Минобразование);

Подпрограмма «Электронная таможня» (заказчик – ГТК);

Подпрограмма «Формирование национального контента» (заказчик – Мининформ).

Грузия

В Грузии с 2015 года начинается программа «Электронная Грузия». В настоящее время в стране развитию электронного правительства уделяется особое внимание. С помощью интернет-порталов граждане могут получить самые разнообразные услуги: от поступления в высшие учебные заведения до получения справок, государственные закупки также ведутся с помощью портала.

Новая программа «Электронная Грузия» призвана подвинуть е-правительство на новый уровень. Развитие электронного правительства в Грузии начиналось каждым ведомством и агентством в отдельности. Консолидация всех госорганов – одна из задач новой стратегии. Она рассчитана на 4 года.

Электронное управление повышает эффективность работы правительственных программ и услуг. Примером этого является случай электронной системы закупок, с введением которой в 2011 году, государство сэкономило 820 млн. лари (около половины миллиарда долларов). 95% налогоплательщиков активно используют электронные технологии СГД (как e declaration, электронных счет-фактур, ePayments, eCustoms) и это в значительной степени экономит людские и материальные ресурсы и уменьшает вероятность ошибок. Обмен документов между государственными органами осуществляется полностью в электронном виде. И это экономит несколько миллионов лари, а главным образом курьерские услуги.

Развитие электронных услуг имеет большое значение, как для бизнеса, так и для государственного сектора. Эти структуры имеют преимущество в том, что чаще всего контактируют с общественными услугами и это очевидно. Грузия продвинулась в мировом рейтинге в плане легкости ведения бизнеса, качества обслуживания и оценки удовлетворения потребностей клиента. Развитие электронного управления вносит свой вклад в снижение рисков коррупции, так как эта система позволяет свести к минимуму непосредственный контакт между государственными должностными лицами и клиентами. Реорганизация и оптимизация деятельности государственных учреждений, роль информационных систем имеет решающее значение. После оптимизации бизнес-процессов в правительственных организациях и реализации крупномасштабных инициатив электронного правительства, удовлетворенность качеством государственных услуг возросла с 12 до 90 процентов.

Отсутствие поддержки и приверженности со стороны политического руководства является главной угрозой для электронного правительства. Без поддержки и приверженности высшего руководства даже хорошие письменные предложения и развитые проекты рискуют быть сорванными. Именно поэтому очень трудно получить поддержку заинтересованных сторон в инновационных проектах. Развивающиеся страны также имеют инфраструктурные проблемы, отсутствие равного доступа к Интернету и низкий уровень компьютерной грамотности. Отсутствие средств также может замедлить много успешных проектов и инициатив, а проекты электронного правительства чаще всего не дешевые.

Документ «Цифровая Грузия: Грузия электронной стратегии и плана действий 2014-2018» иллюстрирует путь, ведущий в современную Грузию, и обеспечивает всестороннюю структуру для социальных изменений, разрешенных ИКТ. Чтобы извлечь выгоду из потенциала ИКТ и оптимизировать эффективность и результативность завоевания инвестиций, Грузия должна сосредоточить свои усилия на обеспечении доступности (т.е. поставлять) и использования (то есть спроса и предложения) онлайн государственных услуг со стороны правительства, бизнеса и граждан. Внедрение электронного бизнеса является ключевым вопросом для инноваций и экономического роста общества, что позволит достичь видения электронной Грузии. Основные цели (или показатели) в эффективности и результативности прибыли могут быть получены путем оптимизации электронных услуг для бизнеса по представлению данных и применения разрешений правительством об упрощении всей стоимостной цепочки общественных торгов и государственных закупок. Чтобы включить онлайн торги в соответствующие правовые рамки и стандарты необходимо общение и обмен данными. Для обеспечения универсальных услуг в области ИКТ, должна быть изучена модель государственно-частного партнерства. Развитие навыков в области ИКТ должно быть согласовано с потребностями профессиональных секторов.

Общая концепция стратегии электронной Грузии состоит в том, чтобы стать ведущей конкурентоспособной и инновационной бизнес-средой в области ИКТ в Кавказском регионе, что само собой требует передового опыта в области развития ИКТ. Для разработки сильного сектора ИКТ, который создаст высококвалифицированные рабочие места и конкурентное преимущество в регионе, необходимы четкие планы, чтобы определить области инвестиций в ИКТ, принять соответствующие навыки и передовой опыт, привлечь таланты в глобальном масштабе, и присоединиться к крупным проектам.

Республика Казахстан

Республика Казахстан активно развивает электронные государственные услуги. Для этого по инициативе правительство был создан проект «электронное правительство».

Идеальное общество характеризуется крепким здоровьем, хорошей работой, обеспеченным бытом, благоприятными условиями для жизни граждан. Однако, неотъемлемой частью такого общества является государство. Государство, которое заботится о своих гражданах. Государство, которое предоставляет возможности для лучшей реализации потенциала каждого гражданина. Государство, которое гарантирует сохранность и соблюдение законных прав граждан. Государство, ориентированное на нужды и потребности граждан. Государство, взаимодействие с которым будет простым, понятным и доступным – государство для людей**.**

Развитие информационно-коммуникационных технологий в Республике Казахстан может гарантировать выполнение как минимум двух последних утверждений. Именно для того, чтобы взаимодействие граждан и государства было комфортным, простым, доступным и понятным была разработана концепция электронного правительства.

Создание электронного правительства было необходимо для того, чтобы сделать работу органов власти более эффективной, открытой и доступной для граждан. Раньше каждый государственный орган «жил своей жизнью» и мало соприкасался с остальными, а гражданам приходилось обходить множество инстанций, чтобы собрать всевозможные справки, подтверждения и прочие бумаги. Все это превращало процесс получения одной услуги в

бесконечную ходьбу по учреждениям. Теперь с этим покончено, благодаря проектам электронного правительства.

Электронное правительство – это единый механизм взаимодействия государства и граждан, а также государственных органов друг с другом, обеспечивающий их согласованность при помощи информационных технологий. Именно этот механизм позволил сократить очереди в государственные органы и упростить и ускорить получение справок, свидетельств, разрешительных документов и многого другого.

Другими словами, электронное правительство – это когда для оформления лицензии необходим только Индивидуальный идентификационный номер (ИИН) (а все остальные данные получают при помощи автоматических запросов), когда можно оплатить коммунальные услуги и штрафы онлайн, когда для получения справки в ЦОН может потребоваться только удостоверение личности, когда гражданин сам может зарегистрировать бизнес или получить справку на портале «электронного правительства» за 10-15 минут, когда узнать очередь ребенка в детский сад можно в любое время дня и ночи, получить адресную справку на мобильный телефон и т.п.

Проект создания электронного правительства был предложен почти девять лет назад. За это время пройдены четыре глобальных этапа становления и развития электронного правительства. Каждый из этих этапов по-своему помогал казахстанцам во взаимодействии с государством.

Первый этап – информационный. В этот период был запущен портал электронного правительства и наполнен информацией. Появилась информация о госорганах, их работе и услугах, которые они предоставляют населению. Кроме того, были приведены регламенты оказания услуг и вывешены для ознакомления нормативно-правовые акты.

На этом этапе каждый казахстанец мог получить на портале всю необходимую информацию – список необходимых документов, размер госпошлины, контактные данные госоргана, в который нужно обратиться. Уже на первом этапе хождение по инстанциям и количество посещений сократились, за счет предоставления полного объема необходимой информации.

Второй этап - интерактивный**,** был ознаменован стартом предоставления на портале электронных услуг. Пользователям портала открылась возможность получать справки из разных учреждений, не бегая по учреждениям и не теряя времени в очередях, отправить запрос в любой госорган, не выходя из дома и отслеживать его статус. Внедрение интерактивных услуг на портале электронного правительства позволило в разы экономить время на сборе пакета документов.

Именно на этом этапе были внедрены ведомственные информационные системы, государственные базы данных, электронное лицензирование и шлюз электронного правительства.

Третий этап развития электронного правительства – транзакционный**.** На этом этапе граждане получили возможность оплачивать государственные пошлины и сборы, штрафы, коммунальные услуги. Если раньше для оплаты услуги необходимо было идти в банк, то теперь услугу можно и получить и оплатить онлайн.

Для предпринимателей транзакционный этап преподнес поистине ценный подарок – электронные государственные закупки. Выгоды очевидны - повысилась прозрачность и открытость проводимых конкурсов, тендеров.

Четвертый этап электронного правительства – трансформационный**,** на этом этапе развития электронное правительство находится в настоящее время. Главной целью является максимальная оперативность в оказании услуг гражданам. Именно ради достижения этой цели интерактивные и транзакционные сервисы объединяются в комплексные услуги, в которых часто нуждается казахстанское население. У пользователей появилась возможность зарегистрировать юридическое лицо за 15 минут или зарегистрировать рождение ребенка при этом одновременно решив все сопутствующие вопросы - подать заявление на назначение пособий и поставить ребенка на очередь в детский сад. Особое внимание на портале электронного правительства уделяется социально-значимым услугам, именно поэтому все они переведены в электронный формат. Для оказания государственных услуг инвалидам 1 и 2 категорий в Центрах обслуживания населения работают специальные мобильные группы. Для вызова такой мобильной группы человеку необходимо обратиться в Единый контакт центр по номеру 1414.

За время своего существования электронное правительство Республики Казахстан преодолело четыре этапа становления и развития, было позитивно принято и высоко оценено мировым сообществом - об этом свидетельствуют высокие позиции в международных и республиканских рейтингах, номинации в конкурсах. Степень развития казахстанского электронного правительства оценивается как «развивающиеся» (emerging leaders) и считается одним из самых успешных.

13 мая 2013 года в Женеве были объявлены результаты международного конкурса WSIS Project Prizes 2013, который прошел в рамках Форума Всемирной встречи на высшем уровне по вопросам информационного общества. Система электронного лицензирования Казахстана (www.elicense.kz) стала лучшим проектом в категории «E-Business». Всего в конкурсе приняли участие более 280 проектов из 64 стран мира. История успеха проекта была опубликована на официальном ресурсе Международного союза электросвязи.

В апреле 2013 года был опубликован доклад Всемирного экономического форума (WEF)**,** согласно которому Индекс сетевой готовности Казахстана находится на 43 месте из 144 стран. По сравнению с 2012 годом и 55 позицией в рейтинге страна показывает стремительный рост по многим параметрам и является лучшей среди стран СНГ. Индекс сетевой готовности определяет уровень развития информационно-коммуникационных технологий (ИКТ) в стране и состоит из 54 показателей, отражающих вклад ИКТ в экономику и готовность национальных экономик к использованию этих технологий.

Каждые два года Департамент по экономическим и социальным вопросам Организации Объединенных Наций проводит исследования по оценке уровня развития электронного правительства в мире (192 страны). В 2012 году электронное правительство республики Казахстан в этом рейтинге заняло 38 место. При этом индекс онлайн-услуг вырос на 10 позиций, а телекоммуникационной инфраструктуры – на 14 позиций. По индексу е-участия, который определяет возможность общения граждан с правительством, Казахстан занял 2-ое место, разделив его с Сингапуром.

В конце 2012 года на X юбилейной церемонии награждения Национальной интернет-премии Award.kz-2012 портал электронного правительства занял первое место в номинации «Органы власти и самоуправления», а также был признан лучшим среди двуязычных сайтов. Внимание к проекту привлек прошедший в октябре редизайн портала электронного правительства,

в результате которого изменилось не только визуальное оформление, но и структура материалов, логика размещения.

Достижения электронного правительства Республики Казахстан с 2005 по 2014 год

Всемирный рейтинг ООН (193 страны)	2014	2013	2012	2010
Индекс развития электронного правительства	28	-	38	46
Индекс человеческого капитала		-	25	16
Индекс онлайн услуг	23	-	14	95
Индекс телекоммуникационной инфраструктуры		-	77	96
Индекс е-участия	23	-	2	18
Рейтинг Всемирного экономического форума(WEF)	2014	2013	2012	2011
Индекс сетевой готовности	38	43	55	67
Подиндекс готовности		62	52	56
Подиндекс использования		54	65	56

Анализ подготовлен ГУ «Инфо-Система» при МФ КР

В Казахстане порядка 675 государственных услуг, из них 77 можно получать через интернет. Согласно предварительному анализу 11,4% государственных услуг Казахстана в настоящее времяпредоставляется через интернет. Для сравнения — в Эстонии этот показатель составляет более 70%. Всего же на портале www.egov.kz в рамках проекта «Электронное правительство» предоставляются более 236 электронных услуг.

Портал электронного правительства www.egov.kz разрабатывается национальным оператором в сфере информационных технологий Республики Казахстан АО «Национальные информационные технологии» (АО НИТ), дочерней компанией АО «Национальный инфокоммуникационный холдинг «Зерде». Национальный инфокоммуникационный холдинг «Зерде» позиционируется как крупнейшая казахстанская государственная компания, созданная для развития современных инфокоммуникационных технологий. Холдинг образован в сентябре 2008 года согласно постановлению Правительства Республики Казахстан, являющегося его единственным акционером.

Также в состав Национального инфокоммуникационного холдинга «Зерде» входят группа компаний:

- АО «Национальные информационные технологии», которое является национальным оператором в сфере информационных технологий РК;
- АО «Национальная компания «Kazsatnet», которое является ответственным исполнителем по развитию Единой транспортной среды государственных органов РК путем организации защищенных каналов передачи данных для государственных органов, охватывающих областные и районные центры РК;

- ТОО «Центр электронной коммерции», которое является единым оператором в сфере электронных государственных закупок в РК;
- АО «Казконтент», деятельность которого направлена на формирование развитого национального сегмента глобальной информационной сети интернет в Казахстане, в том числе развитие сетевых информационных ресурсов, организация ИТ инфраструктуры, стимулирование инвестиционной и инновационной активности в этой сфере;
- АО «Национальный процессинговый центр»;
- АО «Международный университет информационных технологий».

В период с 2007-2009 гг, АО «НИТ» разработало программу документооборота, инфраструктуру выдачи и распознавания электронных ключей, а также единую информационную среду, по аналогу с эстонским x-Road, и национальные регистры идентификационных номеров. 2007 г. — 20 услуг, 2010 — 59 услуг, 2011 — 74 услуги можно получать уже через интернет.

С 1 января 2010 года заработал портал государственных электронных закупок www.goszakup.gov.kz, оператором этой системы является ТОО «Центр электронной коммерции». К 2011-му году создана система «электронное лицензирование» для частных компаний и фирм, единая система «Е-Нотариат» и «Е-Акимат» для автоматизации работы районных администраций. Возможность оплачивать государственные услуги через интернет появилась в 2010 году, теперь через портал электронного государства Казахстана можно оплатить налоги, государственные сборы и пошлины, штрафы за нарушения ПДД, также можно оплачивать услуги ЖКХ.

В 2012-м году, на сайте www.egov.kz осуществляется интеграция баз данных ЗАГСа, Минздрава и МВД. Сейчас на этом портале предлагается 77 государственных услуг, оплата 21 вида госплатежей, 16 госпошлин, 4 вида налоговых платежей и оплата всего перечня штрафов за нарушение ПДД.

Идентификация гражданина в системе осуществляется следующим образом. Каждая электронно-цифровая подпись (ЭЦП), может быть выдана на внутренний паспорт гражданина Казахстана, и записана на его идентификационный номер на ID-карте нового образца. Информация записывается на микрочип через стандартный и недорогой считыватель карт с помощью портала www.egov.kz. В апреле 2012 года выдана миллионная электронно-цифровая подпись — ЭЦП. Обладателем «исторической» электронной подписи (ЭЦП) стал 21-летний житель города Алматы. С начала текущего года Национальным удостоверяющим центром (НУЦ) было выдано свыше 100 000 ЭЦП. Для сравнения в 2010 году выдано 316 000 ЭЦП, а в 2011 478 292 ЭЦП ключей.

Приведём перечень государственных услуг портала по видам www.egov.kz**:**

1. Приобретение недвижимости;
2. Ипотека;
3. Коммунальные тарифы;
4. Адресная справка;
5. Проверка адресных данных физического лица
6. Выдача актов гражданского состояния (рождение, брак, развод, смерть)

7. Пенсионное обеспечение

8. Выдача прав на вождение

9. Регистрация доверенностей

10. Налогообложение и аудит

11. Выдача актов на право земельного пользования

12. Медицинская регистратура, база данных лекарств и рецептов, перечень медтехники

13. Получение гражданства, прописки

14. Постановка на учет СМИ

15. Сертификат о культурной ценности

16. Регистрация и защита интеллектуальной собственности

17. Регистрация контрактов на геологическую разведку, добычу и переработку полезных ископаемых

18. Регистрация воинской обязанности

19. Регистрация радиочастотных устройств

20. Регистрация недвижимости земельных наделов

21. Регистрация гарантийного обязательства для таможни

22. Выдача удостоверений на водный транспорт

23. Регистрация ЖД транспорта

24. Справки и заверения нотариуса

25. Получение школьного аттестата, управления собственностью и

имуществом несовершеннолетних

26. Регистрация сельхозтехники

27. Выдача архивных справок, архивные справки от КНБ

28. Выдача лицензий на производство стройматериалов и строительство

29. Хранение IT-технологий и прав на них в депозитарии

30. Начисление пособий на детей и специальных пособий

Несмотря на созданный портал и Е-государство, в Казахстане существует проблема с использованием данными государственных ресурсов. По данным статистической государственной информационной системы «Талдау», менее 1 миллиона людей пользуются фиксированным подключением к интернету и при этом большая часть интернет-пользователей находится в г.Алматы.

На май 2012 года общее количество интернет-пользователей в Казахстане превысило 9,4 млн. человек, количество сайтов в зоне KZ составил порядка 62000.

Финансовое обеспечение проекта «Электронного правительства» предусматривает общие затраты, предусмотренные в республиканском бюджете на реализацию «Программа по развитию информационных и коммуникационных технологий в Республике Казахстан на 2010 — 2014 годы», которая утверждена Правительством РК 29 сентября 2010 года (по курсу на 28.09.2012 1 доллар США = 150,01 тенге):

- 2010 год — 17 млрд 973 495 000 тенге или 119 млн 815 000 долларов США;
- 2011 год — 23 млрд 249 269 000 тенге или 154 млн 984 000 долларов США;
- 2012 год — 20 млрд 893 445 000 тенге или 139 млн 280 000 долларов США;
- 2013 год — 5 млрд 182 136 000 тенге или 34 млн 545 000 долларов США;
- 2014 год — 4 млрд 491 972 000 тенге или 29 млн 944 480 долларов США.

Всего до конца 2014 года на реализации программы ИКТ планировалось потратить из госбюджета порядка 480 млн. долларов США.

Кыргызская Республика

Использование ИКТ в рамках модели «электронное правительство» предусматривает переход к новой форме отношений государственных органов и организаций на основе использования возможностей Интернета, информационно-коммуникационных технологий с целью непрерывной оптимизации процесса предоставления услуг, повышения уровня участия граждан в вопросах государственного управления и совершенствования внутренних процессов.

Важным этапом для развития отрасли ИКТ в КР стала государственная программа «Электронное управление» (2014-2017), которая определила новый способ взаимодействия между государством, бизнесом и обществом на основе активного использования информационно-коммуникационных технологий (ИКТ) в целях повышения эффективности предоставления государственных услуг. Именно доступность всем категориям граждан должна стать краеугольным камнем при развитии ИКТ и при переходе большинства форм взаимодействия между государством и обществом в электронную форму.

В «Рейтинге стран мира по уровню развития электронного правительства», который подготовлен совместно с представительством Программы развития ООН в России, Кыргызстан занимает 101 место из 193, и его индекс развития электронного правительства составляет 0.4657 на 2015 год.

В Кыргызской Республике создан Государственный центр электронного управления (ГЦЭУ), который разработал проект постановления правительства о создании Государственного центра электронного управления. Разработаны стандарты государственных услуг, предусматривающие полное или частичное предоставление государственных услуг в электронном формате.

В настоящее время в стране имеется порядка 145 разнородных и, как правило, автономно сформированных и функционирующих государственных информационных систем (ИС) в 40 ведомствах и организациях. В основном это – базы данных (БД), системы электронного документооборота (СЭДО), бухгалтерского и кадрового учета. В то время как между некоторыми

БД осуществляется обмен информацией и данными, не существует единой общегосударственной концепции взаимодействия государственных ИС. То есть отсутствует межсистемная совместимость, не только электронная (техническая), но и организационно-информационная. Отметим, что это довольно типичная ситуация на пост-советском пространстве.

Не существует также реализованных на практике общих для всех государственных ИС инфраструктурных, платформенных и программных сервисов. Наличие таких сервисов позволяет архитектурно обеспечить создание эффективной системы межведомственного электронного взаимодействия и совместимости и оказывать на этой основе электронные услуги для конечных пользователей. Отсутствуют модели и сценарии реорганизации и оцифровки внутренних бизнес-процессов и регламентов.

Республика Молдова

Строительство информационного сообщества – национальный приоритет, а методы достижения поставленной цели зависят от способности властей установить правильные направления в развитии и мобилизовать все необходимые ресурсы. По данным международных экспертов, для Республики Молдовы, которая не располагает природными и собственными энергетическими ресурсами, человеческий капитал и создание оптимальных условий труда могут обеспечить добавочную экономическую ценность.

В соответствии с заявлением о намерениях, подписанным в Любляне в 2002 г. странами-членами Пакта стабильности для Юго-Восточной Европы, Республика Молдова (РМ) взяла на себя обязательство создать информационное общество с ориентацией на интересы всех граждан, с учетом принципов, закрепленных в Уставе ООН, во Всеобщей декларации прав человека и в Окинавской Хартии глобального информационного общества (2000 г.). В последние годы развитие информационного общества в РМ проявляется в выраженном росте плотности мобильной и фиксированной телефонной связи, обеспечивающей доступ населения к информационным ресурсам. Также существует надежная международная связь через спутник или волоконно-оптические линии передач. В последние годы в республике значительно возросло число служб по оказанию Интернет-услуг, а также количество пользователей данными услугами. Благодаря тому, что увеличился объем финансирования из государственных и административно-территориальных бюджетов, возросло количество и качество технических средств. Однако уровень потребности населения в них гораздо выше, нежели предложение, а устранение этого дисбаланса и является основным показателем развития информационного общества.

Современный этап развития информационного общества в Республике Молдова во многом характеризуется результатами реализации «Национальной стратегии создания информационного общества – «Электронная Молдова»», утвержденной Постановлением Правительства Республики Молдова № 46-50/336 от 25 марта 2005 года.

Концептуальной основой для ее разработки стали Указ Президента Республики Молдова №1743-III от 19 марта 2004 г. «О создании информационного общества в Республике Молдова» и Постановление Правительства № 632 от 8 июня 2004 г. «Об утверждении Политики создания Национальной стратегии создания информационного общества в Республике Молдова».

Основной целью Национальной стратегии «Электронная Молдова» обозначено развитие Республики Молдовы в качестве активного и конкурентоспособного участника новой экономики,

основанной на знаниях, что обеспечит демократический путь к развитию и экономическому благополучию, интеграцию в европейское информационное пространство.

В ходе реализации Национальной стратегии к 2010 году удалось осуществить 44 ключевых проекта, предусмотренных соответствующим Планом действий. Указанные проекты реализовывались в таких важных направлениях развития информационного общества как: инфраструктура информационного общества, электронное управление и электронная демократия, электронная экономика, электронное образование, электронная наука как решающий фактор развития, электронная культура, электронное здравоохранение.

По итогам реализации «Электронной Молдовы» к 2010 году удалось в основном решить задачи: повышения эффективности процесса управления, повышения уровня ответственности Правительства перед гражданами и граждан перед обществом; повышения уровня доверия каждого гражданина и всего общества к информационным системам путем обеспечения безопасности технических средств и программных продуктов, защиты персональных данных, гарантирования неприкосновенности частной жизни; развития стабильного и защищенного общества путем использования информационно-коммуникационных технологий для предотвращения и управления кризисами, защиты окружающей среды, обеспечения безопасности граждан и государства; развития информационной культуры путем создания условий доступа к образовательным программам по информатике для каждого гражданина, независимо от пола, этнической принадлежности или языка, вероисповедания или социального статуса; интеграции в региональное и международное информационное пространство.

По оценкам экспертов осуществление Национальной стратегии «Электронная Молдова» позволило вовлечь национальные компании в реализацию информационных систем для государства и тем самым, обеспечить хорошие условия для развития моделей государственно-частного партнерства в сфере связи и информатизации.

Учитывая, в частности величину ежегодного бюджета «Электронной Молдовы» в не менее, чем 0,8% от ВВП, представляется, что достигнутые Республикой Молдова результаты достаточно позитивны.

Вместе с тем, ряд проблем продолжает оставаться актуальными. Например, в рамках реализации «Электронной Молдовы» не удалось создать конкурентного и эффективного рынка ИКТ в Республике Молдова, сформировать достаточную нормативную правовую основу для участия зарубежных компаний в национальных инфраструктурных проектах и программах, достичь прогресса в сфере развития кабельного и цифрового телевидения.

В этой связи, необходимо признать, что вектор дальнейшего развития информационного общества в Республике Молдова в настоящее время претерпевает существенные изменения в рамках разработки проекта Стратегии «Цифровая Молдова 2020».

При поддержке местных и зарубежных экспертов были сформулированы видение и цели Стратегии «Цифровая Молдова 2020», которые были представлены 17 мая 2012 года на тематическом заседании на высшем уровне в рамках Саммита «Moldova ICT 2012».

Реализация этой стратегии с одной стороны должна обеспечить осуществление задач по развитию Информационного общества на основе «Цифровой повестки дня для Европы 2020», а также других международных практик в данной области. С другой, открыть возможности для ускоренного развития информационного общества в Республике Молдова с учетом регионального опыта становления информационного общества в государствах Азиатско - Тихоокеанского региона. Согласно Стратегии «Цифровая Молдова 2020», к 2020 году около 80% публичных услуг

будут предоставляться электронным путем, а 60% граждан будут использовать цифровую подпись.

Республика Молдова реализовывала европейскую модель построения информационного общества. Однако, с принятием Стратегии развития информационного общества в Республике Молдова «eMoldova 2020» в 2013 году, европейский путь развития скорректирован с учетом опыта построения информационного общества в Республике Корея и ряде других азиатских государств.

За последние несколько лет внедрено уже много услуг. С 23 июля 2009 г. электронное декларирование стало уже привычным делом для продвинутых бухгалтеров. Они оценили удобство этой услуги, а заодно и защиту от ошибки при заполнении электронной декларации (данные, введенные через бухгалтерские системы, проверяются автоматически). В настоящее время около 26 тыс. предприятий и 5 тыс. граждан заполняют и подают налоговые документы посредством Интернета, используя сайт https://servicii.fisc.md/.

Позже, в августе 2010 г., для внедрения Стратегической программы технологической модернизации управления (e-Преобразование) правительством был создан Центр электронного управления. Он отвечает за развитие национальной платформы электронного управления и национальной электронной системы, создание цифровых услуг и повышение уровня доступа населения к электронным государственным услугам. Все это в итоге нацелено на то, чтобы все желающие пользовались информацией с портала открытых данных и электронными услугами в любое время суток, оперативно и безопасно, а деятельность государственных структур с помощью информационных технологий стала прозрачной. Веб-страница Центра электронного управления http://egov.md структурирована по трём направлениям: «Правительство для граждан», «Правительство для бизнеса» и «Правительство для правительства». В интересующем нас разделе «Правительство для бизнеса» можно ознакомиться со всеми услугами.

С ноября 2012 г. за лицензией можно обратиться (или переоформить/продлить ее) on-line. Кроме того, личного общения со служащими можно вообще избежать, если заказать получение лицензии по почте. С начала действия услуги до 1 января 2014 г. ею воспользовались свыше 6200 заявителей. В декабре прошлого года уже более половины обращений поступило on-line.

Для отчётности есть несколько видов услуг – «e-Отчетность» (с 1 января 2012 г.), а также внедрённые ранее «Электронная декларация» и «Быстрая декларация». Для подачи деклараций в электронном виде в Национальную кассу социального страхования (Rev 5 и 4-BASS) разработана услуга «e-НКСС» (с 18 февраля 2013 г.). Одновременно с ней была запущена аналогичная услуга для отчётности в Национальную медицинскую страховую компанию – «e-НМСК», позволяющая посредством Интернета отправлять в любое удобное время, без лишних затрат и ошибок формуляры «2-03» и «2-04». Эти услуги являются частью отчётной платформы, интегрированной в систему M-Cloud, которую размещает ГП «Центр специальных телекоммуникаций». О популярности этих услуг можно судить по количеству пользователей мобильной подписи, т.к. мобильная подпись – необходимое условие, чтобы воспользоваться электронными видами отчетности. На 1 января 2014 г. таких пользователей было более 5 тыс.

Многие предприятия заинтересованы участвовать в тендерах, проводимых для госзакупок различных товаров и услуг. В последние годы и количество тендеров, и объёмы закупок заметно выросли. Их мониторинг, естественно, усложнился. В этом отношении электронная система «Государственный регистр государственных закупок», созданная Агентством государственных закупок, содействует повышению прозрачности в данной сфере. Таким образом, процесс закупок сместился в электронный формат в режиме on-line и дал много преимуществ по сравнению с

обычным. Например, доступ к документации по торгам предоставляется on-line или, тоже в режиме реального времени, можно следить за всем процессом закупок или запроса ценовых оферт; личные контакты между участниками сведены к минимуму. Услуга «e-Государственные закупки» работает с 7 февраля 2013 г.

17 сентября 2013 г. была введена в действие услуга электронных платежей MPay, с помощью которой можно оплачивать различные услуги. Она разрабатывалась в первую очередь для расчётов в государственном секторе, но может быть использована и в коммерческих целях через банковские карты, платёжные терминалы, системы e-banking и даже наличные платежи посредством банков и отделений «Poşta Moldovei». MPay могут воспользоваться и физические лица - те, кто платит за госуслуги, и юридические, которые тоже рассчитываются или, наоборот, взимают плату за услуги. В общем, владельцы банковских карт теперь могут в электронном формате вносить плату за услуги ГП «Cadastru» и ГП «Registru», e-Cazier, за приобретение идентификационных средств домашних животных, за выдачу дубликатов и выписок из актов записи гражданского состояния, а также оплачивать стоимость типовых форм первичных документов, выдаваемых Государственной налоговой службой, и штрафы, которые выписывает дорожная полиция. Для этого нужно на портале https://servicii.gov.md/ открыть раздел e-Servicii (пока доступно только на румынском языке) и заполнить заявку. Будет подсчитана сумма и предложено ее оплатить через MPay и далее следовать инструкции. В любой момент можно будет проверить статус платежа. С сентября до конца прошлого года через эту систему платежа прошло более 24400 транзакций.

Из последних услуг – «e-Фактура», с помощью которой предприятие может выдавать, редактировать и отправлять в электронном виде товаротранспортные и налоговые накладные, без необходимости приходить их заказывать в офисе Государственной налоговой службы. Выгоды от использования «e-Фактура» очевидны – повышается оперативность при документировании сделок, экономятся средства, которые тратились на покупку накладных, снижается риск подделки налоговых накладных, растет производительность труда, сокращаются расходы на печать бланков этих документов, исключается их утрата (нет ни одного выпуска «Официального монитора» без публикации об утере пачки налоговых накладных, что само по себе очень подозрительно. – прим. ред.) и снижается фактор коррупции. Услуга «e-Фактура» будет внедряться в три этапа. Сначала в течение шести месяцев будет проходить тестирование в узком кругу предприятий, чтобы выявить слабые места программы и скорректировать. С июня 2014 г. начался экспериментальный этап работы данной услуги для всех хозяйствующих субъектов, а с января 2015 г. она должна была заработать на национальном уровне.

Важным шагом в процессе перевода государственных услуг в электронный вид является создание веб-страницы Министерства образования РМ, а также разработка учебных модулей для обучения преподавателей ОУ ПТО и общеобразовательных школ республики в области применения ИКТ в учебном процессе. В настоящее время на веб-странице Министерства образования реализуется функция хранения и предоставления информации, представляющей интерес для всех уровней образования в РМ. Все профессионально-технические школы имеют, по крайней мере, один подключенный к Интернету компьютер, при помощи которого можно войти на веб-сайт Министерства и получить необходимую информацию. Связь между Министерством и ОУ ПТО организована по электронной почте. Правительство РМ намерено осуществить крупномасштабные цифровые преобразования в системе управления. Первоочередная цель состоит в проведении аудита всех государственных предприятий, которые предоставляют платные

услуги предпринимателям и гражданам, в целях повышения эффективности их работы за счет быстрого репроектирования всех процессов с использованием ИКТ. Следующим этапом станет обеспечение доступа к различным государственным реестрам через Интернет, при этом особое внимание будет уделено защите персональных данных и любой другой информации частного характера.

В целях реализации поставленных задач Правительство планирует:

- разработать единую структуру управления и организации в публичном секторе для внедрения ИКТ в государственных учреждениях;
- разработать и внедрить служебные порталы «Правительство – Бизнес» и «Правительство – Граждане»;
- расширить предоставление онлайн и мобильных услуг для граждан и предпринимателей.

В настоящее время граждане РМ имеют доступ к электронной базе данных Департамента информационных технологий, Департамента статистики и социологии, Департамента таможенной службы, Государственной налоговой инспекции и других государственных учреждений. Однако эти разработки не позволяют получать и использовать данные относительно всех уровней власти и гражданского общества. К тому же, хотя многие государственные учреждения – Парламент, некоторые министерства и ведомства – обеспечивают доступ граждан к определенного рода информации на своих сайтах, эти возможности не являются интерактивными. В целом, приходится констатировать, что общие стандарты для интеграции всех ведомственных данных в единую систему пока не были разработаны и внедрены.

В рамках одного из проектов, при финансовой поддержке Всемирного банка, планируется создать информационную систему для картографирования учебных заведений Молдовы в целях повышения эффективности управления образованием.

За формирование и развитие системы электронного правительства в Республике Молдова отвечает Центр реализации проектов электронного правительства.

Республика начала активно работать над введением электронной подписи граждан. Помимо этого проекта есть и ряд других: это стартовавшая в феврале 2013 года реализация программы размещения данных в государственном облаке; переведение государственных услуг в электронный вид; запущенная в апреле 2013 года инициатива по введению онлайн-платежей и проект правительственной платформы, которая призвана облегчить процесс межведомственного обмена данными. В настоящее время также ведется активная работа в области открытых данных.

Портал открытых данных data.gov.md заработал в Молдове в апреле 2011 года, став таким образом первым порталом открытых данных, запущенным в Восточной Европе. Каждое министерство назначает ответственных за публикацию данных на портале.

В свою очередь, Центр реализации проектов электронного правительства координирует работу по раскрытию данных. В настоящее время на портале опубликовано более 700 дата-сетов. План действий включает перечень данных, которые должны были раскрыты до конца 2013 года. Более 80% из них уже раскрыто.

Сейчас правительство Молдовы оценивает прогресс выполнения правительственного плана действий на текущий год и подготавливает «дорожную карту» на следующий.

Российская Федерация

В Российской Федерации действует Государственная программа «Информационное общество (2011-2020гг.)», создан и успешно функционирует портал «Госуслуги» (https://www.gosuslugi.ru/). Аналогичные порталы созданы в субъектах федерации, а также в федеральных государственных и муниципальных организациях.

Государственный проект: МЭДО	Государственный проект: СМЭВ
Решение ЭОС: Сервер электронного взаимодействия	Решение ЭОС: Система оказания госуслуг

«Портал государственных услуг Российской Федерации» — справочно-информационный Интернет-портал (сайт). Обеспечивает доступ физических и юридических лиц к сведениям о государственных и муниципальных услугах в Российской Федерации, государственных функциях по контролю и надзору, об услугах государственных и муниципальных учреждений, об услугах организаций, участвующих в предоставлении государственных и муниципальных услуг, а также предоставление в электронной форме государственных и муниципальных услуг.

Все услуги, размещенные на портале, соотнесены с конкретным регионом Российской Федерации: место получения услуги определяет как наличие самой услуги, так и условия её предоставления.

Функционирование портала Gosuslugi.ru как государственного веб-сайта осуществляется на основе Федерального закона Российской Федерации от 27 июля 2010 г. N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и Постановления Правительства России от 24 октября 2011 года № 861 было утверждено Положение о федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)».

Регистрация на портале проходит с помощью Единой системы идентификации и аутентификации (ЕСИА). Регистрация включает несколько этапов с обязательной привязкой и проверкой электронного адреса, мобильного телефона, а также подтверждением личности пользователя (код подтверждения высылается почтой либо передаётся через офис ОАО «Ростелеком»). Примечательно, что авторизация происходит по страховому номеру индивидуального лицевого счета страхового свидетельства обязательного пенсионного страхования (СНИЛС).

После регистрации перечень стандартных функций портала расширяется, например, становится возможным в два клика получить сведения о состоянии личного лицевого счёта из Пенсионного фонда или подать заявление на получение загранпаспорта нового поколения, непосредственно заполнив форму на портале.

Улучшение качества оказания государственных и муниципальных услуг и повышение эффективности государственного управления являются приоритетными задачами для органов власти на всех уровнях. Внедрение передовых информационных технологий - один из ключевых элементов комплекса проводимых с этой целью мероприятий.

Среди наиболее актуальных задач, связанных с внедрением современных систем управления документами и информацией , можно выделить:

- Создание и расширение существующих ведомственных, региональных и межведомственных систем электронного документооборота.
- Автоматизация приема и обработки обращений заявителей в органы государственного и муниципального управления, организация «виртуальных приемных».
- Обеспечение межведомственного электронного взаимодействия федеральных органов государственной власти и органов субъектов федерации в рамках проекта **межведомственного электронного документооборота (МЭДО)**.
- Обеспечение взаимодействия СЭД с порталами госуслуг и с **системой межведомственного электронного взаимодействия (СМЭВ).**
- Обеспечение взаимодействия с **автоматизированной системой «Обращения граждан» (АС «Обращения граждан»).**

В 2014 году доля населения, пользующегося преимуществами получения государственных услуг в электронном виде, в общей численности населения достигла 40% против 20 % в 2013 году.

Для удобства пользования услугами был разработан новый упрощенный порядок регистрации пользователей на едином портале госуслуг (ЕПГУ) и в единой системе идентификации и аутентификации (ЕСИА). Раньше в процессе регистрации необходимо было использовать страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования (СНИЛС), а начать пользоваться услугами можно было только после визита в центр обслуживания «Ростелекома» или получения заказного письма через «Почту России». Теперь регистрация на портале госуслуг осуществляется с помощью мобильного телефона и в онлайн-режиме.

Быстрый доступ к электронным госуслугам получили и владельцы универсальной электронной карты (УЭК) с квалифицированной электронной подписью. При помощи УЭК они могут регистрироваться и входить на единый портал.

В течение 2013 года ЕПГУ в среднем ежемесячно посещало 3,1 млн. человек, это более чем вдвое превышает показатель 2013 года, когда среднемесячная аудитория портала составляла 1,4 млн человек. Пик посещений 2014 года пришелся на май — 4 423 740 посетителей. Абсолютный прирост зарегистрированных посетителей ЕПГУ в 2014 году — 3,4 млн. человек. В настоящее время общее число зарегистрированных пользователей портала составляет 10 млн. человек.

Самой востребованной среди населения госуслугой стала проверка штрафов ГИБДД (39% от общего числа запросов), следующая по популярности — проверка налоговой задолженности (21%), на третьем месте — выдача загранпаспорта нового образца (14%). Всего в 2014 году через ЕПГУ было подано свыше 14 млн заявлений: более 13 млн. через сайт и более 800 тыс. через мобильные приложения.

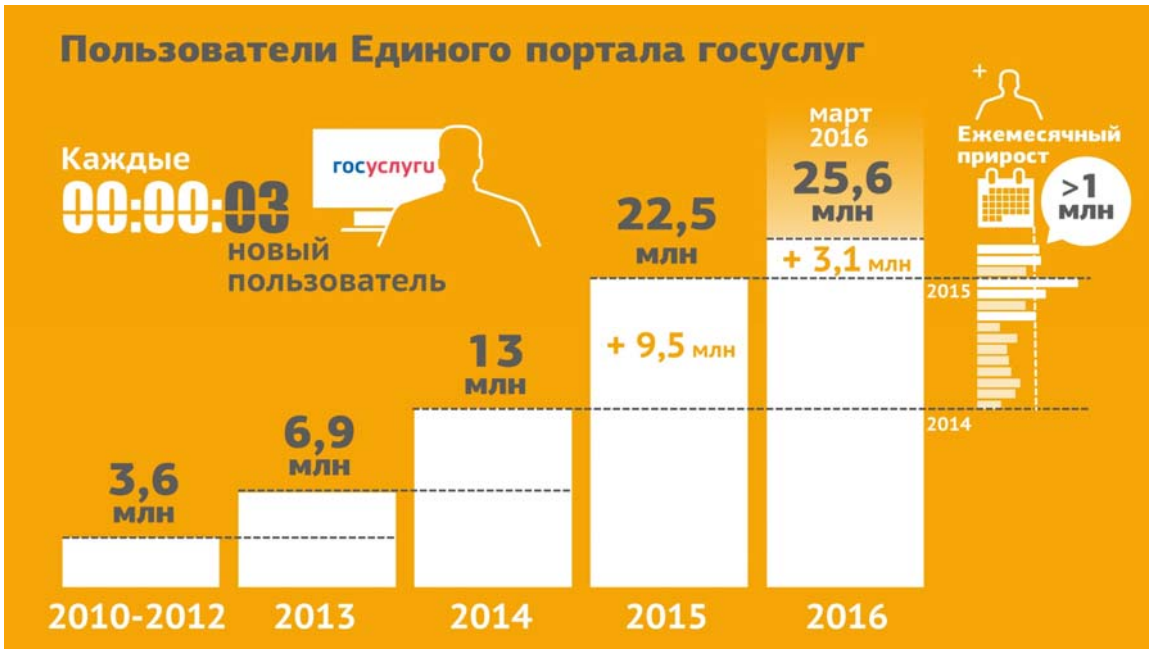
В 2014 году более чем в четыре раза увеличилось количество платежей через ЕПГУ. Было осуществлено транзакций более чем на 560 млн. рублей при общем количестве платежей более 527 тыс. Средний платеж составил чуть более 1000 рублей.

Согласно планам, озвученным первыми лицами государства, уже в 2015 г. все государст - венные услуги (более 1500) должны предоставляться в электронном виде.

На Расширенной коллегии Министерства связи и массовых коммуникаций Российской Федерации были приведены следующие данные.

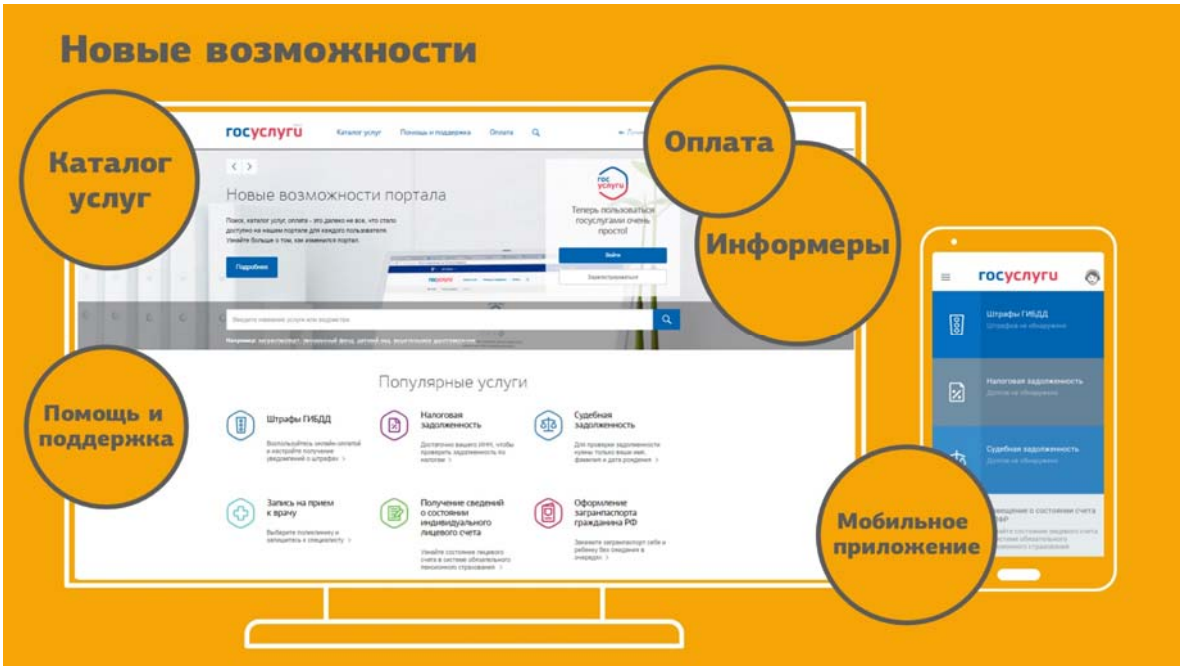
В настоящее время в Российской Федерации достигнут показатель - 39,6% получателей госуслуг в электронном виде. Этот показатель оценен по методике Росстата. Поставлена задача — 70% за два года. Основная технологическая, нормативная готовность к тому, чтобы достичь этого показателя есть, но сохраняется разброс этого показателя от регионов-лидеров до тех регионов, которым еще очень многое предстоит сделать.

На конец 2015 года на Едином портале госуслуг было 22,5 млн. пользователей, которые зарегистрированы в Единой системе идентификации и аутентификации (ЕСИА). В марте 2016 года эта цифра выросла — уже больше 25 млн. человек. Фактически, сегодня каждые три секунды регистрируется новый пользователь.



Подтвержденная регистрация, когда необходимо посмотреть дополнительные идентификационные документы гражданина, проводится и в органах власти, в отделениях «Почты России», в многофункциональных центрах, в офисах банков. К самым популярным услугам относятся проверка штрафов и оплата нарушений правил дорожного движения, вопросы налоговой задолженности, исполнительных производств, оформление загранпаспорта и информирование о состоянии лицевых счетов в системе пенсионного страхования. Сумма электронных платежей в 2015 году увеличилась в 3,5 раза и составила почти 3 млрд. рублей.

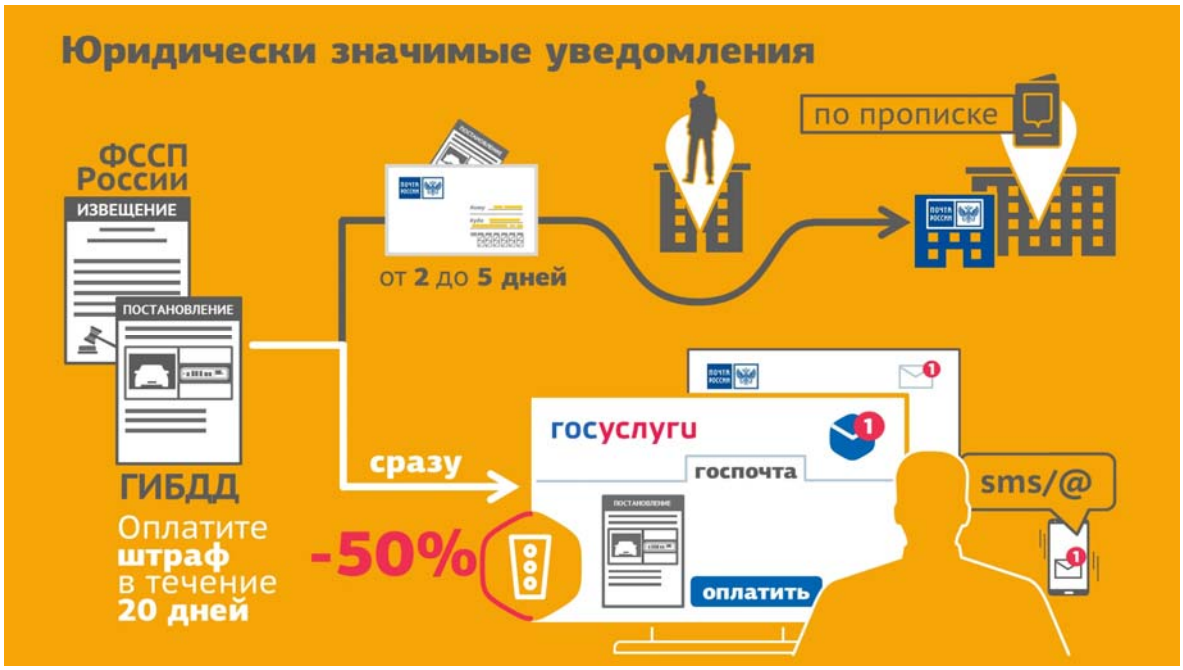
В 2015 году были продолжены работы по развитию бета-версии Единого портала госуслуг с оптимизированными интерфейсами, простыми и понятными даже для неподготовленных пользователей, в том числе в тех селах, куда приходит интернет благодаря программе устранения цифрового неравенства.



На сайте запущен каталог услуг с разбивкой по категориям. Электронные госуслуги доступны не только физическим и юридическим лицам, но и иностранным гражданам. Разделы сайта можно просматривать на нескольких языках. Примером взаимного проникновения государственных услуг и услуг хозяйствующих субъектов стали доступны на портале. Как наиболее яркий пример отметим такую услугу, как запрос о состоянии лицевого счета в системе обязательного пенсионного страхования и перенаправление этих данных в банк. Такой услугой воспользовались более 4,5 млн. раз — эти люди получили данную выписку и использовали ее для получения услуги в коммерческом секторе.

В рамках программы по увеличению распространения электронных госуслуг запущена в пилотную эксплуатацию «Открытая платформа госуслуг». Этот сервис позволяет предоставлять федеральные электронные госуслуги на порталах и сайтах федеральных и региональных органов власти с использованием встраиваемых элементов Единого портала госуслуг. Таким образом, сохраняется единый пользовательский опыт на одном сайте и увеличивается количество каналов доступа к государственным услугам в электронном виде.

В настоящее время запущен и успешно развивается проект по юридически значимым уведомлениям. Это пример реальной реформы, когда фактически меняется традиционный бумажный мир и переводится в электронную форму. Впервые в рамках пилотного проекта с Правительством Московской области, Министерством внутренних дел РФ, Федеральной службой судебных приставов и ФГУП «Почта России» удалось реализовать возможность, когда граждане фактически отказываются от получения бумажных писем, получают информацию в электронном виде, при этом сохраняется ее юридическая значимость. Соответственно, выполняются все регламенты и процедуры, предусмотренные действующим законодательством. Этот сервис уже хорошо отработан и может тиражироваться на другие регионы страны.



В 2015 году был серьезно доработан единый личный кабинет на сайте госуслуг. Запущен пилотный проект по интеграции ведомственных порталов. Однако сохраняется значительный уровень разобщенности. Необходимо продолжить практику единого личного кабинета и развивать её как единую точку и платформу для интеграции самых разных сервисов.

В Российской Федерации успешно развивается система межведомственного электронного взаимодействия. На текущий момент к СМЭВ подключено более 12 тысяч участников, из которых почти 100 участников федерального уровня. Количество обработанных запросов в СМЭВ составило около 7 млрд. единиц. Это значительно больше показателя 2014 года.

Согласно статистике, 80% услуг, оказанных в электронном виде, приходится на 35 видов услуг. Из них 20 региональных и муниципальных и 15 — федеральных. Это точка максимального внимания, в том числе и в рамках работы Правительственной комиссии по информационным технологиям.

Для того чтобы наша работа была правильно выстроена с точки зрения архитектуры, базовых основ, нам предстоит.

В 2015 году была инициирована работа по обновлению системного проекта электронного правительства. С точки зрения базовых принципов «Электронное правительство 2020» — это:

- высококачественные электронные услуги в режиме реального времени, со всех электронных устройств, в проактивном режиме, когда государство вам само напоминает, когда и что нужно сделать;
- снижение расходов всех уровней органов власти за счет использования сервисов электронного правительства не только для услуг, но и для функций;
- электронное гражданское общество, это такие сервисы, как «народный контроль», «народный инспектор», «активный гражданин» — они по-разному называются, но это становится стандартом фактического взаимодействия общества и государства;
- электронное правительство как платформа для бизнеса, и один из примеров по справкам из Пенсионного фонда, предоставляемых для банков.

Большое внимание по реализации указанныз услуг уделяется на Правительственной комиссии по ИТ и соответствующей подкомиссии по работе в части перевода услуг в электронный вид.

По инициативе Минкомсвязи России начат проект по популяризации электронных госуслуг. Впервые состоялась федерально-региональная информационная компания, которая охватила более 22 млн. человек. Для достижения показателя 70% по оказанию госуслуг в электронном виде необходимо эту работу усиливать.

В настоящее время госуслугами в электронном виде пользуются 35% населения страны. К 2018 году, согласно Указу Президента России, доля граждан, получающих услуги в электронном виде, должна составить 70%. Также в 2016 году 90% услуг должны оказываться по принципу «одного окна», а в 2018 году 90% жителей должны быть довольны качеством оказания государственных услуг.

В мае 2016 года состоялось заседание (http://www.minsvyaz.ru/ru/events/35147/) Подкомиссии по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности. Участники обсудили статус реализации сервиса «Открытая платформа госуслуг», основные показатели функционирования инфраструктуры электронного правительства (ИЭП), а также развитие региональной системы электронного правительства в Крымском Федеральном округе (КФО).

На заседании подкомиссии Минкомсвязь России доложила о статусе реализации проекта «Открытая платформа госуслуг». Сервис, запущенный в 2015 году, позволяет предоставлять федеральные электронные государственные услуги на порталах и сайтах федеральных и региональных органов исполнительной власти с использованием вспомогательных программных элементов (виджетов) Единого портала государственных и муниципальных услуг (ЕПГУ). Таким образом, пользователь может получать госуслуги на привычном ему портале. Также увеличивается количество каналов доступа к государственным услугам в электронном виде.

В настоящее время к сервису подключились Москва, Тюменская и Тульская области, а также Красноярский край и Хабаровский край. Они разместили на страницах сервиса виджеты популярных госуслуг «Проверка налоговых задолженностей» и «Узнай свой ИНН». В процессе подключения находится Архангельская область. Еще 19 субъектов РФ намерены присоединиться к «Открытой платформе».

Минкомсвязь России планирует дальнейшее развитие сервиса. Совместно с Федеральной налоговой службой (ФНС) сформирован план мероприятий по размещению виджетов услуг ФНС России на ЕПГУ посредством сервиса «Открытая платформа госуслуг». Запланировано расширение числа виджетов государственных услуг, уже разработан новый виджет услуги по оформлению загранпаспорта.

В рамках заседания подкомиссии был представлен регулярный отчет с показателями функционирования ИЭП. Сохраняется темп роста новых пользователей в системе, наметившийся с конца 2015 года, — более 1 млн человек в месяц.

В 36 субъектах РФ доля граждан, зарегистрированных в ЕСИА, превышает 20%. В числе лидеров с показателем выше 40% — Приморский край, Ханты-Мансийский автономный округ,

Тюменская и Калининградская области. В Чукотском автономном округе, Забайкальском крае, Республиках Дагестан, Ингушетия, Кабардино-Балкария и Крым, а также Севастополе данный показатель ниже 10%. Указанным регионам было рекомендовано принять меры по увеличению доли граждан в системе.

По состоянию на конец апреля 2016 года 54 субъекта РФ завершили интеграцию с системой межведомственного электронного взаимодействия (СМЭВ) 3.0. Остальным регионам также необходимо завершить эту работу.

На регулярной основе Минкомсвязь России проводит мониторинг уровня ошибок в работе электронных сервисов СМЭВ. Решением Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности в июле 2015 года установлен допустимый уровень таких ошибок — не более 1% от общего количества обращений. В данный момент 40 федеральных органов исполнительной власти (ФОИВ) не исполнили поручение, 12 ведомств не превышают допустимый показатель, 9 удалось достичь нулевого уровня ошибок. По итогам заседания подкомиссии ФОИВ дано поручение до 10 июня 2016 года снизить уровень ошибок до минимального.

Еще одной темой заседания стало развитие региональной системы электронного правительства в Крымском Федеральном округе в 2016 году. Минкомсвязь России в рамках реализации федеральной целевой программы «Социально-экономическое развитие Республики Крым и города Севастополя до 2020 года» разработала региональную систему электронного правительства. Новый функционал позволил выполнить 60% целевого показателя по доле сведений, находящихся в распоряжении органов власти КФО.

В 2016 году Минкомсвязь России продолжает развивать региональные системы электронного правительства и расширяет перечень сведений, доступных органам исполнительной власти субъектов КФО. Разработано техническое задание на развитие региональной системы электронного правительства. Документ позволит достичь целевого показателя по доле региональных сведений.

Также на подкомиссии одобрен план мероприятий по оптимизации приоритетных государственных услуг в сфере социальной защиты населения. План-график включает в себя оптимизацию ряда услуг, среди которых — прием заявлений, документов, а также постановка на учет граждан, нуждающихся в жилых помещениях, предоставление гражданам субсидий на оплату коммунальных услуг, назначение и выплата пособия на оплату проезда на общественном транспорте.

Оптимизация данных услуг позволит предоставлять их полностью в электронном виде, отменив необходимость посещать ведомства. Кроме того, это исключит ряд документов, ранее обязательных для предоставления услуги, а также снимет необходимость для физических лиц подтверждать доходы.

В 2015 году Минкомсвязи России запустило обновленную версию Единой межведомственной информационно-статистической системы (ЕМИСС). Сегодня это крупнейший поставщик данных для портала открытых данных. Пользователями ЕМИСС являются и ведомства и граждане. Такую же центральную роль выполняет и система управления кадровым составом. По состоянию на декабрь 2015 года 6,5 тыс. органов местного самоуправления, 2,5 тыс. органов

государственной власти субъектов РФ, 86 федеральных органов исполнительной власти подключены к системе и продолжается работа на базе инфраструктуры портала пилотной версии Единой информационной системы управления кадровым составом государственной гражданской службы РФ.

Продолжается проект по предоставлению субсидий регионам РФ на становление информационного общества, для которого были определены очередные приоритетные проекты. Объем финансирования суммарно составил 367 млн. рублей.

Республика Таджикистан

Внедрение в 2010 году системы биометрических паспортов, имеющих электронные чипы, считается первым шагом на пути электронизации государственных услуг.

В 2013 году, была осуществлена другая инициатива, а именно: внедрена система идентификационной карты, заменившей внутренний паспорт гражданина Республики Таджикистан.

Эти два шага, доказывая свою надежность, способствуют изготовлению документов на поездку в соответствии с международными требованиями, а также помогают при электронизации данных о гражданах.

В 2015 году в Республике Таджикистан принято решение о реализации ряда проектов по дальнейшему развитию системы электронизации государственных услуг, укреплению национальной безопасности путем создания единой системы управления государственной границей, а также по внедрению единой системы управления выдачи виз и для иностранных граждан - упрощенной системы получения виз посредством «электронных виз».

Реализация успешных проектов по внедрению «электронной визы» и электронной информационной системы визы Республики Таджикистан невозможна без создания соответствующей инфраструктуры в пограничной системе республики. Поэтому не только все посольства и консульские учреждения Республики Таджикистан за рубежом будут соединены с министерством, но и все пункты пропуска через государственную границу Республики Таджикистан будут соединены между собой и превратятся в единую систему управления.

Более того, все посольства и консульские учреждения республики за рубежом будут обеспечены специальной программой управления оформления визы, все пункты пропуска через государственную границу Республики Таджикистан будут обеспечены специальной программой въезда и выезда граждан республики и её гостей.

Следует отметить, что указанные объекты будут обеспечены сканерами отпечатков пальцев, оборудованием для чтения биометрических паспортов, фотооборудованием, сканерами для копирования и т.д. В конечном итоге, министерство будет располагать единой системой управления виз, а пограничники страны - единой системой пограничного управления.

В результате реализации этих проектов не только у Министерства иностранных дел и Пограничных войск, но и у органов безопасности и миграции в рамках их полномочий появится возможность для полного контроля и оперативного доступа к сведениям.

Более того, ожидается, что проект «электронной визы» даст серьезный импульс дальнейшему развитию электронизации государственных услуг.

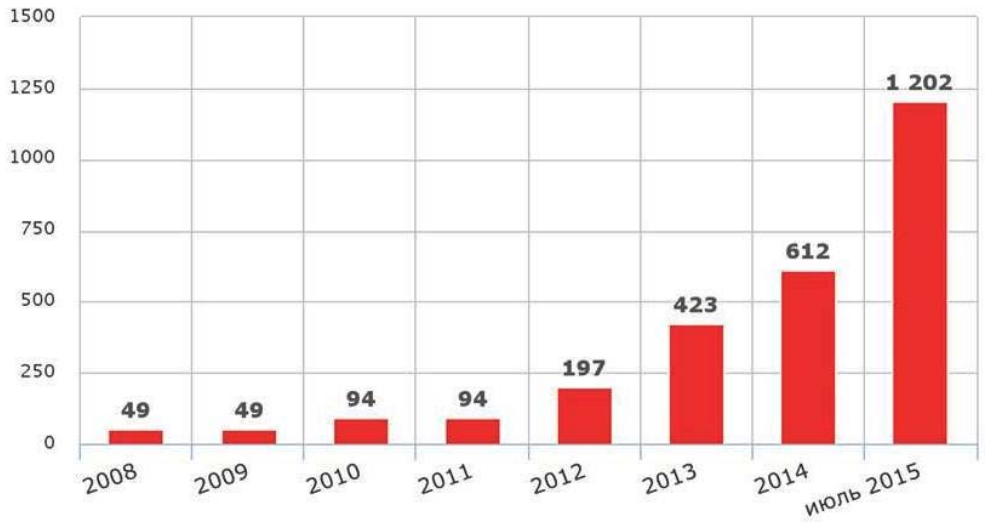
Преимущество реализации этого проекта связано с созданием упрощенных условий для туристов, участников конференций, симпозиумов, семинаров и лиц, прибывающих в Республику Таджикистан с целью участия на деловых переговорах. Внедрение электронной визы также создаст условия для граждан, совершающих поездки в Республику Таджикистан, стран, в чьих государствах отсутствуют посольства и консульские учреждения Республики Таджикистан, а также способствует устранению посредников и коррупционных факторов в процессе получения визы Республики Таджикистан.

В настоящее время ответственные регуляторы Республики Таджикистан вместе с крупной французской компанией прилагают усилия по реализации указанных планов в течение первого полугодия 2016 года.

Республика Узбекистан

Программа по развитию системы «Электронное правительство» включает разработку и принятие закона «Об электронном правительстве», разработка и утверждение стандартов и регламентов по межведомственному взаимодействию и обмену данными, формирование баз данных по различным направлениям, создание новых и интеграция существующих комплексов информационных систем в сфере государственных закупок, налогообложения, таможенного оформления, здравоохранения, образования и многих других.

Создан Центр развития системы «Электронное правительство» и Центра обеспечения информационной безопасности.



Количество видов государственных интерактивных услуг (ед.)

Предполагается внедрение единой платформы системы «Электронное правительство», которая будет являться основой для создания новых и интеграции действующих информационных систем.

Информационное взаимодействие государственных органов в системе «Электронное правительство» с юридическими и физическими лицами будет осуществляться через недавно запущенный в тестовом режиме Единый портал интерактивных государственных услуг, обеспечивающий доступ к сведениям об услугах и функциях государственных органов, предоставление пользователям возможности обмена данными в электронной форме, оформление запросов через единую точку доступа к интегрированным интерактивным государственным услугам.

Для идентификации пользователей системы «Электронное правительство» в программе предусмотрен проект по созданию Единой системы идентификации на базе инфраструктуры открытых ключей.

Ключевыми проектами программы развития системы «Электронное правительство» является формирование национальных баз данных и реестров: данные о физических и юридических лицах, данные о транспорте, кадастровая информация, недвижимость, единые справочники и классификаторы и т.д.

Для эффективного управления, учета и повышения информационной безопасности ведомственных информационных ресурсов и баз данных будет создан межведомственный государственный центр обработки данных системы «Электронное правительство», который должен обеспечить централизованное хранение и обработку ведомственных информационных ресурсов, а также интеграцию межведомственных информационных систем.

Таким образом, в результате внедрения системы «Электронное правительство» ожидается переход к полностью транзакционным услугам, которые исключают необходимость посещения разных инстанций и общения с госслужащими для получения государственных услуг населением

и представителями бизнеса, что в свою очередь будет способствовать созданию для них дополнительных удобств и улучшению условий ведения бизнеса.

В результате принятых мер по развитию интерактивных государственных услуг, в частности:

- количество пользователей ключей электронной цифровой подписи превысило 1,4 млн. ед.;
- количество государственных информационных ресурсов достигло 296 ед., а информационных систем 465 ед.

К Единому порталу интерактивных государственных услуг подключено более 600 государственных органов и оказывается более 250 интерактивных государственных услуг.

Узбекистан в рейтинге Организации Объединённых Наций (Документ под названием «The United Nations E-Government Survey : E-Government for the Future We Want») об использовании информационно-коммуникационных технологий (ИКТ) для предоставления гражданам государственных услуг занимает 100е место с индексом 0,4695 (по состоянию на 2014 год).

В целях дальнейшего развития и широкого внедрения в систему государственного управления современных информационных систем, ресурсов и баз данных Постановлением Президента Республики Узбекистан от 27.06.2013 г. утверждена Программа развития системы «Электронное правительство» на период 2013–2020 годов.

Программой предусматривается реализация проектов по созданию 6 центральных баз данных электронного правительства, 12 межведомственных комплексов информационных систем, строительство государственного дата-центра и другое (всего 28 проектов).

Согласно принятой концептуальной схеме организации системы «Электронное правительство» единой точкой доступа к интерактивным государственным услугам служит Единый портал интерактивных государственных услуг.

Архитектура системы «Электронное правительство» Республики Узбекистан

Вместе с этим, министерства и ведомства могут также оказывать услуги посредством своего официального веб-сайта. К Единому порталу интерактивных государственных услуг, а также веб-сайтам министерств и ведомств будут интегрированы различные создаваемые межведомственные комплексы информационных систем и базы данных посредством интеграционного шлюза электронного правительства.

Для координации реализации проектов электронного правительства создан Центр развития системы «Электронное правительство» и Центр обеспечения информационной безопасности, обеспечивающие единый технологический подход и информационную безопасность системы «Электронное правительство».

В результате принятых мер по развитию интерактивных государственных услуг, в частности:

- доля субъектов предпринимательства, сдающих налоговую и статистическую отчетность, а также оформляющих таможенные декларации в электронном виде, доведена до 100%;
- более 48 тыс. исковых заявлений и ходатайств поданы в хозяйственные суды в электронном виде;
- количество пользователей ключей электронной цифровой подписи превысило 1,4 млн. ед.;
- через единую систему бухгалтерской отчетности обслуживаются свыше 25 тыс. бюджетных организаций, имеющих более186 тыс. лицевых счетов;
- созданная площадка для осуществления государственных электронных закупок позволила с начала года сэкономить более 60,0 млрд. сумов;
- количество государственных информационных ресурсов достигло 296 ед., а информационных систем 465 ед.

1 июля 2013 г. создан Единый портал интерактивных государственных услуг (my.gov.uz), являющийся единой точкой доступа населения и субъектов предпринимательства к интерактивным государственным услугам государственных органов.

К Единому порталу подключено более 600 государственных органов и оказывается более 250 интерактивных государственных услуг.

На сегодняшний день подано более 323,3 тыс. заявок на получение интерактивных услуг, из которых 58% подано со стороны субъектов предпринимательства.

Самыми популярными интерактивными услугами являются:

- Представление данных по внешнеторговым контрактам в Единую электронную информационную систему внешнеторговых контрактов (подано более 167,8 тыс. заявок);
- Рассмотрение обращений (подано более 87,6 тыс. заявок);
- Онлайн-регистрация субъектов предпринимательства (подано более 36,2 тыс. заявок);
- Получение акта сверки по таможенным платежам (подано более 8,9 тыс. заявок);
- Выдача справок об отсутствии (наличии) судимости (подано более 6,6 тыс. заявок);
- Выдача архивных справок о подтверждении стажа работы (подано более 2,2 тыс. заявок);
- Выдача архивных справок о подтверждении заработной платы (подано более 1,3 тыс. заявок);
- Портал налогоплательщика, обеспечивающего прием и обработку электронной налоговой отчетности, которым уже пользуются 99% всех предпринимателей;
- Единый портал лицензиата, в котором доступна полная информация о перечне лицензируемых видов деятельности и разрешительных процедур, требуемых документах для получения лицензий и разрешений;
- Единый портал декларантов, через который с начала года 99% всех грузовых таможенных деклараций оформлено в электронном виде;
- В результате внедрения автоматизированной системы электронной статотчетности «eStat» доля резервирования фирменных наименований в электронном порядке достигла 97%;
- Портал коммунального хозяйства и жилищного фонда предоставляет целый спектр услуг в сфере ЖКХ, включая прием и обработку жалоб, оплату коммунальных услуг, а также информацию о тарифах;
- За счет внедрения информационной системы E-Visa доля оформленных иностранцам виз в Узбекистан в электронном виде превысила 90%;
- Более 35 тыс. исковых заявлений и ходатайств в хозяйственные суды были поданы в электронном виде через систему e-Sud.

Благодаря внедрению на Едином портале централизованной системы мониторинга оказания интерактивных услуг обеспечивается прозрачность процедур их оказания, а также мониторинг сроков рассмотрения заявлений и обращений.

10 марта 2015 года был запущен Портал открытых данных, который будет служить единой платформой для хранения открытых данных, т. е. систематизированных данных государственных

органов, организованных в формате, обеспечивающем их автоматическую обработку (в машиночитаемом виде).

На портале размещены сведения, обладающие высокой востребованностью среди физических и юридических лиц, информация о деятельности госорганов и статистические данные по основным сферам их деятельности, а также сведения из государственных информационных систем и ресурсов. Данные, публикуемые на портале, можно свободно и бессрочно воспроизводить, копировать, публиковать и передавать, а также использовать их в коммерческих целях, в том числе для создания различных программ и приложений.

На портале размещено уже 568 видов наборов открытых данных от 50 государственных органов, которыми пользователи воспользовались более 126 тыс. раз.

В целях совершенствования работы портала открытых данных, создания необходимых условий для обеспечения доступа к открытой информации о государственных органах и их деятельности Кабинетом Министров принято постановление «О мерах по дальнейшему совершенствованию Правительственного портала Республики Узбекистан в сети Интернет с учетом предоставления открытых данных» от 7 августа 2015 года.

Для создания массовых, социально значимых инновационных программ и сервисов на основе данных, полученных на портале и веб-страницах государственных органов Республики Узбекистан, представительством ООН в Узбекистане и Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан проводится хакатон (состязание). В дальнейшем хакатон будет способствовать популяризации идеи открытых данных среди программистов, дизайнеров-графиков, аналитиков, журналистов и менеджеров страны.

С 1 января 2015 г. на Едином портале функционирует система обсуждения разрабатываемых нормативно-правовых актов и оценки воздействия актов законодательства на предпринимательскую деятельность (СОВАЗ).

Оценка воздействия проектов, разрабатываемых и принятых нормативно-правовых актов на предпринимательскую деятельность путем их обсуждения на Едином портале позволяет систематически выявлять имеющиеся и возможные проблемы, сдерживающие развитие частного сектора, а также определить, какие именно меры следует принять в целях совершенствования деловой среды, установить приоритетность их принятия, исходя из степени важности выявленных проблем.

Учитывая большой спрос и активное участие населения и предпринимателей в обсуждении проектов нормативно-правовых актов, СОВАЗ с 14 мая 2015 г. мигрировала с Единого портала интерактивных государственных услуг на отдельную информационную систему (*regulation.gov.uz*), что позволило улучшить качество предоставления сервисов как пользователям, так и государственным органам (инициаторам проектов нормативных актов)

Согласно статистике в настоящее время:

В СОВАЗ размещено в общей сложности 194 проекта нормативно-правовых актов от 45 государственных органов, из них 11 ед. находятся в стадии обсуждения, по 170 ед. обсуждение завершено и 12 ед. утверждены с учетом мнений пользователей.

В общей сложности поступило 392 комментария, из них ответили на *149* комментариев (98 приняты и 51 отклонен).

С момента запуска СОВАЗ поступило 30 заполненных опросных листов по оценке действующих актов законодательства, из них новых 5 ед., рассмотрено 17 ед., на стадии рассмотрения 2 ед. и аннулированно 3 ед.

В целях информирования общественности о деятельности СОВАЗ в социальной сети facebook.com создана специальная страница, освещающая среди пользователей сведения о новых проектах нормативно-правовых актов.

В целях дальнейшего развития в республике производства программного обеспечения, усиления стимулирования отечественных разработчиков по расширению производства качественных, конкурентоспособных программных продуктов соответствующим решением Президента Республики Узбекистан разработчики программного обеспечения освобождены от уплаты всех видов налогов, обязательных отчислений, а также таможенных сборов до 1 января 2017 г.

В случае роста объема экспорта программного обеспечения не менее чем на 50%, указанные льготы продлеваются дополнительно на 2 года. Представленные преференции служат хорошим стимулом для разработки качественных, конкурентоспособных на внутреннем и внешнем рынках отечественных программных продуктов.

Количество компаний-разработчиков программного обеспечения в республике увеличилось до 294 ед., а за счет принимаемых мер по созданию благоприятных условий развития рынка программных продуктов объем оказанных услуг по компьютерному программированию в республике за январь–август 2015 года превысил 145,9 млрд. сумов.

Правительством республики уделяется особое внимание вопросам ускоренного развития и широкого внедрения в отраслях реальной экономики информационно-коммуникационных технологий и программных продуктов и на этой основе повышения эффективности управления, снижения издержек производства, обеспечения прозрачности финансово-хозяйственной деятельности хозяйственных объединений и крупных предприятий, повышения их конкурентоспособности на внутреннем и внешних рынках.

Украина

Единый государственный портал административных услуг Украины утвержден постановлением кабинета министров Украины 3 января 2013 г. В настоящее время (2015 год) портал находится в режиме тестирования. Этот портал создан для того, чтобы пользователи могли получить доступ к любой информации об административных услугах, их перечню, органах, которые их оказывают, и документах, которые их регулируют. Также, с помощью этого сайта пользователи смогут загружать и заполнять заявления на услуги от украинских госорганов, а также отсылать их через интернет.

Похожие проекты на местном уровне на Украине уже разрабатывались ранее. Так еще в 2011 году в г.Киеве был запущен городской портал административных услуг. В настоящее время киевский портал интегрирован с единым порталом, и со временем предполагается, что все подобные локальные ресурсы также в него войдут, так что он превратится в общую точку доступа к государственным услугам.

Так же с 2013 года на Украине работает система электронного обращения граждан. Сообщается, что с помощью системы можно подавать обращения в органы государственной власти и местного самоуправления, при наличии электронной подписи. Кроме того, физические и юридические лица получили возможность отправки запросов на получение публичной информации. Сообщается, что госсистема нацелена на повышение качества и прозрачности процесса обработки обращений граждан и запросов на публичную информацию.

16 июня 2015 года органы государственной власти Украины и волонтеры начали внедрение системы оказания электронных услуг. Результат совместной работы – портал государственных услуг iGov.org.ua презентован во время пресс-брифинга в Украинском кризисном медиа-центре.

По информации представителя Администрации Президента Украины, Закон «Об административных услугах» был принят еще в 2012 году, и внедрением занималось Министерство экономического развития, однако портал не был запущен. Но гражданское общество и бизнес активно приобщились к развитию он-лайн услуг на Украине и созданию конкретных ресурсов. Это модель, когда граждане приобщаются к созданию информационных ресурсов, а государство обязуется их использовать, не тратя на это государственные средства. «Такое распределение является классическим примером частно-государственного партнерства, и сегодня эта модель эффективно работает и быстро приносит результат. Проблема в том, что законодатели не успевают за современными технологиями, они не должны сдерживать продвижение электронных технологий», – отметил представитель Администрации Президента Украины.

Председатель Государственного агентства по вопросам электронного управления пояснил, что первые два этапа развития электронных услуг внедрены. Речь идет о доступе к информации относительно порядка предоставления услуг, а также возможности доступа к электронным формам документов. С введением следующих двух этапов есть проблемы. Речь идет о том, что учреждения пока не готовы принимать документы в электронном виде. И следует настроить полную автоматизацию всех процедур: информирование, результат, оплата. «То, что существует сейчас, это регистрационный портал, кабинет административных услуг, электронный кабинет налогоплательщика, а также электронные разрешения в строительстве», – пояснил Председатель Государственного агентства по вопросам электронного управления.

Заместитель председателя правления ПриватБанка пояснил, что на призыв принять участие в создании iGov.org.ua откликнулось около тысячи волонтеров-специалистов в области IT. «Сам продукт, если бы его делал бизнес, стоил бы миллионы долларов, но это сделали волонтеры», – пояснил он. На портале собраны почти все услуги, которые предоставляет государство гражданам и бизнесу. 9 услуг уже доступно онлайн, 47 – планируется внедрить в ближайшем будущем, а 492 услуги прорабатываются на перспективу. «В настоящее время около 60 различных государственных органов, как центрального уровня, так и местного, работают с нами по внедрению своих услуг», – отметил Заместитель председателя правления ПриватБанка.

Например, жители Днепропетровска теперь могут заказать он-лайн такую услугу, как получение справки о несудимости. Достаточно в поисковой базе портала найти эту услугу и заполнить бланк он-лайн.

В настоящее время уже доступны некоторые услуги в Государственном агентстве строительства и Министерстве экологии Украины. В течение следующих месяцев планируется запустить регистрацию автомобиля в МРЭО. «Эта услуга заняла первое место в голосовании по желаемым услугам он-лайн для внедрения в первую очередь. И в течение одной-двух недель мы

запускаем пилотный проект в Киеве и Днепропетровске», – анонсировал Заместитель председателя правления ПриватБанка. Также в планах внедрение услуги он-лайн получения загранпаспорта, формы №4 в Министерстве юстиции Украины и других услуг. До конца 2015 года 20% государственных услуг должны бали быть переведены в электронный вид.

Если гражданин не нашел необходимую ему услугу в поисковой базе портала, можно заполнить форму, и она будет добавлена к порталу. Срок введения электронных услуг зависит от готовности самих учреждений и регионов к внедрению новейших технологий.

Правительство Украины заявляет о готовности содействовать в развитии ИТ-технологий и планирует создать так называемую «IT-диспетчерскую», которая будет ускорять внедрение указанных инициатив, и будет способствовать созданию украинского национального G-Store, как, например, App Store, Google Play, чтобы пользователям, как гражданам, так и бизнесу, было удобно добраться до этих услуг.

4. Защита детей в «online» среде

Международным союзом электросвязи и командой авторов из ведущих организаций, работающих в отрасли информационно-коммуникационных технологий и занимающихся проблемами защиты детей, были подготовлены Руководящие указания для директивных органов по защите ребенка в онлайновой среде в 2009 году. Эти Руководящие указания подготовлены в рамках инициативы Защита ребенка в онлайновой среде (COP), для того чтобы создать основу безопасного и защищенного кибермира для будущих поколений. Предполагается, что они будут действовать в качестве плана, который может быть адаптирован и использован таким образом, который согласуется с национальными или местными обычаями и законами. Кроме того, их ценность повышается от того, что эти Руководящие указания рассматривают вопросы, которые могут влиять на всех детей и молодых людей, не достигших 18 лет, но каждая возрастная группа будет иметь свои потребности.

Инициатива МСЭ «Защита детей в онлайновой среде» содействует пониманию рисков для детей и поощряет обмен знаниями о соответствующих инструментах между практическими работниками. МСЭ и Детский фонд Организации Объединенных Наций опубликовали в 2014 году новые руководящие принципы для промышленности, касающиеся защиты детей в онлайновой среде, а Детский фонд Организации Объединенных Наций опубликовал исследова- ние, озаглавленное «Дети, ИКТ и развитие в 2013 году», в котором рассматривается ряд возможностей, проблем и угроз, связанных с детьми в изменяющейся цифровой среде.

Ниже приведён краткий анализ ситуации с принимаемыми мерами по защите детей в онлайновой среде в странах СНГ и Грузии.

Республика Азербайджан

В настоящее время в Республике Азербайджан нет никакого конкретно посвященного Интернету законодательства, касающегося онлайн-контента. Вслед за Россией, государственные органы предложили установить более обширный фильтрационный режим, для защиты детей от вредного контента и преследования детской порнографии.

Очень большое количество развивающихся стран подали заявки в МСЭ на продолжение работ по созданию потенциала (capacity building). Во многих развивающихся странах ИКТ-потенциал настолько невелик, что правительства даже не начинали думать о разработке собственных политических позиций по таким вопросам, как защита ребенка в онлайновой среде, кибербезопасность и управление Интернетом. Поэтому такие правительства часто полагаются на МСЭ или G77 (Group of Seventy Seven, межгосударственная организация развивающихся стран), чтобы получить помощь в том, как продвигать ИКТ в пределах своих границ. Это не значит, что их заявления являются менее важными. Но это значит, однако, что не все государства-члены МСЭ участвуют или заинтересованы в политических дебатах на ПК-14. Если дойдёт до голосования, эти делегации могут объединиться с G77.

МСЭ совместно с Всемирным банком, Всемирным экономическим форумом и Интерполом также оказал поддержку правительству Азербайджана в организации международной конференции по вопросам кибербезопасности в 2013 году.

Республика Армения

Защита ребенка в онлайновой среде в эру общедоступного широкополосного интернета является важнейшей проблемой, которая срочно требует глобальной скоординированной реакции. Дети и молодые люди в онлайновой среде часто бывают особенно уязвимыми. При поддержке Интерпола и компании Microsoft, Международный центр по пропавшим без вести и эксплуатируемым детям (ICMEC) сделал обзор законодательства по детской порнографии, по которой можно судить о ситуации в Республике Армения. Армения в свою очередь делает всё возможное, чтобы обезопасить детей в своей стране.

Страна	Специальное законодательство по детской порнографии	Определение «детской порнографии»	Преступления, совершенные с использованием компьютера	Владение материалами	Сообщения поставщиков интернет-услуг (ISP)
Республика Армения	Да	Нет	Да	Нет	Нет

В настоящее время в стране принято специальное законодательство по детской порнографии, наказываются преступления, совершённые с использованием компьютера.

Однако в нормативно-правовых актах не дано определение «детской порнографии», не преследуется по закону просто владение порнографией и поставщики услуг интернета (ISP), предоставляющие доступ к сайтам с порнографической информацией.

Республика Беларусь

В Республике Беларусь введена возрастная маркировка информационной продукции.

Проект Закона «О внесении дополнений и изменений в некоторые законы Республики Беларусь» (первоначально назывался «О внесении изменений и дополнений в некоторые законы Республики Беларусь по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию») предполагает разделить всю информационную продукцию в зависимости от ее воздействия на психику детей. Сама по себе идея не является, новой, поскольку подобным образом маркируются кинофильмы.

Предлагается ввести комплекс мер по защите детей от информации, причиняющей вред здоровью и развитию ребенка, определяющий условия распространения информационной продукции и предоставления ряда услуг по доступу к информации. В частности, обязать изготовителей и распространителей маркировать информационную продукцию знаком возрастной категории (звуковым или визуальным предупреждением), указывающим, среди детей какого возраста допустимо распространение данной продукции. Для информации, распространяемой через интернет, норма будет носить лишь рекомендательный характер.

Изготовителей и распространителей информационной продукции обяжут соблюдать ограничение периода суток, в течение которого допускается распространение информации, способной причинить вред здоровью и развитию ребенка (например, с 4.00 до 23.00). При предоставлении доступа к интернет-услугам потребуется информировать пользователей о существующих средствах и способах контроля за содержанием информационной продукции, распространяемой через интернет.

По информации Постоянной комиссии по правам человека, национальным отношениям и средствам массовой информации Палаты представителей, критерии отнесения информационной продукции к той или иной возрастной категории будут определены отдельным постановлением Совета Министров.

Для координации действий в сфере защиты детей от потенциально вредной информации законопроект предлагает создать общественно-консультационный совет при Правительстве Республики Беларусь.

Законопроект направлен на реализацию международных обязательств государства по обеспечению защиты ребенка от информации и материалов, наносящих вред его благополучию, и установлению необходимых ограничений в распространении информации, содержащей насилие, жестокость, поощряющей прием наркотиков или имеющей порнографическое содержание.

В связи с этим предлагается также внести корректировки в законы «О правах ребенка», «О рекламе», «О средствах массовой информации», «Об информации, информатизации и защите информации», «Аб выдавецкай справе ў Беларусі».

Грузия

Проблемой защиты детей в сети Интернет Грузия, вместе со странами СНГ начала заниматься еще в конце 90-х годов прошлого столетия. Все без исключения страны региона СНГ присоединились к Конвенции о правах ребёнка без каких-либо заявлений и оговорок к статьям 16, 17 и 34 (c). Также были подписаны и ратифицированы Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии. При этом, базируясь на международных нормативных документах, законодательство отдельных стран

в области защиты детей имеет некоторое различие. Уголовным кодексом Грузии предусмотрено наказание за преступления связанные с эксплуатацией детей в онлайн-среде (статьи 255 и 255.1).

Следует отметить, что организация CERT Грузии, а также некоторые неправительственные организации создали механизмы для оповещения про инциденты связанные с защитой детей в сети Интернет.

Республика Казахстан

В настоящее время в Республике Казахстан нет четкого законодательного регламента, оговаривающего защиту детей в Интернете. Правительством рассматривался проект закона о Защите детей от вредной информации, однако он был признан не соответствующим конституции Республики Казахстан. Родителям, желающим защитить своих детей в интернете приходится полгаться на функции родительского контроля, предоставляемы провайдерами и защитное ПО третьих лиц.

В 2015 году принят проект закона Республики Казахстан «О защите детей от информации, причиняющей вред их здоровью и развитию». Под распространением информационной продукции будем понимать деятельность распространителя информационной продукции, а равно иные действия, направленные на ознакомление с информационной продукцией, неопределенного круга лиц любым способом, включая продажу (подписка, доставка, раздача), аренду, прокат, рекламирование, выход в эфир радио-, телепрограмм, демонстрация, в том числе посредством кабельного и эфирно-кабельного вещания, зрелищных мероприятий, размещение на интернет-ресурсах.

Законом Республики Казахстан «О защите детей от информации, причиняющей вред их здоровью и развитию» предусматривается маркировка информационной продукции и требования к обороту информационной продукции в соответствии с возрастными категориями информационной продукции. Маркировка информационной продукции осуществляется ее производителем и (или) ее распространителем посредством нанесения соответствующего знака возрастной категории информационной продукции:

1) «до 6 лет» – знак «6–» в окружности;

2) «с 6 лет» – знак «6+» в окружности;

3) «с 12 лет» – знак «12+» в окружности;

4) «с 16 лет» – знак «16+» в окружности;

5) «с 18 лет» – знак «18+» в ромбе.

Маркировка компьютерных и иных электронных игр, включая маркировку на экране игры онлайн в Интернете и игры для технических устройств телефонной мобильной (сотовой) связи, осуществляется в порядке, установленном уполномоченным органом исполнительной власти государства. Маркировка компьютерных и иных электронных игр кроме сведений о возрастной категории информационной продукции игры должна содержать предупреждение о необходимости обратиться за медицинской помощью в случае возникновения игровой зависимости.

Предусмотрены специальные требования к распространению информационной продукции с использованием информационно-коммуникационных сетей:

- Доступ детей к информационной продукции, распространяемой с использованием информационно-коммуникационных сетей общего пользования (в том числе Интернет-ресурсов) в образовательных учреждениях, реализующих учебные программы дошкольного воспитания и обучения, начального, основного среднего, общего среднего образования, профессиональные учебные программы технического и профессионального, послесреднего, высшего и послевузовского образования, а также в иных организациях, предоставляющих услуги Интернет-ресурсов, независимо от их формы собственности и организационно-правовой формы, разрешается при условии применения указанными организациями аппаратно-программных, технико-технологических и иных средств, обеспечивающих информационную безопасность детей;
- Организации, предоставляющие услуги пользования информационно-коммуникационными сетями (в том числе Интернет-ресурсов), вправе применять не запрещенные законодательством Республики Казахстан меры для установления возраста лица, которому предоставляются указанные услуги.

Также предусмотрены дополнительные требования к распространению компьютерных и иных электронных игр:

1. В компьютерных и иных электронных играх (включая игры онлайн в Интернет-ресурсах), игры на игровых консолях, игры для технических устройств сотовой связи, находящихся в обороте на территории Республики Казахстан, запрещается использование скрытых вставок и иных технических приемов и способов распространения информации, воздействующих на подсознание ребенка или оказывающих вредное влияние на его здоровье и развитие (включая приемы и средства гиперстимуляции восприятия информации и сенсорной агрессии у пользователей игры), в том числе модулей скрытой функциональности, скрытых бонусов, позволяющих активировать игровые эпизоды либо иным образом получать доступ к информационной продукции, запрещенной для оборота среди детей в соответствии с настоящим Законом или иными Законами Республики Казахстан.

2. На территории Республики Казахстан не допускается распространение среди детей компьютерных и иных электронных игр, содержащих сюжеты:

- провоцирующие ребенка на пренебрежительное или негативное отношение к физическим недостаткам других людей, на агрессивные насильственные и иные антиобщественные действия, в том числе вызывающие у него проявления агрессии и жестокости по отношению к персонажам игры или партнерам по игре;
- связанные с возможностью совершения игроком виртуальных убийств и нанесения виртуальных увечий персонажам игры, в том числе сопряженные с натуралистическим изображением человеческой крови;
- сопряженные с натуралистическим изображением или моделированием бесчеловечного обращения, связанного с причинением особых физических или психических страданий человеку (а равно существу, имеющему явное сходство с человеком) или животному, включая пытки, истязания, мучения, глумление, применение особо жестоких способов нанесения увечий и лишения жизни;
- эксплуатирующие интерес к сексу, натуралистично изображающие, моделирующие или имитирующие половые органы, половые сношения или иные действия сексуального

характера, в том числе с использованием реальных или виртуальных образов человека, животных или существ, имеющих явное сходство с человеком, либо несущие в себе иную информацию сексуального характера, способную вызвать у детей – пользователей игры не соответствующий возрастной норме интерес к сексуальным проблемам, в том числе содержащие изображения или моделирующие сцены изнасилования или иных насильственных действий сексуального характера, изображения сексуальной эксплуатации детей и любых иных действий сексуального характера в отношении ребенка, а также использование голоса и облика ребенка в сексуальных сюжетах;

- способные вызвать появление у детей повторяющихся страхов, паники или внушающие им ужас, в том числе детально моделирующие или натуралистично изображающие оккультно-мистические практики или магические ритуалы; акты вскрытия человеческого тела, самоубийства, членовредительства; физиологические подробности процесса и последствий смерти или предсмертной агонии живых существ; устрашающие последствия несчастных случаев, аварий, катастроф (травмы, увечья, следы обильного кровотечения, трупы, искалеченные тела или ампутированные части тел людей или животных, следы кровопролития).

3. Провайдеры услуг Интернет-ресурсов и сетей сотовой радиотелефонной связи, владельцы и администраторы пунктов коллективного доступа к Интернет-ресурсам обязаны обеспечивать применительно к многопользовательским онлайн играм соблюдение предусмотренных настоящим Законом возрастных ограничений в доступе к таким играм детей.

В Законе также предусмотрено, что в печатной продукции, аудио-, кино- и видеопродукции, предназначенной для детей, не допускается размещение объявлений о проведении отбора детей, а равно фото-, кино- и видеосъемок, конкурсов, зрелищных мероприятий или иных объявлений, содержащих информацию, причиняющую вред здоровью и развитию детей, в том числе предусматривающих участие детей в обороте информационной продукции, отнесенной настоящим Законом к категории «с 18 лет», ограничивается доступ детей к указанной информации, распространяемой с использованием информационно-коммуникационных сетей общего пользования (включая Интернет-ресурсы и сети сотовой связи).

Кыргызская Республика

На Всемирной конференции по развитию электросвязи 2014 г. (ВКРЭ-14) было принято, что необходимо создать центр по защите ребенка в онлайновой среде для региона СНГ (в том числе и Киргизии) в рамках региональной инициативы. Ее целью является обеспечение государств – членов МСЭ региона централизованной консультационной и технической помощью по различным аспектам защиты ребенка в онлайновой среде. Но также безопасность работы в интернете зависит от учителей, родителей и самих детей.

Республика Молдова

Основным документом является Кодекс телевидения и радио Республики Молдова от 27 июля 2006 года 260-XVI (с изменениями и дополнениями по состоянию на 17.09.2010 года) (далее - Кодекс).

Кодексом запрещается распространение программ, могущих нанести значительный вред физическому, умственному или нравственному развитию несовершеннолетних, в частности содержащих порнографию, чрезмерное насилие и ненормативную лексику. Трансляция иных программ, способных повлиять на психическое, умственное или нравственное развитие несовершеннолетних, может производиться только в случае обеспечения (путем выбора времени вещания или при помощи технических средств) условий для того, чтобы находящиеся в зоне покрытия несовершеннолетие не могли смотреть и слушать соответствующие передачи.

Реклама, в том числе в целях самопродвижения, и телеторговля должны не оказывать негативного влияния на физическое, психическое и нравственное развитие несовершеннолетних. Реклама и телеторговля спиртными напитками не должны предназначаться несовершеннолетним или изображать их потребляющими спиртные напитки.

Чтобы не причинять вреда физическому, психическому и нравственному развитию несовершеннолетних, реклама и телеторговля не должны:

a) эксплуатировать неопытность и доверчивость несовершеннолетних с целью спровоцировать их на покупку определенных товаров или услуг;

b) прямо провоцировать несовершеннолетних на оказание давления на родителей или других лиц с целью приобретения рекламируемых товаров или услуг;

c) эксплуатировать особое доверие несовершеннолетних к родителям, учителям и другим лицам;

d) необоснованно изображать несовершеннолетних в опасных ситуациях.

Телеторговля должна не провоцировать несовершеннолетних на заключение договоров купли-продажи или аренды имущества или услуг.

Новые риски возникают в результате развития и расширения доступа к современным информационным технологиям. Исследование о безопасности детей, пользующихся услугами Интернета, «Дети Республики Молдова одни и в безопасности в режиме он-лайн» (2011) предупреждает о том, что приставание к детям в Интернете также ведет к совершению конвенционных преступлений, позволяя преступникам легко обнаруживать местонахождение потенциальных жертв через других преступников по всему миру.

Проведенное в Республике Молдова исследование относительно безопасности детей в Интернете показало, что 10% детей подключаются к Интернету ночью, с 22.00 до 08.00; более 39% респондентов заявили, что находятся в Интернете 3-4 часа в день, а 6% - 7-8 часов и более. Еще большее беспокойство вызывают данные о том, с кем общаются дети: 51% опрошенных детей встречались в реальной жизни с людьми, с которыми познакомились в Интернете, и около 20% из них никому не сообщали об этом; другие 38% публично указывали свои личные данные и фотографии тем, с кем познакомились в Интернете. 7% детей, познакомившихся по Интернету с

людьми из других стран, сообщили, что получали непристойные предложения и обсуждали темы сексуального характера.

Единственная мера по решению этой проблемы в Стратегии защиты ребенка на 2014-2020 годы: обеспечение защиты детей от информации на любых существующих носителях, способной отрицательно повлиять на психическое и моральное состояние детей.

Российская Федерация

Стремительное развитие информационных технологий заставило современное поколение детей и подростков столкнуться с принципиально новыми вызовами. Взросление, обучение и социализация детей проходят в условиях гиперинформационного общества.

Процесс социализации через традиционные институты (семьи, школы) все активнее дополняется средствами массовой информации и массовых коммуникаций, особенно информационно-телекоммуникационной сетью «Интернет», которые становятся важнейшими институтами социализации, образования и просвещения нового поколения, в определенной мере замещая традиционно сложившиеся формы. Главным образом это происходит в тех случаях, когда родители (законные представители) в семье отстраняются от своих обязанностей по воспитанию и развитию детей и перекладывают их на внешних игроков.

При разумном и эффективном сотрудничестве общественных и государственных институтов информационные и коммуникационные технологии могут быть ключевыми элементами политики, способствующими сохранению культуры России, укреплению нравственных и патриотических принципов в общественном сознании, а также развитию системы культурного и гуманитарного просвещения.

В настоящее время в РФ существует специализированный закон, согласно которому дети должны быть защищены от информации определённого рода. Это нормативный акт, предусматривающий отнесение информационной продукции к одной из пяти категорий, и запрещающий её распространение среди детей в зависимости от их возраста (Федеральный закон от 28.07.2012 N 139-ФЗ (ред. от 14.10.2014) «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации»).

Указом Президента России от 1 июня 2012 года №761 утверждена Национальная стратегия действий в интересах детей на 2012–2017 годы, одно из основных направлений реализации которой – обеспечение информационной безопасности детей.

Правительство Российской Федерации 2 декабря 2015 года приняло Распоряжение № 2471-р, которым утвердило «Концепцию информационной безопасности детей». Указанное Распоряжение включает в себя:

- Общие положения;
- Основные принципы обеспечения информационной безопасности детей;
- Приоритетные задачи государственной политики в области информационной безопасности детей;

- Механизмы реализации государственной политики в области информационной безопасности детей;
- Ожидаемые результаты.

Данное распоряжение «будет способствовать реализации единой государственной политики в области информационной безопасности детей, созданию современной медиасреды, учитывающей риски, связанные с развитием интернета и информационных технологий».

В нем отмечается, что положения концепции базируются на принципах признания детей и подростков активными участниками информационного процесса, ответственности государства за соблюдение законных интересов детей в информационной сфере, воспитания у детей навыков самостоятельного и критического мышления, создания в информационной среде благоприятной атмосферы для детей и подростков вне зависимости от их социального положения, религиозной и этнической принадлежности.

Приведём некоторые статистические данные о поведении детей в сети Интернет и технические средства по их защите. По данным исследований «Лаборатории Касперского» в 2014 году дети из России посещали следующие сайты:

- Социальные сети (59,6%);
- Интернет – магазины (9,1%);
- Порнография, эротика (8,8%);
- Почта (5,7%);
- Нелегальное ПО (3,4%).

Эксперты «Лаборатории Касперского» отметили, что среди остальных стран Россия лидирует по количеству детей, посещающих социальные сети.

В России по данным того же исследования 70% детей 9-10 лет и свыше 90% школьников старше 13 лет пользуются Интернетом без надзора старших. По данным «Лаборатории Касперского», дети изучают «запрещенные ресурсы» в часы, когда уроки уже закончились, а родители еще не пришли с работы, то есть с 15 до 17 часов.

По данным исследования «Института семейной безопасности в Интернете» об осведомленности, отношении и использовании функции «Родительского контроля», проблема безопасности в Интернете не является предметом повышенного внимания родителей.

Подавляющее большинство (86%) сообщили, что считают нахождение ребенка в интернете абсолютно (42%) и достаточно (44%) безопасным. И только 13% родителей признались, что сетевая активность детей очень (3%) и несколько (10%) небезопасна. Из опрошенных родителей 53% сообщили, что они использовали настройки или программное обеспечение для контроля или ограничения деятельности детей в Интернете.

Из технических средств защиты детей в сети Интернет для Российской Федерации можно назвать следующие:

1. «Родительский контроль» от антивирусных вендоров. «Родительский контроль» включает в себя стандартный набор функций, а именно:

- Ограничение времени нахождения ребенка в сети;

- Ограничение времени пользования компьютером;
- Возможность создания графики с допустимыми часами работы в течение дня;
- Блокировка сайтов с запрещенным контентом – создание «чёрных» списков на основе баз данных антивирусного производителя по категориям (наркотики, социальные сети и т.д.) и создание «белых списков» родителем;
- Ограничение на запуск приложений (например, игр) и установку новых программ; - возможность следить за перепиской ребенка в соцсетях и чатах (ICQ, Skype) и контролировать пересылку личной информации (в основном, это платные пакеты услуг).

В качестве примера можно привести разработку российской компании Etensys - программу KinderGate. Некоторые ресурсы сравнивают функциональность этой недорогой программы с «Родительским контролем» известных вендоров. KinderGate неоднократно занимала первые места в списках рейтингов, так что если вы пользуетесь антивирусом без встроенного «Родительского контроля», то эта программа может стать для вас хорошим решением.

2. Операционные системы

В операционных системах Microsoft Windows и Apple iOS автоматически встроены функции «Родительского контроля». Изучив настройки, можно назначить ребенка отдельным пользователем со своим паролем и задать ему ограничения – например, по времени использования компьютера, блокировку новых программ, а так же возможность отслеживать действия ребенка в Интернете после приобретения им дополнительных приложений. Дополнительные функции Windows7 позволяют родителю настроить «Безопасный поиск», который задействует механизмы фильтрации поисковых систем в Интернете, таких как google.ru и yandex.ru.

3. «Родительский контроль» от провайдера

Провайдеры со своей стороны предоставляют схожие услуги. Например, МГТС предлагает родителям вводить ограничения по времени пребывания в Интернете ребенка в их отсутствие, предоставляет отчеты о просмотренных сайтах. Из минусов этой системы – возможность ребенком при наличии данных, например, номера договора, получить пароль для изменения настроек в личном кабинете. При входе в личный кабинет интересующийся родитель сразу же увидит произошедшие изменения и сможет самостоятельно принять меры.

Реализация «Концепции информационной безопасности детей» обеспечит в 2020 году формирование в Российской Федерации поколения молодых граждан, которые смогут свободно и самостоятельно ориентироваться в современном информационном пространстве. Будет создана новая медиасреда, соответствующая следующим характеристикам:

- наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;
- свободный доступ детей к историко-культурному наследию предшествующих поколений;
- качественный рост уровня медиаграмотности детей;

- увеличение числа детей, разделяющих ценности патриотизма;
- гармонизация меж- и внутрипоколенческих отношений;
- популяризация здорового образа жизни среди молодого поколения;
- формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов;
- снижение уровня противоправного и преступного поведения среди детей;
- формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования «пиратского» контента.

Республика Таджикистан

Защита ребенка в онлайновой среде в эру общедоступного широкополосного интернета является важнейшей проблемой, которая срочно требует глобальной скоординированной реакции. Все больше людей присоединяются к сети сегодня, причем очень часто первыми это делают дети и молодые люди, которые часто бывают особенно уязвимыми.

Существует множество проблем, связанных с использованием интернета детьми и молодыми людьми, которые постоянно беспокоят как родителей, так и детей, а также правительства, политиков и директивные органы. Области этой озабоченности можно сформулировать следующим образом:

- Контент;
- Контакты;
- Поведение;
- Торговля;
- Чрезмерное использование;
- Общественная жизнь.

При поддержке Интерпола и компании Microsoft, Международный центр по пропавшим без вести и эксплуатируемым детям (ICMEC) сделал обзор законодательства по детской порнографии в 187 странах – членах Интерпола.

Ниже приведено состояние существующего законодательства по детской порнографии в Республике Таджикистан.

Страна	Специальное законодательство по детской порнографии	Определение «детской порнографии»	Преступления, совершенные с использованием компьютера	Владение материалами	Сообщения поставщиков интернет-услуг (ISP)
Республика Таджикистан	Да	Нет	Нет	Нет	Нет

Из приведенной таблицы видно, что Республика Таджикистан имеет законодательство, касающееся специально детской порнографии, но:

- не дает в своем законодательстве определения детской порнографии;
- не предусматривает ответственности за преступления, совершенные с помощью компьютера;
- не квалифицирует как уголовное преступление владение материалами детской порнографии, независимо от наличия намерения их распространять;
- не отвечает критерию, относящемуся к информированию со стороны провайдеров интернет-услуг.

Республика Узбекистан

Президент Узбекистана 19 февраля 2014 года своим постановлением утвердил государственную программу «Год здорового ребенка». В связи с чем в 2014 году приступили к разработке закона «О защите детей от информации, оказывающей вредное воздействие на их физическое и духовное развитие».

Проект закона с учетом современных стандартов возрастной классификации информационной продукции будет устанавливать ограничения на распространение определенных видов информации для конкретных возрастных категорий детей, определять механизмы защиты детей от вредного информационного воздействия, в том числе с использованием глобальной сети Интернет, влияния элементов «массовой культуры» и других информационных угроз на общественное сознание.

Нижняя палата парламента Узбекистана приняла закон "О защите детей от информации, оказывающей вредное воздействие на их физическое и духовное развитие".

После всестороннего рассмотрения депутаты одобрили основные положения законопроекта и приняли документ в первом чтении, документ направлен на утверждение в Сенат (верхнюю палату парламента), где он рассмотрен в начале 2015 года.

В ходе разработки закона был изучен опыт России, учитывая, сопоставимость существующего контента для детей и общий рынок ее распространения.

Закон предусматривает ряд ограничений для публикации материалов в СМИ. В соответствии с документом, контент СМИ должен быть промаркирован по нескольким степеням ограничения: "6+", "12+", "16+" и "18+". Законопроект запрещает использовать в школах и других образовательных учреждениях учебники и пособия, содержащие вредную информацию, уточнил представитель парламента. Кроме того, закон будет контролировать распространение электронных игр, пропагандирующих насилие, жестокость, наркоманию и порнографию.

В Узбекистане, где 40% населения составляет дети в возрасте до 18 лет и 64% — люди в возрасте до 30 лет, вопросы социального обеспечения и прав ребенка имеют приоритетное значение.

Украина

С целью реализации и соблюдения требований действующего законодательства Украины в области защиты информационного пространства в 2003 г. создана Национальная экспертная комиссия Украины по вопросам защиты общественной морали. Комиссией на государственном уровне проводится работа по формированию каталога «белых сайтов», который включает перечень безопасных Интернет-ресурсов, рекомендованных для просмотра детьми. Уже проанализировано и отобрано свыше 200 сайтов (специализированные порталы детской литературы, электронные библиотеки, образовательно-информационные ресурсы, сайты библиотек, музеев и т. д.).

Комиссией в 2009 г. разработана Памятка для родителей «Дети, Интернет, Мобильная связь». С целью урегулирования вопросов и выработки правил безопасного использования Интернет, в октябре 2011 г. были приняты «Рекомендации владельцам веб-ресурсов, целевой аудиторией которых являются дети». В документе, с учетом возрастных психофизиологических особенностей детского восприятия, даются рекомендации по контенту, рекламной продукции, стилистическому оформлению, которых желательно придерживаться при создании и функционировании детских веб-ресурсов.

Успешно реализуется на Украине программа «Безопасность детей в Интернете». Ряд мероприятий, направленных на обучение детей, учителей и родителей, инициированы Коалицией за безопасность детей в Интернете, основанной компанией «Майкрософт Украина» в рамках программы «Партнерство в образовании». Стартом кампании стал запуск безопасной электронной почты «Онляндия» – первого в Украине специального почтового сервиса для детей и подростков, которые могут не только отправлять электронные письма, но и общаться с друзьями в режиме онлайн с помощью сервиса обмена мгновенными сообщениями. Интерфейс почтового домена @onlandia.org.ua не содержит рекламы, а электронный ящик защищен от несанкционированного спама и вирусов.

В 2012 года на пресс-конференции в Киеве телеком-оператор «Киевстар» сообщил журналистам о старте новой всеукраинской социальной кампании «За безопасность детей в интернете». Цель инициативы – повысить осведомленность украинских родителей о технических средствах защиты детей во время использования «Домашнего интернета». Украинские родители теперь могут защитить от онлайн-угроз своих детей с помощью сервиса «Родительский контроль». Новый социальный сервис был разработан «Киевстар» совместно с «Майкрософт».

Основные результаты программы:

- Создан «белый список» рекомендованных детских сайтов;
- Издано пособие для родителей «Дети в Интернете: как научить детей безопасности в виртуальном мире»;
- Проведена информационная работа среди более чем 2000 детей, 4000 родителей и 5000 учителей по всей стране;

- Разработана новая услуга компании «Родительский контроль», которая гарантирует защиту детей от онлайн-угроз во время выхода в Интернет через мобильный телефон.

В феврале 2012 г. на Украине подписан меморандум о сотрудничестве по внедрению Кодекса о защите детей от жестокого поведения в Интернет, направленного на борьбу с вредным для детей Интернет-контентом. Инициатором создания Кодекса стал правозащитный центр «Ла-Страда-Украина» при участии Интернет-ассоциации Украины, уполномоченного Президента Украины по правам ребенка Юрия Павленко, общественных организаций. Первыми меморандум подписали компании «МТС-Украина», «Киевстар» и «Укртелеком», которые заявили о своей готовности защищать детей от информации, которая может повредить их психическому здоровью.

С 2000 г. активно ведет работу по вопросам безопасности в Сети Интернет Ассоциация Украины (ИнАУ), в задачи которой входит проведение исследований и профилактических мероприятий по распространению безопасных правил, ресурсов и специальных программ для работы в Интернете.

Ярким примером является проект Государственной библиотеки Украины для юношества – «Безопасное и приветливое веб-пространство», посвященный вебобщению и этикету. Кроме понимания технических аспектов работы в Интернете, стратегий поиска информации, в ходе его реализации поднимаются чрезвычайно важные вопросы этики и безопасности. Библиотекой разработаны и проводятся тренинги по формированию сетевой культуры для специалистов (библиотечные сотрудники, педагоги), родителей, подростков и молодежи. Проект стал победителем 2010 года в конкурсе «Учебно-инновационная библиотека» программы «Библиомост».

Защита детей в онлайновой среде определяется международным правом и законом Украины «Об охране детства», в частности, раздел 2. статья 9. «Право ребенка на свободное выражение мнения и получение информации». Данный документ отмечает, что каждый ребенок имеет право на свободное высказывание личного мнения, формирование собственных взглядов, развитие собственной общественной активности, получение информации, соответствующей его возрасту. Это право включает свободу искать, получать, использовать, распространять и сохранять информацию в устной, письменной или иной форме, с помощью произведений искусства, литературы, средств массовой информации, средств связи (компьютерной, телефонной сети и т.п.) или других средств по выбору ребенка. Ему обеспечивается доступ к информации и материалов из различных национальных и международных источников, особенно тех, которые способствуют здоровому физическому и психическом развитии, социальном, духовном и нравственном благополучию.

Дети имеют право обращаться в органы государственной власти, органов местного самоуправления, предприятий, учреждений, организаций, средств массовой информации и их должностных лиц по замечаниям и предложениями относительно их деятельности, заявлениями и ходатайствами относительно реализации своих прав и законных интересов и жалобами об их нарушении.

С целью реализации этого права государство способствует:

- распространению средствами массовой информации материалов, полезных для развития ребенка;

- изданию и распространению детской литературы и учебников путем создания льготных условий для их издания;
- международному сотрудничеству в сфере обмена и распространения информации и материалов, поступающих из различных национальных и международных источников;
- деятельности средств массовой информации, направленной на удовлетворения языковых потребностей детей, в том числе тех, которые относятся к национальным меньшинствам.

Осуществление прав ребенка на свободное выражение мнения и получение информации может быть ограничено законом в интересах национальной безопасности, территориальной целостности или общественного порядка с целью предотвращения беспорядков или преступлений, для охраны здоровья населения, защиты репутации или прав других людей, предотвращения разглашения информации, полученной конфиденциально, или обеспечения авторитета и беспристрастности правосудия.

Необходимо так же упомянуть, что, если международным договором, согласие на обязательность которого предоставлено Верховной Радой Украины, установлены иные правила, чем те, содержащиеся в законодательстве Украины об охране детства, применяются правила международного договора.

Отметим также негосударственные меры по защите детей в онлайновой среде. Украинский телекоммуникационный оператор «Киевстар» разработал программу «Центр семейной безопасности Киевстар» , которая включает в себя: антивирус; брандмауэр и родительский контроль. Программа позволяет установить фильтры для просмотра сайтов только из «белого списка», сайтов для детей, сайтов для всех (кроме сайтов для взрослых), на общение в Сети, а также включает предупреждение о контенте для взрослых.

В ходе реализации Региональной инициативы МСЭ CIS1 «Создание центра по защите ребенка в онлайновой среде для региона СНГ» Одесская национальная академия связи (ОНАС) имени А.С.Попопва в сотрудничестве с Международным союзом электросвязи (МСЭ) разработала «Мультимедийный учебный дистанционный курс безопасного пользования ресурсами сети Интернет».

Курс состоит из трёх уровней: базовый (для детей дошкольного и младшего школьного возраста), средний (для детей 5-9 классов) и продвинутый (для старшеклассников, студентов, молодых родителей и учителей). Все три уровня курса включают более 300 интерактивных экранов включающих 10 интерактивных игр, 14 анимационных роликов или мультипликационных фильмов, 23 фотографии, а также более 150 рисунков.

Курс предназначен для распространения в общеобразовательных учебных заведениях региона СНГ и размещен в интернете на: http://onlinesafety.info/. Также курс доступен на сайте http://АСИКТ.РФ. Для общеобразовательных учебных заведений, не располагающих достаточной скоростью интернет-соединения, имеются компакт-диски с записью курса.

Курс был представлен Проректором Одесской национальной академии связи им. А.С. Попова Вадимом Каптуром на Учебном семинаре для руководителей общеобразовательных учебных учреждений «Безопасный Интернет: ключевые аспекты и современные тенденции», организованном Департаментом образования и науки Одесского городского совета, совместно с

ОНАС и при поддержке Международного союза электросвязи, который состоялся в г. Одесса, Украина, 2 декабря 2015 года.

Аналогичный Учебный семинар для руководителей общеобразовательных учебных учреждений «Безопасный Интернет: ключевые аспекты и современные тенденции» был организован Институтом электроники и телекоммуникаций (ИЭТ) при Кыргызском государственном техническом университете (КГТУ) имени Исхака Раззакова совместно с ОНАС и МСЭ и состоялся в г. Бишкек, Кыргызская Республика, 10 декабря 2015 года. В семинаре приняли участие более 70 директоров школ Бишкека, которым также был представлен «Мультимедийный учебный дистанционный курс безопасного пользования ресурсами сети Интернет».

Кроме того, в рамках реализации региональной инициативы CIS1 МСЭ ОНАС разработала Рекомендации по выбору системы фильтрации контента.

Реализация региональной инициативы CIS1 обсуждалась на Заседании круглого стола «Использование ИКТ для развития человеческого потенциала: защита ребёнка в онлайновой среде, помощь людям с ограниченными возможностями, укрепления доверия и безопасности при использовании ИКТ» г. Бишкек, 8 декабря 2015 года.

«Мультимедийный учебный дистанционный курс безопасного пользования ресурсами сети Интернет» был также представлен в рамках мероприятий, посвященных Всемирному дню безопасного интернета, которые прошли в общеобразовательных учреждениях г. Одесса 9 февраля 2016 года. В детском саду №29 Департамент образования и науки Одесского горсовета совместно с Одесской национальной академией связи имени А. С. Попова провели мини-спектакль на тему «Безопасный мир Интернета», после просмота которого дошкольники получили сертификаты о прохождении базового уровня курса.

5. Организация доступа лиц с ограниченными возможностями к ИКТ

Республика Азербайджан

Обучение людей с ограниченными возможностями использовать современные информационно-коммуникационные технологии поможет значительно улучшить качество их жизни.

ИКТ в стране развиваются быстрыми темпами, и успешно внедряются во все сферы социально-экономической жизни.

В Республике Азербайджан придается особая значимость развитию ИКТ навыков каждого члена общества, в том числе, для лиц с ограниченными возможностями создаются условия для пользования информационно-коммуникационными технологиями и электронно-информационными ресурсами.

В декабре 2005 года, в рамках проекта «По обеспечению доступа к информационно-коммуникационным технологиям (ИКТ) для слепых и людей с ограниченным зрением», реализованного Программой развития ООН совместно с Фондом Гейдара Алиева, для слепых и слабовидящих детей Республиканской интернет школы, были созданы модельные ИКТ классы.

В качестве продолжения данных работ, в рамках совместного проекта Фонда Гейдара Алиева, Министерства связи и информационных технологий Азербайджана и Программы развития ООН, с целью расширения возможностей для использования инвалидами

информационно-коммуникационных технологий, в г.Гяндже был создан Региональный информационный центр.

Услугами Регионального информационного центра смогут воспользоваться более 60 тысяч людей с физическими недостатками, проживающих в городах Гянджа и Нафталан, а также в Агстафинском, Дашкесанском, Газахском, Гедабекском, Геранбойском, Гейгельском и Шамкирском районах.

Аналогичный центр создается и в Нахчыванской Автономной Республике. В центре, на основе современных технологий, будут функционировать читальный зал, учебно-образовательный сектор, аудио-библиотека, студия звукозаписи для перезаписи литературного фонда в аудио-формат, компьютерный центр, специально предусмотренный для слепых и слабовидящих детей, обеспечивающий выход в интернет. Будет создан интернет сайт Центра. Посредством звукозаписывающей студии предполагается перевести в аудиоформат до 50-и книг напечатанных шрифтом Брайля.

В центре планируется: установить увеличительные приборы на компьютерах для людей со слабым зрением, издание книг со шрифтом брайля, демонстрация фильмов с субтитрами для глухонемых, создание компьютерных игр, для людей со слабым интеллектом, развивающих мозг. Здесь будут созданы все необходимые условия для беспрепятственного передвижения тех, кто посещает центр в инвалидных колясках.

Данные центры, создающиеся в рамках совместного сотрудничества, направлены на обеспечение активного участия людей с физическими недостатками в жизни общества, получение информации посредством информационно-коммуникационных технологий и расширение возможностей для повышения своих знаний, и в общем, на улучшение образа жизни.

Законодательство Республики Азербайджан в сфере защиты авторских прав находится на высоком уровне. К сожалению, в стране проживает большое число слепых и людей, имеющих слабое зрение. Правительством поставлена задача сделать так, чтобы эти люди в полной мере могли пользоваться своими авторскими правами. В этом вопросе особую роль играет Марракешский договор об облегчении доступа слепых и лиц с нарушениями зрения или иными ограниченными способностями к печатной продукции. Этот документ расширяет доступ к книгам людям с ограниченной способностью воспринимать печатную информацию и требует, чтобы договаривающиеся стороны включили в свое национальное законодательство положения, позволяющие воспроизводить, распространять и предоставлять опубликованные произведения в доступных форматах. В нем также нашли отражение положения о трансграничном обмене этими произведениями в доступных форматах между организациями, которые обслуживают слепых и лиц с нарушениями зрения или ограниченными способностями воспринимать печатную информацию.

Договор гарантирует авторам и издателям, что эта система не будет подвергать их опубликованные произведения опасности неправомерного использования или распространения. Концепцией развития «Азербайджан-2020: взгляд в будущее» предусмотрена национальная стратегия в сфере защиты авторских прав.

Республика Армения

По данным статистики на сентябрь 2015 в Республике Армения проживают около 8 тыс. детей с ограниченными физическими возможностям, что составляет 4% от общего числа

инвалидов. Общее число проживающих в Армении лиц с ограниченными физическими возможностями составляет 200 тыс. человек, или 6,6% от общей численности населения. Среди них 136,7 тыс. человек - инвалиды с детства.

На основе информационно-коммуникационных технологий в стране разработаны новые инструменты, способствующие интеграции граждан с ограниченными возможностями в цифровую экономику. Новые технологии облегчают включение детей с инвалидностью в школьную систему, позволяют повысить их успеваемость и интегрироваться в профессиональную и социальную сферы. Армения начала внедрение амбициозной программы по расширению использования ИКТ такими гражданами, программу, в центре внимания которой — обучение детей с ограниченными физическими возможностями.

В ноябре 2011 г. в рамках партнерского проекта ИИТО и Международного союза электросвязи (МСЭ) в Ереване, Республика Армения, был открыт и успешно действует ИТ-центр для лиц с нарушениями зрения.

Основная цель проекта – поддержка инклюзивной политики и создание с помощью средств ИКТ доступной информационно-образовательной среды для людей с ограничениями по зрению.

Технологическая инфраструктура центра включает в себя типичные рабочие места, оборудованные стандартными и специализированными программно-аппаратными средствами для двух групп пользователей: (1) слепых; и (2) слабовидящих людей. Центр станет не только местом, обеспечивающим доступ к знаниям и информации для лиц с нарушениями зрения, но и платформой для общения и обмена опытом среди специалистов.

Проект предусматривает разработку методических и дидактических материалов по обеспечению доступности обучения с помощью средств ИКТ. Эти материалы предназначенны для лиц, принимающих решения и определяющих политику в области образования, ИТ-специалистов и педагогов, работающих в сфере обучения и социальной реабилитации лиц с ограниченными возможностями здоровья.

Республика Беларусь

В подпрограмме Национальной программы ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы поставлена задача реализация которой позволит обеспечить вовлечение малоэффективно занятых специалистов, безработных, людей с ограниченными возможностями, жителей сельской местности, студентов в реализацию проектов с использованием ИТ-технологий.

Грузия

Законодательство Грузии не всегда соответствуют лучшей международной практике, защищающей права инвалидов. Правозащитники утверждают, что в Грузии инвалиды, практически не выходящие из дома и лишенные возможности найти работу, являются одной из самых маргинализированных групп. Такое бедственное положение дел позволяет судить о их уровне доступности к ИКТ.

После окончания школы молодые люди с ограниченными возможностями, как и многие другие выпускники, хотят продолжить своё обучение в ВУЗах, что позволит им в дальнейшем адаптироваться в обществе. Как известно, Интернет является наиболее удобной, а иногда и единственной возможностью получить образование, работу, информацию, поддерживать общение, принимать участие в жизни общества, вести активный образ жизни.

До настоящего времени многие веб-сайты государственных органов недоступны для людей с ограниченными возможностями здоровья, в том числе сайты, предназначенные для оказания государственных услуг. Хотя в Грузии наравне со специальным образованием реализуется политика инклюзивного образования, издание учебников шрифтом Брайля для незрячих и укрупненным шрифтом для слабовидящих учащихся по-прежнему остается проблемой. Право детей с ограниченными возможностями здоровья на получение качественного образования реализуется не в полной мере. Система финансирования высшего образования не позволяет обеспечить учебные заведения оборудованием, необходимым для работы с людьми с ограниченными возможностями.

Республика Казахстан

В настоящее время доступность среды является одной из приоритетных задач для развития ИКТ, что прописано в Государственной Программе «Информационный Казахстан 2020». В целях повышения готовности населения и бизнеса к возможностям информационного общества планируется проводить курсы по базовым навыкам компьютерной грамотности и получению государственных услуг в электронной форме для предпринимателей малого и среднего бизнеса (самозанятые лица), безработной и/или частично занятой молодежи, а также лиц с ограниченными возможностями здоровья, пожилых людей и других категорий социально-незащищенных слоев населения. Также документом предусматриваются способы внедрения ИКТ в повседневную жизнь граждан, в частности с целью помощи людям с ограниченными возможностями.

Министерство труда и социальной защиты населения совместно с Агентством Республики Казахстан по связи и информации ведет работу по подготовке к внедрению электронной композитной услуги для людей с ограниченными возможностями, которая объединит 9 видов государственных услуг.

В сотрудничестве с Министерством здравоохранения РК рассматривается вопрос внедрения международной классификации функционирования, ограничения жизнедеятельности и здоровья (МКФ), которая позволит определить степень трудоспособности людей с ограниченными возможностями, путем соотнесения состояния их здоровья и уровня возможностей.

Закон республики Казахстан о социальной защите инвалидов регулирует общественные отношения в области социальной защиты инвалидов в Республике Казахстан и определяет правовые, экономические и организационные условия обеспечения социальной защиты инвалидов, создания им равных возможностей для жизнедеятельности и интеграции в общество. В законе приведено определение сурдотехнических средств - технические средства для коррекции и компенсации дефектов слуха, в том числе усиливающие средства связи и передачи информации. Также приведены обязательства государства по обеспечению доступа инвалидов к информации, а именно государство берёт обязательства обеспечить инвалидам доступ к информации в соответствии с законодательством Республики Казахстан посредством выпуска периодической,

научной, учебно-методической, справочно-информационной и художественной литературы для инвалидов, в том числе издаваемой на аудиокассетах, дисках, рельефно-точечным шрифтом Брайля и видеокассетах с сурдопереводом; организацию сурдоперевода информационных программ не менее чем на одном из республиканских телевизионных каналов. В качестве средства межличностного общения используется язык жестов, который применяется также в программах обучения организации образования для глухих и слабослышащих детей.

Кыргызская Республика

В рамках реализации Региональной инициативы CIS2 «Обеспечение возможности доступа к услугам электросвязи/ИКТ для лиц с ограниченными возможностями» специалистами Института электроники и телекоммуникаций при Кыргызском государственном техническом университете имени И.Раззакова проведён анализ существующих нормативных документов, в которых устанавливаются требования доступности услуг образования, ИКТ и веб-ресурсов

По статистическим данным Министерства социального развития Кыргызской Республики с каждым годом в Кыргызстане увеличивается количество людей с ограниченными возможностями здоровья (ЛОВЗ), т.е. в стране по состоянию на 1 января 2014 года проживают 155893 лиц с ограниченными возможностями здоровья, из них 26672 детей до 18 лет. Так, если в 2010 году всего первично признано инвалидами -18380 человек, из них 3943 дети до 18 лет, то в 2012 году 18659, из них детей 4663, в 2013году 16687, из них 4342 детей. Такие люди постоянно сталкиваются с препятствиями при доступе к услугам электросвязи/ИКТ, образования, здравоохранения, транспортных коммуникаций, трудоустройства. Эти препятствия приводят к нарушениям прав лиц с ограниченными возможностями здоровья (ЛОВЗ), гарантированные международными договорами о правах человека, к которым присоединилась Кыргызская Республика, Конституцией Кыргызской Республики и другими законодательными актами государства. Конституция Кыргызской Республики, Законы Кыргызской Республики «О правах и гарантиях лиц с ограниченными возможностями здоровья», «Об основах социального обслуживания населения в КР», «О содействии занятости населения», «Об охране здоровья граждан Кыргызской Республики», Трудовой Кодекс направлены на улучшение жизни лиц с ограниченными возможностями здоровья, на ликвидацию различных препятствий для интеграции в общество. Как известно, принятие организацией объединенных наций в 2008 г. Конвенции «О правах инвалидов» (далее – Конвенция) вызвал прилив положительных эмоций в сообществе людей с ограниченными возможностями. Распоряжением Правительства Кыргызской Республики от 16 сентября 2011 года №422-р одобрена Конвенция ООН о правах инвалидов и 21 сентября 2011 года подписана. На настоящий момент, Кыргызская Республика не ратифицировала данную Конвенцию, которая определяет основные стандарты прав инвалидов, а также обязательства государства и других сторон по обеспечению данных прав.

С точки зрения существующего законодательства государство создало мощный механизм защиты прав инвалида. Они направлены на предоставление ЛОВЗ равных с другими гражданами возможностей реализации конституционных прав и свобод. Вместе с тем, необходимо отметить, что в законодательстве Кыргызской Республики существуют пробелы, которые требуют рассмотрения и внесения изменений. Так, законодательство Кыргызской Республики не в полной мере предусматривает меры по устранению физических препятствий для доступа ЛОВЗ к физическому окружению, к транспорту, к информации и связи, включая

информационнокоммуникационные технологии и системы, а также к другим объектам и услугам, открытым или предоставляемым для населения, например: В Законе Кыргызской Республики «О градостроительстве и архитектуре Кыргызской Республики» от 11 января 1994 года N 1372-XII гарантии обеспечения лицам с инвалидностью доступной среды отсутствуют Законы Кыргызской Республики «О средствах массовой информации» от 2 июля 1992 года № 938-XII, «О гарантиях и свободе доступа к информации» от 5 декабря 1997 года № 89, «Об информатизации» от 8 октября 1999 года № 107, «О системе научнотехнической информации» от 8 октября 1999 года № 108 не предусматривают надлежащих мер по обеспечению доступа ЛОВЗ к объектам и услугам, открытым или предоставляемым для населения. Законы Кыргызской Республики «Об электрической и почтовой связи» от 2 апреля 1998 года №31, «О почтовой связи» от 20 июня 2001 года № 52, «О транспорте» от 8 июля 1998 года №89, «О железнодорожном транспорте» от 9 июля 1998 года №90 не содержат норм по обеспечению доступа ЛОВЗ к услугам транспорта и связи. Право на образование гарантировано ст. 45 Конституции Кыргызской Республики, однако в законодательстве Кыргызской Республики отсутствует общее понятие инклюзивного образования для всей системы образования, оно обозначено лишь в Законе Кыргызской Республики «О дошкольном образовании» от 29 июня 2009 года № 198 (ст.1) отсутствуют нормы, мотивирующие работодателя принимать на работу лиц с инвалидностью. В связи с этим существует необходимость внесения изменений и дополнений в действующее законодательство республики. В то же время совершенствование законов само по себе не решает проблему, поскольку сегодня остро стоит вопрос о неудовлетворительном исполнении действующего законодательства органами государственной власти Кыргызской Республики, и это является основной причиной массовых нарушений прав людей с ограниченными возможностями здоровья. Помимо этого, в законах часто отсутствуют механизмы их реализации. Таким образом, необходимая нормативная база обеспечения доступной для ЛОВЗ среды жизнедеятельности в основном создана, но реальная ситуация с реализацией прав ЛОВЗ показывает значительное расхождение с законодательными предписаниями. Анализ доступности услуг образования Лица с ограниченными возможностями здоровья наравне с другими гражданами имеют право на образование. Каждый может в соответствии со своими способностями бесплатно получить соответствующее образование в государственных учебных заведениях. Согласно ст. 33 Закона Кыргызской Республики «О правах и гарантиях лиц с ограниченными возможностями здоровья» государство гарантирует лицам с ограниченными возможностями здоровья создание необходимых условий для доступа к получению образования и профессиональной подготовки. ЛОВЗ после окончания школы, как и многие другие выпускники, хотят продолжать образование в вузах. Несмотря на то, что получение высшего образования лицами с ограниченными возможностями здоровья закреплено законодательно, только с 2012 года в Кыргызстане лицам с ограниченными возможностями здоровья осуществляется предоставление квоты в ВУЗах. Так, постановлением Правительства Кыргызской Республики «О внесении изменений и дополнений в некоторые нормативные правовые акты Кыргызской Республики» от 29 декабря 2011 года № 255 предусмотрено изменение процедуры приема на грантовое обучение абитуриентов из числа инвалидов первой и второй групп. В 2012 году в высшие учебные заведения приняты 42 абитуриента из числа ЛОВЗ, в 2013 году в рамках данной квоты принято 60 абитуриентов. Мотивация лиц с ограниченными возможностями здоровья к поступлению в ВУЗ снижается из-за низкого качества подготовки в интернатах, из-за страха неприспособленной среды, отсутствия специальных приспособлений и оборудования в вузах, затрудненной мобильности ввиду отсутствия специального транспорта. К сожалению, по статистическим данным в нашей стране в 2011/12 учебном году в Вузах обучалось

около 42 инвалида, в 2012/13 году – 48, в 2013/14 году – 60, в 2014-15 году - 17. Получение высшего образования лицами с ОВЗ включает в себя создание специальных условий для получения ими образования с учетом особенностей их состояния. Лица, имеющие заболевания органов зрения и слуха, в силу специфики заболеваний весьма ограничены в возможностях получения информации в обычном понимании. ВУЗы страны в минимальном объеме оснащены специальными средствами обучения и методиками, не имеют в своем штате преподавателей, прошедших специальную подготовку для работы с данной категорий обучающихся. Такое неудовлетворительное решение проблемы доступности ВУЗов для лиц с нарушениями зрения и слуха, функций опорно-двигательного аппарата обретает форму значительного нарушения конституционного права на образование. Кроме вопросов по созданию доступной среды в учреждениях образования, остается открытым вопрос об организации подвоза людей с инвалидностью в ВУЗы, а также отсутствие специального транспорта. Не реализуется норма законодательства о выпуске периодической, научной, учебно-методической, справочно-информационной и художественной литературы для лиц с ограниченными возможностями здоровья, в том числе издаваемой на аудиокассетах, дисках, рельефно-точечным шрифтом Брайля и видеокассетах с сурдологическим переводом. Органы государственной власти не обеспечивают доступности официальным интернет-сайтам для лиц с ограниченными возможностями здоровья.

На основании анализа состояния прав лиц с ограниченными возможностями здоровья можно сделать следующий вывод: на сегодняшний день лица с ограниченными возможностями здоровья при получении государственных услуг, гарантированных Конституцией Кыргызской Республики они сталкиваются с нарушениями их прав и свобод. Они имеют очень низкий доступ к инфраструктуре, возможности получения образования, медицинских и социальных услуг. Важнейшими факторами, влияющими на их повышение доступа, являются: отсутствие специальных условий для получения ими образования с учетом особенностей их состояния, доступных средств ИКТ.

Также специалистами Института электроники и телекоммуникаций при Кыргызском государственном техническом университете имени И.Раззакова был проведён анализ адаптации официальных веб-сайтов госорганов с учетом потребностей инвалидов по зрению; обеспечение доступа инвалидов и других маломобильных групп населения к электронным государственным услугам посредством сети Интернет; создание и поддержание в сети Интернет сайтов, имеющих социальное или образовательное значение. Для оценки официальных веб-сайтов госорганов на предмет соответствия содержания, механизмов обратной связи веб-сайтов запросам основных групп потребителей информации, а также доступности к ЛОВЗ были изучены следующие параметры:

• параметры, характеризующие наличие и полноту механизма обратной связи (наличие кнопки автоматической отправки электронного сообщения администратору/регулятору веб-сайта);

• обновляемость информационных материалов на веб-сайте;

• соответствие единым требованиям по созданию и поддержке веб сайтов госорганов и органов МСУ Кыргызской Республики (Постановление Правительства Кыргызской Республики от 14 декабря 2007 года №594);

• наличие альтернативных вариантов сайта для доступа лиц с ОВЗ.

Фактически все действующие сайты соответствуют единым требованиям по созданию и поддержке веб сайтов госорганов и органов МСУ Кыргызской Республики (Постановление Правительства Кыргызской Республики от 14 декабря 2007 года №594), однако в требованиях не предусмотрены требования доступности веб-ресурсов для лиц с ОВЗ. Из всех веб-сайтов госорганов только информационные порталы ГНС, ГТС, МЭ, МЗ, ГРС имеют возможности интерактивного взаимодействия с гражданами и организациями, но не отвечают требованиям доступности веб-ресурсов для лиц с ОВЗ.

В рамках реализации Региональной инициативы CIS2 «Обеспечение возможности доступа к услугам электросвязи/ИКТ для лиц с ограниченными возможностями» в г. Бишкек в октября 2015 года в Институте электроники и телекоммуникаций при Кыргызском государственном техническом университете имени И.Раззакова был открыт специализированный информационно-обучающий центра «Ийгилик» для людей с ограниченными возможностями, созданный при поддержке МСЭ.

В центре имеются все необходимые условия для продолжения школьного образования и освоения различных профессий людьми с ограниченными возможностями здоровья. Из 12 рабочих мест, 6 предназначены для людей с нарушением зрения и 6 - для людей с нарушениями опорно-двигательного аппарата.

Для представления технологий, позволяющих людям с ограниченными возможностями здоровья, получить доступ к ИКТ, а также для обучения сотрудников центра «Ийгилик» использованию специального оборудования, которым оснащен центр, ИЭТ в сотрудничестве с МСЭ и Институтом ЮНЕСКО по информационным технологиям в образовании провели Учебно–информационный семинар по современным адаптивным технологиям для людей с ограниченными возможностями здоровья (с нарушениями зренияи и опортно-двигательного аппарата), Бишкек, Кыргызская Республика, 7-8 декабря 2015 года.

Реализации региональной инициативы CIS2 обсуждалась на заседании круглого стола «Использование ИКТ для развития человеческого потенциала: защита ребёнка в онлайновой среде, помощь людям с ограниченными возможностями, укрепления доверия и безопасности при использовании ИКТ» г. Бишкек, 8 декабря 2015 года.

В ходе реализации указанной Региональной инициативы разработаны и создаются:

- Рекомендации и нормативные документы, в которых устанавливаются требования к инфраструктуре и контенту по доступности и удобству использования ИКТ лицами с ограниченными возможностями.
- Рекомендации по адаптации веб-ресурсов для обеспечения их максимальной доступности для лиц с ограниченными возможностями.
- Пункты коллективного доступа для лиц с ограниченными возможностями, оснащенные специализированным программно-аппаратным обеспечением.
- Информационно-обучающий центр для обучения лиц с ограниченными возможностями в регионе СНГ.
- Методики обучения лиц с ограниченными возможностями навыкам пользования средствами электросвязи/ИКТ и подготовка преподавателей по применению данных методик.

Республика Молдова

В Республике Молдова существует закон «О социальной интеграции лиц с ограниченными возможностями» от 30 марта 2012 года №60. Данный закон декларирует государственную политику в области доступности различных сфер жизни для лиц с ограниченными возможностями и устанавливает следующее.

В целях обеспечения лицам с ограниченными возможностями независимого образа жизни центральные и местные органы публичной власти, неправительственные организации, хозяйствующие субъекты, независимо от их организационно-правовой формы, исходя из своих функциональных полномочий оценивают положение дел в данной области и принимают конкретные меры для облегчения доступа указанных лиц наравне с другими лицами к физической среде, транспорту, информации и средствам связи, в том числе к информационным технологиям и электронным коммуникациям, а также к другим общественно-полезным объектам и услугам, открытым или предоставляемым населению как в городских, так и в сельских населенных пунктах в соответствии с действующими нормативами.

Министерство информационных технологий и связи, другие компетентные органы публичной власти содействует доступу лиц с ограниченными возможностями к информации и средствам массовой информации, а также к информационным технологиям и электронным коммуникациям.

Государство через Министерство просвещения, Министерство культуры, другие компетентные центральные и местные органы публичной власти, а также через хозяйствующих субъектов обеспечивает в соответствии с действующим законодательством издание с использованием альтернативных форм коммуникации (в системе Брайля и звуковой версии, в простом и доступном изложении и т.д.) художественной литературы, школьных учебников, других дидактических материалов и средств обучения.

Органы публичной власти и публичные учреждения обязаны обеспечивать доступность своих веб-страниц для лиц с ограниченными возможностями в соответствии с основными международными положениями в области доступности.

При закупке оборудования и информационного обеспечения публичные учреждения должны учитывать соблюдение критериев доступности.

Хозяйствующие субъекты, предоставляющие услуги в области связи и информации, устанавливают лицам с ограниченными возможностями скидки на оплату данных услуг.

Нормативы приспособления информационно-коммуникационных систем к потребностям лиц с ограниченными возможностями, а также использования альтернативных форм коммуникации (система Брайля и звуковая версия, язык мимики и жестов и др.) в информационно-коммуникационной системе утверждаются Правительством.

Российская Федерация

В Российской Федерации особое значение уделяют внедрению специализированных средств для доступа лиц с ограниченными возможностями к услугам связи.

С 2006 года у ОАО «ВымпелКом» существует специальный тарифный план «Со-общение», разработанный в г.Екатеринбурге по инициативе и при участии одного из обществ слабослышащих людей «Страна глухих». Позднее, тарифный план стал доступен слабослышащим людям на всей территории России. В 2011-2012 годах ОАО «ВымпелКом» реализовала бесплатный доступ с мобильных устройств к «нулевым зонам» в Интернете, включающим в себя социальные сети и ряд новостных порталов. Эта опция позволила слабослышащим людям бесплатно общаться в социальных сетях. В сентябре 2014 года ОАО «ВымпелКом» стала первым оператором, внедрившим проект по обслуживанию на жестовом языке людей с нарушениями слуха.

Важность и значительный потенциал имеют мобильные технологии в России, предназначенные для приобщения пожилых людей и людей с ограниченными возможностями к цифровой экономике и обществу. По итогам конференции M-Enabling Russia 2015 в Москве стало ясно, что российские разработчики и компании могут внести значительный вклад в развитие мирового рынка. Каждый день во всем мире используется семь миллиардов мобильных устройств, один миллиард из которых приходится на людей с ограниченными возможностями, включая пожилых людей. Доступные и вспомогательные технологические решения пользуются колоссальным спросом.

Компании ОАО «ВымпелКом» (Бренд «Билайн»), Lexmark и «ИстокАудио» в настоящее время прорабатывают возможности доступа лиц с ограниченными возможностями к услугам связи и ИКТ в целом. Группа компаний «ИстокАудио» является крупнейшим российским разработчиком, производителем и поставщиком слуховых аппаратов, высокотехнологичной реабилитационной техники и ассистивных устройств для людей с инвалидностью по слуху и зрению. Компания также занимается оборудованием для создания условий доступной среды и универсального дизайна в быту, в учреждениях при получении комплекса услуг, при реализации задач инклюзивного образования и трудовой деятельности. Компания Lexmark занимается разработкой многофункциональных устройств (принтер-сканер-копир), облегчающих пользование техникой людьми с ограниченными физическими возможностями.

В мае 2015 года в г.Москве впервые прошла Международная конференция по вопросам доступности мобильных и информационно-коммуникационных технологий для пожилых людей и людей с ограниченными возможностями здоровья M-Enabling Россия 2015 на которой представители государственных органов, международных и российских общественных организаций, ведущих коммерческих компаний и инвалидных организаций обсудили вопросы доступности мобильных и информационно-коммуникационных технологий для пожилых людей и людей с ограниченными возможностями здоровья.

В настоящее время в мире насчитывается миллиард инвалидов из которых13 млн. живет в России (председатель конференции M-Enabling Russia 2015). При этом 2/3 из них существенно ограничены в средствах и не могут приобрести себе современные гаджеты, смартфоны, органайзеры, компьютеры и другие мобильные средства, помогающие им быть полноценными участниками общественной жизни. В 2015 году остро поставлен вопрос о развитии в Российской Федервции полноценного рынка ассистивных и ИТ-технологий для инвалидов общим объёмом свыше 60 млрд. рублей в год и создании общества равных возможностей. Особое внимание было уделено поддержке молодых инноваторов, занимающимся разработкой и производствам ТСР и иных асситивных технологий, способных улучшить качество жизни людей с ограниченными возможностями здоровья, а также поддержке проектам предпринимателей - инвалидов, т.к.именно

самозанятось людей с ограниченными возможностями это показатель высочайшего уровня их социализации и независимости.

В качестве поддержки стартапам в России реализуется не имеющая аналогов в Россиипрограмма поддержки проектов социального предпринимательства в области решения проблем инвалидов «Технологии возможностей».

В стране остро стоит вопрос доступности Интернета для инвалидов и пожилых граждан. Минкомсвязь России ведёт целый ряд работ по повышению доступности информационных технологий для людей с ограниченными возможностями здоровья. Среди них: предоставление широкополосного доступа в Интернет; работа по совершенствованию единого портала государственных услуг; реализация инициатив по развитию дистанционного образования и дистанционной занятости. Разработанная новая версия портала государственных услуг помимо общих улучшений, учитывает потребности инвалидов, что дает возможность данной категории граждан снять барьеры при пользовании государственными услугами.

Республика Таджикистан

Ежегодно в Таджикистане отмечается День инвалидов и пожилых людей. В настоящее время Таджикистан не подписал и не ратифицировал Конвенцию о правах инвалидов, которая является одним из первых единых международно-правовых документов, закрепляющих весь комплекс прав лиц с инвалидностью.

Согласно статистике, количество людей с ограниченными возможностями (ЛОВЗ) в Таджикистане значительно возросло за последние 20 лет и на данный момент составляет около 160 тыс. человек.

Принятие Таджикистаном нового Закона о социальной защите инвалидов представляет собой важный шаг на пути ратификации Конвенции о правах инвалидов. Ратификация Конвенции о правах инвалидов послужит новым импульсом к искоренению стигмы и дискриминации в отношении лиц с ограниченными возможностями в Таджикистане и еще раз подчеркнет приверженность Таджикистана соблюдению прав человека в стране.

Республика Узбекистан

В Постановлении Президента страны от 27 июня 2013 года Комплексной программы развития Национальной информационно-коммуникационной системы Республики Узбекистан на период 2013-2020 годы рассматривается организация доступа лиц с ограничеными возможностями к информационно-коммуникационным технологиям. В частности рассматривается создание необходимых условий для лиц с ограниченными возможностями при оказании электронных государственных услуг. Предусматривается провести работы, которые обеспечат при оказании госуслуг возможность навигации по сайту организации с выключенной функцией отображения графических элементов страниц в веб-обозревателе, поддержку лиц с ослабленным зрением, возможность масштабировать (увеличивать и уменьшать) шрифт и элементы интерфейса официального веб-сайта средствами веб-обозревателя, возможность звукового сопровождения действий пользователя на веб-сайте.

Организация доступа лиц с ограниченными возможностями к информационно-коммуникационным технологиям предусмотрена законом Республики Узбекистан «О социальной защищённости инвалидов в Республике Узбекистан», а именно статьи 9 - 11. В них, в частности предусматривается учёт потребностей инвалидов при проектировании и застройке населенных пунктов, разработке и производстве транспортных средств, средств связи и информации. Проектирование и застройка населенных пунктов, формирование жилых районов, разработка проектных решений на новое строительство, реконструкция зданий, сооружений и их комплексов, а также разработка и производство транспортных средств, средств связи общего пользования и информации без приспособления указанных объектов для доступа к ним инвалидов и использования их инвалидами не допускаются.

Законом предусматривается обеспечение беспрепятственного доступа инвалидов к объектам социальной инфраструктуры, пользования транспортом, средствами связи и информации. Органы государственного управления, органы государственной власти на местах, предприятия, учреждения и организации (далее — организации) обязаны создавать условия инвалидам (включая инвалидов, использующих кресла-коляски и собак-проводников) для беспрепятственного доступа к объектам социальной инфраструктуры (жилым помещениям, общественным и производственным зданиям, строениям и сооружениям, объектам здравоохранения и спорта, культурно-зрелищным и другим учреждениям), а также для пользования железнодорожным, воздушным, водным, междугородным автомобильным транспортом, всеми видами городского и пригородного пассажирского транспорта, транспортными коммуникациями, средствами связи общего пользования и информации.

За невыполнение предусмотренных настоящим Законом требований по созданию условий инвалидам для беспрепятственного доступа к объектам социальной инфраструктуры (жилым помещениям, общественным и производственным зданиям, строениям и сооружениям, объектам здравоохранения и спорта, культурно-зрелищным и другим учреждениям), а также для пользования железнодорожным, воздушным, водным, междугородным автомобильным транспортом, всеми видами городского и пригородного пассажирского транспорта, транспортными коммуникациями, средствами связи общего пользования и информации должностные лица организаций привлекаются к административной ответственности.

Применение административного взыскания не освобождает организации от обязанности исполнения требований настоящего Закона по созданию условий для беспрепятственного доступа инвалидов к объектам социальной инфраструктуры, пользования транспортом, транспортными коммуникациями, средствами связи общего пользования и информации.

Украина

В 2008 году Украина подписала конвенцию ООН о правах инвалидов. В Таким образо, Правительство Украины гарантирует лицам с ограниченными возможностями доступ к ИКТ и экстренным службам на равной основе, способствует доступу к новым ИКТ, включая интернет, способствует проектированию, производству и распространению доступных ИКТ на раннем этапе, гарантирует, что лица с ограниченными возможностями могут реализовать свое право на свободу выражения мнения и убеждений, предоставляет информацию в доступных форматах и с использованием технологий, учитывающих разные формы ограниченных возможностей.

В июне 2010 года Украина провела семинар МСЭ для стран Европы и СНГ по обеспечению доступа ИКТ для лиц с ограниченными возможностями.

Целью семинара являлось:

- обмен опытом и информацией среди участников о последних достижениях в области обеспечения доступа к ИКТ для лиц с ограниченными возможностями, рассмотрение таких вопросов как продвижение помогающих технологий, включая оборудование, программное обеспечение и услуги связи, а также использование доступных ИКТ для социального и экономического развития лиц с ограниченными возможностями;
- повышение осведомленности о ресурсах, доступных с помощью онлайнового инструментария МСЭ-G3ict для органов, отвечающих за выработку политики, по вопросам, связанных с лицами с ограниченными возможностями;
- сдействие Государствам - членам МСЭ в усилиях, направленных на реализацию Программы цифровой доступности согласно Конвенции ООН по правам лиц с ограниченными возможностями.

На Украине реализуется образовательный проект (2014-2016гг.) для людей с инвалидностью и ограниченными возможностями. В рамках проекта пилотная группа из 90 человек начала дистанционное обучение по ИТ-специальностям (компьютерная грамотность, HTML, CSS, Python, PHP, SQLite, Java SE). Обучение бесплатное и проходит в формате вебинаров, видеоуроков и онлайн-тестов. Каждый участник пилотной группы может пройти обучение по пяти специальностям. Полный курс длится полгода, после чего выпускникам помогут найти работу в украинских ИТ-компаниях. Организатором программы выступает Фонд Восточная Европа в партнерстве с Благотворительным фондом развития компьютерных и информационных технологий для инвалидов «АИК». Финансовую поддержку оказывает британская благотворительная организация «Всемирная еврейская помощь» (WorldJewish Relief).

Курсы разрабатывались совместно с институтом компьютерных технологий университета «Украина». Помимо удаленных занятий и тестов, учащиеся могут лично пообщаться с преподавателями и получить все необходимые консультации. Принять участие в проекте могут все украинцы с ограниченными возможностями. При отборе учитывают группу инвалидности (1, 2), уровень доходов (ниже среднего) и мотивацию к обучению и трудоустройству. Организован «фидбек» от ИТ-работодателей, чтобы оценить их заинтересованность в трудоустройстве людей с особыми потребностями, существующие преграды и т.д. После обучения организаторы планируют провести ярмарки вакансий в городах Киеве, Харькове и Львове.

Фонд также организует тренинги для HR-специалистов ИТ-компаний по разным аспектам трудоустройства людей с инвалидностью.

6. Проблемы доверия и безопасности при Интернет-торговле (e-Commerce)

Электронная коммерция открывает совершенно новые возможности перед потребителями в плане поиска товаров и удобства оформления сделки. Однако она порождает и новые проблемы. Например, Интернет-торговля предъявляет повышенные требования к доставке, в том числе почтовой, которая должна отвечать стандартизированным уровням скорости и точности.

Существенным препятствием интенсивного развития Интернет-торговли является проблема доверия. Готовность клиентов взаимодействовать через Интернет-рынок является значимым социально-психологическим фактором привлекательности Интернет-рынка для предприятия и готовности предприятия к интеграции в среду электронной коммерции.

Интернет магазины чаще предоставляют лучший и более широкий ассортимент, чем аналоги, размещенные в супермаркетах. Наличие проблемы доверия в Интернет-торговли связано со спецификой осуществления товарно-денежных отношений с помощью Интернет: получение товара или услуги разнесены по времени с получением денег. Особенности осуществления Интернет-торговли инициируют такие угрозы, которые снижают доверие покупателей к Интернет-торговле:

- Отсутствие возможности непосредственно ознакомиться с товаром во время его приобретения;
- Трудности, связанные с возвратом товара в случае обнаружения брака;
- Риски, связанные с задержкой доставки и возможные повреждения товара по вине транспортной компании;
- Риски, связанные с возможным наличием случайных или преднамеренных ошибок в программном обеспечении, обслуживающим Интернет-торговлю.

Вопрос защиты прав потребителей в электронной коммерции является ключевым. Очевидно, что без его решения не будет доверия кинтернет-торговли и ее развития.

Республика Азербайджан

Национальные программы Республики Азербайджан по развитию ИКТ позволяют все большему количеству граждан получать доступ к глобальным информационным сетям и ресурсам, что способствует международным интеграционным процессам во всех сферах жизни общества (торговля, образование, медицина, государственные услуги и пр.).

При информационном взаимодействии остро встает вопрос обеспечения доверия и безопасности обмена данными. Это особенно актуально для процессов, предполагающих совершение юридически значимых действий, к которым относится и Интернет-торговля.

В 2014 году объем рынка электронной коммерции составил в Азербайджане 6,4 млн манатов, что в 2,4 раза превысило оборот за 2013 год.

В январе-феврале 2015 года объем электронной розничной торговли составил в Азербайджане 1 млн 688,7 тыс. манатов. В сравнении с аналогичным периодом 2014 года рынок интернет-торговли (e-commerce) вырос в 1,5 раза.92,7% товаров было приобретено в онлайн-режиме в объектах торговой сети, принадлежащих юридическим, 7,3% - физическим лицам. При этом 95,9% оборота рынка e-commerce пришлось на товары непродовольственного назначения.

Наиболее известным игроком на этом рынке является международная сеть онлайн-продаж Kaymu, которая открыла свое представительство в Республике Азербайджан.

Особенностью предложения компании Kaymu является то, что она служит платформой, на которой можно создавать свои собственные интернет-магазины. Таким образом, платформа Kaymu является посредником между покупателями и продавцами. В настоящее время

государства – участники СНГ провозгласили развитие информационно-коммуникационных технологий одним из приоритетов и необходимым условием устойчивого экономического роста и повышения качества жизни граждан.

Несмотря на стремительное развитие интернет-торговли во многих странах, в Республике Азербайджан в этом секторе экономики остаётся много открытых вопросов.

Республика Армения

К числу основных проблем развития e-commerce в Республике Армения можно отнести: отсутствие доверия со стороны покупателей; отсутствие актуального законодательства, охватывающего все аспекты интернет-торговли; проблемы с доставкой товаров и ограниченный доступ в интернет. Рассмотрим два аспекта развития интернет-торговли в Республике Армения.

При организации внутренней Интернет-торговли в настоящее время можно отнести вопросы регулирования электронных денег в Армении (инициатор обсуждения Центральный банк), концепция системы электронной оплаты ArCA, проблемы оплаты в сфере электронного управления (E-gov), проблемы электронной оплаты в электронной торговле, принципы возможных моделей развития электронной торговли в Армении, использование опыта других стран в электронной торговле (Россия, Грузия, Македония), проблемы логистики, технического обеспечения и безопасности в интернет-торговле.

Трансграничная Интернет-торговля растет темпами, опережающими рост на внутреннем рынке. Динамика развития трансграничной интернет-торговли на фоне уменьшения доли внутренней интернет-торговли объясняется неравными конкурентными условиями, сложившимися на этом рынке.

По данным 2015 г. в Армении без уплаты таможенных пошлин разрешается ввоз не более одной посылки в течение полугода, и стоимостью не более 50 тысяч драм (примерно 91 евро). Разница в стоимости посылки, превышающая установленный лимит, и все дополнительные входящие почтовые отправления облагаются таможенной пошлиной. Это является несомненно одной из ключевых проблем, требующих незамедлительного решения.

Республика Беларусь

При организации внутренней Интернет-торговли (e-commerce) в Республике Беларусь применяются следующие основные законодательные акты:

- Указ Президента Республики Беларусь от 01.02.2010 № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»;
- Закон Республики Беларусь от 08.01.2014 № 128-З «О государственном регулировании торговли и общественного питания в Республике Беларусь»;
- Закон Республики Беларусь от 09.01.2002 № 90-З «О защите прав потребителей»;
- Правила продажи товаров при осуществлении розничной торговли по образцам, утвержденные Постановлением Совета Министров Республики Беларусь от 15.01.2009 № 31;

- Правила продажи отдельных видов товаров и осуществления общественного питания, утвержденные Постановление Совета Министров Республики Беларусь от 22.07.2014 № 703;

- Положение о Торговом реестре Республики Беларусь, утвержденное Постановление Совета Министров Республики Беларусь от 23.12.2014 № 1227;

- Инструкция о порядке регистрации доменных имен в пространстве иерархических имен национального сегмента сети Интернет, утвержденная Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 18.06.2010 № 47.

Если интернет-торговля осуществляется лицом, зарегистрированным в Беларуси, вне зависимости от того, на кого ориентирован интернет-магазин (на внутренний либо на внешний рынок), требования к организации деятельности интернет-магазинов едины (что следует из п. 2 Указа № 60). Необязательным соблюдение требований белорусского законодательства является лишь для лиц, действующих с территории иностранных государств и зарегистрированных на такой территории. То есть, интернет-магазин может быть ориентирован как на внутреннюю, так и на внешнюю торговлю товарами, но при этом важно соблюсти все требования белорусского закона.

При организации трансграничной Интернет-торговли внешнеэкономическая инфраструктура выступает как основной интегрирующий инструмент процессов международного экономического сотрудничества регионов Республики Беларусь и других стран СНГ. К ее объектам относятся торговые представители, торговые дома, сервисные центры, филиалы предприятий, консигнационные склады, а также различного рода дилеры и дистрибьюторы.

К факторам, затрудняющим эффективное использование внешнеэкономической инфраструктуры в межрегиональном экономическом сотрудничестве, можно отнести: узкую специализацию объектов товаропроводящей сети, низкий уровень информационно-маркетингового обслуживания межрегиональных связей Республики Беларусь и других стран СНГ; низкую эффективность деятельности отдельных объектов как самостоятельных хозяйствующих субъектов, преимущественно отраслевой подход к созданию внешнеэкономической инфраструктуры, что не отвечает задаче комплексного охвата интеграционными связями экономических субъектов двух стран и очень часто сопровождается нехваткой финансовых ресурсов; слабую координацию деятельности между всеми видами инфраструктуры.

Дальнейшее совершенствование функционирования внешнеэкономической инфраструктуры может быть связно с созданием постоянно функционирующих в регионе торговых домов, к функциям которых были бы отнесены закупка товаров за счет собственных средств и на условиях комиссии, продажа товаров по каталогам и посредством Интернет.

Грузия

В 2001 году в Тбилиси в третий раз прошла конференция «Интернет Бизнес Грузия», проведенная совместно с Министерством транспорта и коммуникации Грузии и Ассоциацией молодых экспертов Грузии. Основной темой конференции стало обсуждение вопросов

по созданию платформы для электронной коммерции в стране. К сожалению дополнительная официальная информация в открытых источниках отсутствует.

Республика Казахстан

Объем рынка интернет-торговли в Республике Казахстан составил около 400 млн. долларов США по итогам 2012 года. Рост интернет-торговли увеличивается в 2-2,5 раза в год. К концу 2015 года оборот e-commerce в Казахстане (именно в казахстанских интернет-магазинах, а не в иностранных, действующих на территории республики) приблизился к 3,6 млрд. долларов США, то есть 4% от общего рынка ритейла в Республике Казахстан, который, к началу 2016 года составит порядка 90 млрд. долларов США.

В настоящее время большая часть платежей приходится на зарубежные интернет-магазины. Можно привести следующие цифры: за год В Казахстане на покупки в интернет-магазинах тратится порядка 1,5 млрд. долларов США, но при этом на долю магазинов в самом Казахстане из указанной цифры приходится чуть больше 100 млн. долларов США.

Вопросы укрепления доверия к интернет-торговле играют ключевую роль в её развитии. Например, крупным международным брендам, которые известны в оффлайне не нужно прикладывать много усилий, чтобы стать известными и завоевать доверие при интернет-торговле. Для начинающих национальных магазинов этот вопрос стоит очень остро. Анализ проведённых в Республике Казахстан социальных опросов показывает, что одной из основных проблем таких стартапов является менталитет местных покупателей. Испытывая определённое недоверие местные покупатели очень долго выбирают интернет-магазин, сопоставляют по цене, качеству и другим параметрам несколько предложений и, только после этого, совершают покупку. Если епо каким-либо причинам он останется недоволен предложенным ему сервисом, в следующий раз он обратиться в другой интернет-магазин.

Одной из составляющих успеха электронной коммерции является наличие удобных средств платежей. По данным Национального банка Республики Казахстан наибольшей проблемой, связанная с использованием платежных карт в Казахстане являются высокие комиссии, отказы в осуществлении электронного платежа, а также недостаточный уровень компетенции держателей банковских карт, что приводит к большому числу кибермошенничества при интернет-торговле (например, кражи персональных данных).

Таким образом, можно сделать вывод, что одной из важных проблем интернет-торговли является отсутствие доверия со стороны клиентов к интернет магазинам и онлайн сервисам. Недоверие можно объяснить несколькими факторами: отсутствие узнаваемых и надежных брендов, слабая информированность населения об основных правилах оплаты через интернет, нежелание банков развивать интернет платежи в связи их высокой рискованностью и т.д. В качестве решения подобных проблем, некоторым известным и крупным компаниям в Казахстане удается использовать свои бренды в роли гаранта качества сервиса в интернете. Такие компании как Kcell, Air Astana и Meloman инвестируют в интернет-развитие делая ставку на будущее. Однако компании среднего и малого бизнеса не могут использовать свои бренды как рычаг, чтобы привлечь достаточное количество клиентов для стабильной и прибыльной работы.

Другая серьезная проблема это проблема электронных денег и платежей. На данный момент платежи в интернете затруднены как для клиентов, так и для продавцов. Существующие

сервисы онлайн оплаты делают экономику ведения бизнеса для предпринимателей не выгодной по причине высоких процентов и больших сроков выплат выручки банками. Другая проблема это легальность проведения операций в интернете. На данный единственный легальный способ принимать олнайн платежи это использовать сервис epay от Казкомерцбанк.

Несмотря на указанные проблемы рынок дистанционных продаж в Казахстане продолжает развиваться ускоренными темпами. Площадкой, на которой обсуждаются и решаются многоие вопросы интернет-торговли является международная конференция «Торговая миссия в Казахстане».

Преимущества партнерства рынка электронной коммерции с национальным почтовым оператором заключаются в том, что Казпочта представлена в более чем 130 странах, имеет международное авиасообщение, магистральное сообщение, 3300 почтовых отделений по всему Казахстану, свой парк автотранспорта. Ведутся переговоры с почтовыми союзами Вьетнама, Катара, России, Китая, ОАЭ, Турции о возможном создании более дешевого канала доставки.

В настоящее время существует несколько проектов, направленных на улучшение логистики. Первый проект – это внедрение системы мониторинга автотранспортных средств, оснащение 898 единиц транспорта GPS-трекерами, позволяющими отслеживать движение машины по заданному маршруту. Второй проект – перевод транспортных средств на газ. Два первых проекта направлены на оптимизацию затрат. Третий проект – внедрение автоматизированной линии для сортировки посылок. При этом ожидаемые результаты – повышение скорости обработки посылок на 30%.

Также начат проект по установке видеокамер в почтовых вагонах. То есть видеокамеры позволят обеспечить сохранность посылок и планировать правильную загрузку вагонов. И еще один проект – создание собственной сети постаматов. К концу 2015 года планировалось установить 100 постаматов более чем в 20 городах Казахстана. Таким образом, все вышеперечисленные проекты направлены на качество, скорость и оптимизацию расходов.

Следует отметить, что на сегодняшний день в Республике Казахстан успешно реализовано несколько международных проектов, например, с ТОО «НИЛ «Гамма Технологии». Его целью было обеспечение возможности участия пользователей, являющихся нерезидентами Республики Казахстан в системе электронных закупок АО «ФНБ «Самрук-Казына», с применением юридически значимой электронной подписи. В связи с тем, что основными иностранными поставщиками в Казахстане являются российские организации, было принято решение обеспечить на казахстанской электронной торговой площадке работу с «российскими» электронными подписями (ЭП). Выпуск сертификатов ключа проверки ЭП взял на себя Удостоверяющий центр (УЦ) «Гамма Технологии».

Кыргызская Республика

Для совершения интернет-торговли в Кыргызской Республике требуется обеспечить развитие национальных удостоверяющих центров электронной цифровой подписи и принять правовые акты, определяющие порядок их взаимодействия. Перспективным является направление по созданию общего центра удостоверения доверия к электронной цифровой подписи всех партнеров – участников электронных сделок.

Республика Молдова

Одним из факторов, влияющих на развитие интернет-торговли в Республике Молдова, является национальное законодательство в области электронных платежей. Ниже приведены наиболее значимые нормативно-правовые акты (НПА) в этой области.

Основным НПА в области безналичных платежей в Республике Молдова является Закон Республики Молдова от 18 мая 2012 года №114 «О платежных услугах и электронных деньгах». Закон регулирует деятельность поставщиков платежных услуг и эмитентов электронных денег, условия и порядок их лицензирования, режим транспарентности условий предоставления платежных услуг, выпуска и выкупа электронных денег, права и обязанности поставщиков платежных услуг и эмитентов электронных денег в контексте предоставления на профессиональной основе услуг, права и обязанности пользователей услуг, пруденциальный надзор за поставщиками платежных услуг и эмитентами электронных денег. Осуществление безналичных платежей регулируется также Постановлением Национального банка Республики Молдова от 15 октября 2010 года №204 «Об утверждении Регламента о деятельности поставщиков платежных услуг в системах перевода денег» и Постановлением Национального банка Республики Молдова от 27 июня 2013 года №123 «Об утверждении Регламента о деятельности эмитентов электронных денег и небанковских поставщиков платежных услуг».

Надзор и контроль в сфере безналичных платежей и переводов осуществляется Национальным Банком Молдовы в соответствии с Законом Республики Молдова от 21 июля 1995 года №548-XIII «О Национальном банке Молдовы». В соответствии с п.”f” ч.1 ст.5 Закона, Национальный банк осуществляет надзор за системой платежей в республике и способствует эффективному функционированию системы межбанковских платежей.

Закон «О платежных услугах и электронных деньгах» определяет следующие понятия, имеющие значение в области осуществления мобильных платежей:

Общество, выпускающее электронные деньги - хозяйственное общество, отличное от банка, обладающее в соответствии с настоящим законом лицензией на выпуск электронных денег.

Оператор платежной системы - юридическое лицо или юридические лица, юридически ответственные за функционирование платежной системы;

Перевод денег - платежная услуга, в рамках которой средства поступают от плательщика, без открытия платежного счета на имя плательщика или получателя платежа, с единственной целью перевода соответствующей суммы получателю платежа или другому поставщику платежных услуг, действующему от имени получателя платежа, и/или в рамках которой средства получены на имя получателя платежа и предоставлены в его распоряжение;

Платежная система - система перевода средств, действующая на основе формальных стандартных общих норм (правил, процедур, договоров и т.д.) в области обработки, клиринга и/или расчета по платежным операциям;

Платежное общество - хозяйственное общество, отличное от банка, поставщика почтовых услуг или общества, выпускающего электронные деньги, обладающее в соответствии с настоящим законом лицензией на предоставление платежных услуг;

Платежный инструмент - персонализированное средство (платежная карта, мобильный телефон и т.д.) и/или совокупность процедур (технических - PIN-коды, TAN-коды, другие виды кодов, логин/пароль и т.д. или функциональных - кредитовый перевод, прямое дебетование), согласованных между пользователем платежных услуг и поставщиком платежных услуг и используемых пользователем платежных услуг для инициирования платежного поручения; тесные связи - положение, в котором два или более лица;

Электронные деньги - хранящиеся в электронном виде, в том числе на магнитном носителе, денежные средства, представленные в виде требования к эмитенту, которые эмитируются при получении средств, отличных от электронных денег, для осуществления платежных операций и которые принимаются лицом, отличным от эмитента электронных денег.

Законом «О платежных услугах и электронных деньгах» установлена обязанность поставщика платежных услуг по информированию клиента.

На территории Молдовы эмиссия, обслуживание и использование платежных карт регулируются Регламентом о платежных карточках, утвержденный Постановлением Административного совета Национального Банка Молдовы №157 от 01.08.2013. В указанном акте даны определения платежной, кредитной, дебетовой и предоплаченной карт, перечислены права и обязанности поставщиков платежных услуг и клиентов в сфере применения платежных карт, установлен порядок проведения операций по платежным картам.

Закон Республики Молдова от 26 июля 2007 года №190-XVI «О предупреждении и борьбе с отмыванием денег и финансированием терроризма», определяет идентификационные меры, которые применяются в отношении физических или юридических лиц, а также выгодоприобретающего собственника.

Закон Республики Молдова от 15 июля 2004 года №264-XV «Об электронном документе и цифровой подписи» устанавливает правовые основы использования электронных документов и применения цифровой подписи, определяет основные требования, предъявляемые к электронному документу и цифровой подписи, а также основные правила осуществления электронного документооборота.

Признание иностранных сертификатов электронной подписи осуществляется на основании двусторонних или многосторонних соглашений между Республикой Молдова и другими государствами или международными организациями на взаимной основе.

Российская Федерация

Прогнозы развития Интернет-торговли указывают на её неукоснительный рост в Российской Федерации. По данным ФОМ в 2014 году более 72 млн. жителей России в возрасте от 18 до 64 лет формировали интернет-аудиторию, по статистике агентства Data insight за 2015 год 25 млн. человек в данной возрастной категории совершали покупки через интернет. Несмотря на снижение реальных доходов населения, количество онлайн-покупателей в 2016 году продолжает расти. Причинами такого роста являются: высокий уровень проникновения интернета, рост уровня доверия граждан к интернет-покупкам, и как следствие - увеличение доли покупателей, отказавшихся от офлайн-ритейла в пользу онлайна.

Анализ текущего регулирования трансграничной торговли на территории Евразийского экономического союза (ЕАЭС), проведённый Ассоциацией компаний интернет-торговли (АКИТ), показал, что российский рынок Интернет-торговли в настоящее время находится в стадии активного развития и на протяжении последних лет демонстрирует стремительный рост. Особое место в его структуре занимает трансграничная торговля, доля которой по итогам 2014 года приблизилась к 30% от всего объема рынка электронной коммерции (в совокупности около 208 млрд. рублей). Трансграничная Интернет-торговля растет темпами, опережающими внутренний рынок, и по прогнозам экспертов АКИТ в 2015 году достигнет 35% (240 млрд. рублей) от всего объема российского рынка e-commerce.

В 2014 году логистическими операторами (включая Почту России) было доставлено 78 млн. отправлений с товарным вложением из зарубежных интернет-магазинов (более 85% отправлений из Китая). В 2015 году количество входящих международных почтовых отправлений возросло на 35%.

Подобная динамика связана с тем, что перемещение товаров для личного пользования практически не обременено фискальной нагрузкой: в России действуют самые высокие в мире нормативы для беспошлинного ввоза товаров (1000 евро в месяц на человека), импорт таких товаров не облагается НДС.

Мировой опыт показывает, что отсутствие взвешенного регулирования в данной сфере приводит к сокращению доли локальных компаний и доминированию зарубежных интернет-гигантов. Это, в частности, можно наблюдать на примере Австралии, находящейся на втором месте после России по величине порога беспошлинного ввоза. В Австралии на сегодняшний день 75% всего рынка электронной коммерции составляет трансграничная Интернет-торговля, и практически отсутствуют локальные онлайн ритейлеры. Кроме того, отсутствие налогообложения по месту образования прибыли дает необоснованные конкурентные преимущества зарубежным интернет-магазинам и создает стимул для вывода инфраструктуры локальных компаний за рубеж.

Вместе с тем, на сегодняшний день на территории ЕАЭС отсутствуют единые правила регулирования ввоза товаров для личного пользования. В Республике Казахстан установлены критерии коммерческих партий и без уплаты таможенных пошлин возможен ввоз не более одной посылки в месяц, причем количественные показатели пересылаемых товаров строго ограничены, например, в одном отправлении невозможно ввезти более двух мобильных телефонов или схожих предметов одежды на одного человека. В Республике Беларусь на настоящий момент таможенными пошлинами облагаются товары, пересылаемые в международных почтовых отправлениях, превышающие по стоимости 200 евро или вес в 31 кг.

Объем рынка интернет-торговли в России по итогам 2014 года вырос на 31%. Вместе с тем, существенный вклад в этот рост внес трансграничный сегмент, объем которого по итогам 2014 года вырос более чем на 55% (по количеству посылок на 135%). Доля трансграничной Интернет-торговли по итогам 2014 года составила 30% всего объема рынка электронной коммерции. Трансграничная торговля занимает все более существенную долю в объеме интернет-торговли и по итогам 2015 года. Эксперты АКИТ отмечают, что при такой динамике в 2015 году этот сегмент займет 35% всего объема рынка интернет-торговли в России.

Такие темпы связанны во многом с тем, что регулирование в России для локальных и зарубежных магазинов строится таким образом, что зарубежные интернет-магазины не обременены никакой фискальной нагрузкой и, тем самым, заведомо находятся в более выгодных

конкурентных условиях и могут предлагать товары по заведомо более низким ценам (в среднем на 30%).

В международной практике существует несколько групп стран с различными типами государственного регулирования интернет-торговли и импорта товаров на территорию страны.

Первая группа включает в себя страны, в которых нет минимального порога для беспошлинного ввоза товаров. Вся импортируемая продукция облагается пошлиной. При этом эти страны можно разделить на две категории по размеру ввозных таможенных платежей:

a. Низкие и умеренные средние таможенные платежи (Китай, Индия, ОАЭ).

Пошлиной облагаются все импортируемые товары. Диапазон пошлин при этом в этих странах в зависимости от категории товара колеблется от 0-100%. Средние таможенные платежи в Китае составляют 12,5%, в Индии - 11%, ОАЭ -4,5%. Также в Индии и ОАЭ не взимается НДС, при этом в Китае НДС и пошлина взимаются только тогда, когда они суммарно превышают 50 юаней (~7 евро)

b. Высокие средние таможенные платежи (Аргентина, Бразилия).

Пошлиной облагаются все импортируемые товары. При этом в зависимости от категории размер пошлин в этих странах колеблется от 0% до 35%. Средние таможенные платежи в Аргентине и Бразилии составляют 23%. Уровень налоговой нагрузки в этих странах довольно высокий, однако локальные игроки хорошо защищены условиями импорта товаров, так как находятся в равных конкурентных условиях.

Вторая группа охватывает страны, в которых установлен незначительный минимальный порог для полного освобождения от налогов. Среди них: Канада (14 евро), Таиланд (23 евро), Новая Зеландия (34 евро), Южная Африка (37 евро) и Мексика (39 евро). Сюда же можно отнести и Индонезию (39 евро), но с одной оговоркой, что в отличие от вышеперечисленных стран ввоз на территорию Индонезии товаров на сумму до 39 евро предполагает освобождение от уплаты импортной пошлины, но не НДС. Для этой группы стран характерны достаточно высокие ставки НДС (Канада — 5-15%, Таиланд — 7%, Новая Зеландия — 14%, Южная Африка — 14%, Мексика — 16%, Индонезия — 10%) и в то же время относительно высокие (по европейским меркам) ставки таможенных пошлин (Канада8,56%, Таиланд — 20,93%, Новая Зеландия — 5,11%, Южная Африка — 18,74%, Мексика — 13,97%, Индонезия— 10,89%) .

Третья группа включает страны Европейского союза. На территории этих стран установлена многоступенчатая система регулирования импорта товаров для личного пользования. Минимальный порог в этих странах колеблется от 1,7 до 22 евро (на Кипре это 17,09 евро, в Великобритании — 18 евро, во всех остальных странах ЕС — 22 евро). Начиная с этой суммы, со всех импортируемых товаров взимается НДС. Далее с суммы свыше 150 евро взимается дополнительная пошлина. При этом важно отметить, что на территории стран ЕС взимается далеко не самый низкий НДС. Наименьшие ставки НДС наблюдаются в Люксембурге (15%), на Кипре (18%) и на Мальте (18%), а самые высокие — в Венгрии (27%), Швеции (25%), Хорватии (25%) и Дании (25%). Что же касается импортных пошлин, то в большинстве стран ЕС их среднее значение колеблется в районе 4-6%. Подобная система регулирования Интернет-торговли дает равные конкурентные условия зарубежным и локальным игрокам, позволяя развиваться обоим сегментам Интернет-торговли и может быть предложена для

использования в качестве унифицированной для регулирования трансграничной торговли на территории стран Евразийского экономического союза.

К четвертой группе относятся страны с относительно высокими порогами беспошлинного ввоза товаров. В этих странах без какой-либо налоговой нагрузки разрешается импортировать товар, стоимость которого не превышает в Сингапуре - 236 евро, в США - 200 долларов, Южная Корея - 103 евро, Япония - 76 евро. При этом такой высокий порог обусловлен относительно невысокой налоговой нагрузкой на импортеров внутри страны. НДС в этих странах составляет 4-10%, а в США и вовсе отсутствует. Ввозная пошлина товаров в этих странах колеблется от 0% до 5%. Таким образом, конкурентных преимуществ зарубежные игроки не получают, ввиду низкой налоговой нагрузки на локальных игроков.

Отдельно от всех групп стоят Россия (порог 1000 евро) и Австралия (порог 673 евро). При этом в России, помимо высокого порога беспошлинного ввоза, высокая налоговая нагрузка на игроков (в среднем около 30%).

Особое место в структуре рынка интернет-торговли занимает трансграничная торговля. Она растет темпами, опережающими внутренний рынок. Так, если рост интернет-торговли в целом последние 5 лет находится на уровне в 30%, среднегодовой совокупный темп роста рынка трансграничной интернет-торговли за последние 6 лет составляет 91,2%. В 2014 году объем рынка трансграничной интернет-торговли составил 208,6 млрд. рублей, что составляет 30% от всего рынка интернет-торговли. Подобная ситуация показывает, что с каждым годом локальный рынок снижает темпы роста и все большую долю занимает трансграничная Интернет-торговля.

В 2014 году было доставлено 78 млн. отправлений с товарным вложением на территорию РФ. Причем более 70 млн. доставила почта России. В 2015 году Почта России ожидает рост количества посылок на 35% по сравнению с 2014 годом. Общее число отправлений с товарным вложением в 2015 году составит 101 млн. Более 80% этих отправлений - мелкие пакеты (посылки весом менее 2 кг, отправка которых по цене равна отправке письма).

Важно отметить, что 90% всех отправлений доставляется в Россию из Китая. При этом в денежном выражении на Китай приходится 48% всего объема трансграничной торговли. Таким образом, требования еще более жесткие: без уплаты таможенных пошлин разрешается ввоз не более одной посылки в течение полугода, стоимостью не более 50 000 драм (-91 евро). Разница в стоимости посылки, превышающая установленный лимит, и все дополнительные входящие почтовые отправления облагаются таможенной пошлиной

Однако, в связи с тем, что на территории единого экономического пространства перемещение товаров между государствами-членами ЕАЭС производится в свободном режиме, отсутствие единого регулирования по периметру ЕАЭС приводит к тому, что импорт товаров для личного пользования осуществляется через страну с наиболее лояльным режимом ввоза. Это позволяет недобросовестным участникам рынка производить пересылку почтовых отправлений через границы других стран, тем самым уходя от уплаты таможенных пошлин. На приграничных территориях создаются логистические комплексы, легально предлагающие услуги по пересылке почтовых отправлений через Россию в другие страны ЕАЭС. Этим же пробелом, а также отсутствием необходимости уплаты каких-либо налогов начинают активно пользоваться и из-за границы, не инвестируя в развитие экономик стран присутствия. Развитие бизнеса по такой модели приводит к прямому субсидированию экономик зарубежных стран и оказывает негативное влияние на экономику и бизнес локальных компаний в сфере Интернет-торговли.

Необходимо отметить, что наряду с открытостью периметра ЕАЭС для импорта товаров для личного пользования, рынки других стран для членов ЁАЭС закрыты. Мировой опыт демонстрирует широкую палитру подходов к регулированию трансграничной торговли.

Например, в Китае, Аргентине, Бразилии установлен нулевой порог беспошлинного ввоза и все входящие почтовые отправления облагаются налогом и пошлиной; в Канаде, Таиланде, Новой Зеландии установлены невысокие пороги (соответственно 14, 23 и 34 евро); в странах Евросоюзаустановлена многоступенчатая система регулирования ввоза товаров для личного пользования:отправления стоимостью свыше 22 евро облагаются НДС, в случае превышения стоимости в 150 евро посылка облагается НДС и таможенной пошлиной. Данное регулирование может быть предложено для использования на территории всего ЕАЭС.

В Австралии, несмотря на относительно невысокую налоговую нагрузку (в среднем 12%), подобная планка беспошлинного ввоза привела к тому, что более 75% всей интернет-торговли занимает трансграничный сегмент,

Россия, в которой ситуация еще больше усугублена, неизменно движется по пути Австралии, где неравные конкурентные условия способствуют уходу локальных интернет-игроков, выводу инфраструктуры за рубеж и переходу к трансграничной модели интернет-торговли, при которой государство не получает ни рабочих мест, ни пошлин, ни НДС. видно, что средний чек покупок в Китае сильно ниже среднего чека покупок в ЕС и США. Средний чек посылок из Китая составляет $40, при этом средний чек заказов на Aliexpress составляет $20.

Подобная динамика развития трансграничной торговли на фоне внутренней интернет-торговли объясняется неравными конкурентными условиями, сложившимися на этом рынке. Зарубежный игроки не платят НДС и пошлину, тем самым могут предлагать товар по цене на 20-30% ниже, чем игрок в России. Чаще всего в денежном выражении при трансграничной торговле российские покупатели покупают бытовую технику и электронику (33,1%) и одежду и обувь (34,6%). При этом маржинальность при торговле бытовой техникой и электроникой у локальных игроков не превышает 20%, а в среднем находится на уровне 10%, что делает невозможным конкурировать с зарубежными игроками по цене. Также крупными сегментами трансграничной торговли являются Парфюмерия и косметика (7,2%), автозапчасти (6,7%), товары для дома (3%), спорттовары (2,6%). Важно отметить, что вся продукция, покупаемая трансграничным способом, не проходит сертификации на территории РФ, что может быть опасным для сегментов парфюмерии и косметики и одежды и обуви. Кроме того, технически сложные товары из сегмента БТиЭ не могут быть должным образом обсажены на территории РФ.

В настоящее время в рамках Евразийского экономического союза Минкомсвязи России проводит работу по созданию интегрированной информационной системы, которая увязывает между собой процессы взаимной и внешней электронной торговли всех участников союза и обеспечивает отслеживание товаров от момента пересечения границы ЕЭС до их конечного потребителя. К системе подключены все страны-участницы союза. В 2015 году с участием Российской Федерации завершены мероприятия по проведению межгосударственных испытаний национального сегмента Российской Федерации в составе единой информационной системы Евразийской экономической комиссии.

Также в Российской Федерации действует система «Независимый регистратор», которая позволяет бороться с электронным мошенничеством в сфере закупок товаров, работ и услуг, в том числе связанных с госзаказом, с госкомпаниями. Это важная инициатива, потому что Российская

Федерация является сегодня одним из мировых лидеров по объему проводимых электронных аукционов.

Республика Таджикистан

Можно назвать следующие основные проблемы в области развития электронной коммерции в стране:

- неразвита система логистических услуг;
- в стране нет ни одной компании республиканского масштаба предлагающей услуги доставки грузов и почты, за исключением национальной почтовой службы ГУП «Почтаи Точик», уровень качества услуг которой удовлетворительный;
- законодательная неопределенность статуса интернет-магазинов;
- слабое развитие сетевой инфраструктуры в регионах;

Развитие Интернет-торговли в Таджикистане до 2014 года во многом сдерживалось отсутствие в стране компании, сертифицированной компанией Visa на эквайринг карт Visa в глобальной сети Интернет. В феврале 2014 года ЗАО «Казкоммерцбанк Таджикистан» впервые в Таджикистане запустил данную услугу, что обеспечило новые благоприятные условия для развития Интернет-торговли.

На сегодняшний день в Таджикистане более миллиона людей (около 17% населения страны) подключены к Интернету, что говорит об актуальности и своевременности внедрения новой услуги Казкоммерцбанк Таджикистан.

Согласно данным исследования ЗАО «Казкоммерцбанк Таджикистана» использования карт Visa по совершению онлайн покупок, жители Таджикистана в основном совершают Интернет-покупки за границей – в Великобритании, Ирландии, США, Германии, России, Латвии, Украины, Франции, Турции, Нидерландах.

Первой таджикской компанией, запустившей услугу Интернет-торговли, стал интернет магазин техно-торгового центра «Волна» (www.volna.tj).

Республика Узбекистан

Президент Узбекистана 22 мая 2015 года подписал закон «Об электронной коммерции» в новой редакции. Закон вступил в силу с 23 мая 2015 года. Предыдущий закон действовал с 2004 года.

В законе дается обновленное определение понятию «электронная коммерция» и другим терминам и включен ряд новых статей, в частности, статья, регулирующая использование персональных данных в e-commerce.

Под электронной коммерцией понимается «купля-продажа товаров (работ, услуг), осуществляемая в соответствии с договором, заключаемым с использованием информационных систем».

Основными принципами электронной коммерции, согласно закону, являются свобода осуществления предпринимательской деятельности, добровольность заключения договоров, равенство условий участия, а также защита прав и законных интересов участников электронной коммерции.

В соответствии с законом, электронные документы, а также информация, зафиксированная в электронной форме, позволяющая идентифицировать ее отправителя (электронные сообщения), в e-commerce приравниваются к документам на бумажном носителе, подписанным собственноручно, и могут быть использованы в качестве доказательства совершения сделок.

Договор в e-commerce не может быть признан недействительным только на том основании, что он заключен с использованием информационных систем.

Оферта в e-commerce формируется в виде электронного документа, а ответ участника e-commerce о принятии оферты (акцепт) может осуществляться в виде электронного документа или электронного сообщения либо путем совершения действий по выполнению условий, содержащихся в оферте.

В законе уточняется, что продавцом товаров (работ, услуг) в электронной коммерции может быть юридическое лицо или индивидуальный предприниматель.

Отдельно подчеркивается, что участие в e-commerce не может быть основанием для установления в отношении ее участника требований или ограничений, дополнительных по отношению к предпринимательской деятельности, осуществляемой без использования информационных систем, если иное не установлено законом.

В новой редакции закона прописаны права и обязанности участников (продавцов и покупателей) e-commerce и информационных посредников. Продавцы товаров (работ, услуг) обязаны соблюдать законодательство о конкуренции и защите прав потребителей, обеспечивать хранение электронных документов и электронных сообщений в соответствии с законодательством, а также соблюдать стандарты, нормы и правила в области e-commerce.

В законе значительно расширено понятие «информационные посредники» — к ним относятся операторы и провайдеры сетей телекоммуникаций, оказывающие услуги по обороту электронных документов и электронных сообщений участников e-commerce, банки, оказывающие услуги по обеспечению доступа к платежным системам и проведению платежей участников e-commerce, юридические лица, осуществляющие организацию электронных ярмарок, аукционов и конкурсов, а также юридические лица, оказывающие услуги по хранению электронных документов и электронных сообщений участников e-commerce.

Договор в e-commerce может заключаться путем осуществления акцепта в виде электронного документа, электронного сообщения или посредством совершения действий по выполнению условий, содержащихся в оферте. Договор признается заключенным в момент получения участником e-commerce, направившим оферту, ее акцепта.

Документы, связанные с исполнением договора в e-commerce, могут быть оформлены в виде электронного документа или на бумажном носителе.

Расширены требования к содержанию оферты в электронной коммерции. В ней должны присутствовать полное наименование, почтовый и электронный адрес участника e-commerce, делающего оферту, условия поставки и оплаты товаров (работ, услуг), а также предлагаемые цены (тарифы) на них, а в предусмотренных законодательством случаях — сведения о наличии лицензии или документа разрешительного характера

Отдельная статья закона посвящена использованию персональных данных в электронной коммерции. Законом запрещено использование персональных данных в целях, отличных от целей договора в e-commerce, и их передача третьим лицам, если иное не предусмотрено соглашением сторон и (или) законодательством. Не допускается использование персональных данных без согласия их владельца для распространения оферты и (или) рекламы, в том числе путем массовой рассылки электронных документов или электронных сообщений.

Дополнительно закон определяет основные направления государственной политики в области электронной коммерции. К ним, в частности, отнесены поддержка и стимулирование

предпринимательской деятельности, осуществляемой посредством e-commerce, создание условий для привлечения в сферу предпринимательства, осуществляемого посредством e-commerce, инвестиций, современных технологий и оборудования, а также стимулирование научно-технических исследований, подготовка и повышение квалификации кадров.

Формирование новых экономических отношений, основанных на новейших информационных технологиях и развитии глобальных телекоммуникационных сетей, в том числе Интернета, создание нового сектора экономического сотрудничества, называемого «электронной торговлей», позволяет проводить соответствующие рыночные преобразования и в Узбекистане.

Электронная торговля - это новый этап развития информационной инфраструктуры для формирования цивилизованного рынка в стране. Технологическая революция в сфере электронной связи повлекла развитие электронного обмена данными, что, в свою очередь, изменило способы осуществления торговых операций и как следствие упростило процедуру торговой сделки.

В Узбекистане в настоящее время действует несколько электронных торговых площадок и виртуальных магазинов, страна находится как бы в стороне от международного процесса развития электронной торговли. И причина этого - отсутствие надежной инфраструктуры этого сектора коммерции.

Узбекистан принимает все меры к тому, чтобы стать полноправным членом ВТО, и поэтому необходимо выполнять существующие международные требования и в области электронной торговли.

Украина

На Украине Интернет-торговля является одной из отраслей экономики, демонстрирующая самые быстрые темпы роста среди всех отраслей экономики. Объемы торговли в Интернете относительно розничной торговли в целом сравнительно малы. На конец 2012 года Интернет-торговля составила около 1,5-1,6% от общего объема розничной торговли, что намного меньше, чем в России, где проникновение Интернет-торговли приблизилось к 2%, не говоря уже о среднемировом показателе 6,5 %, или показатель США 10,1% .

По оценкам экспертов рынка, рост рынка e-Commerce на Украине в 2012 году составил от 30% до 50%. Более точную цифру назвать невозможно, т.к. на Украине Интернет-торговля очень непрозрачна. Это связано, во-первых, с большой долей наличных расчетов, во-вторых, с наличием большого количества маленьких интернет-магазинов, учесть деятельность которых почти невозможно.

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Объем интернет-торговли в Украине, млрд. дол.	**0,40**	**0,60**	**0,55**	**0,73**	**1,10**	**1,59**	**2,37**	**3,24**	**4,44**	**5,65**
Рост, год к году %		**50%**	**-8%**	**34%**	**50%**	**45%**	**49%**	**37%**	**37%**	**27%**
Проникновение интернет-торговли в Украине, %	**0,6%**	**0,7%**	**1,0%**	**1,1%**	**1,3%**	**1,6%**	**2,3%**	**2,9%**	**3,8%**	**4,5%**
Объем розничной торговки в Украине, млрд. грн.	319	449	443	530	675	804	902	967	1025	1087
Объем розничной торговки в Украине, млрд. дол.	63,2	85,2	56,9	66,8	84,7	99,5	105,5	111,8	118,5	125,6
Рост, год к году %		35%	-33%	17%	27%	17%	6%	6%	6%	6%

Развитие интернет-торговли (e-Commerce) на Украине

На Украине работает 8 тыс. интернет-магазинов, из которых около 300 с более или менее значительным товарооборотом. Интернет-магазины продают практически любую продукцию, но большинство из них небольшие игроки, которые не в состоянии обеспечить достаточный уровень инвестиций в рекламу и маркетинг, инфраструктуру и логистику.

Крупнейшие игроки рынка — это магазины, специализирующиеся на продаже бытовой техники и электроники, хотя большинство из них пытается диверсифицироваться, расширяя ассортимент продукции. Например, крупнейший Интернет-магазин в Украине предлагает, кроме бытовой техники, мебель, часы, товары для отдыха и туризма, товары для детей.

В настоящее время наиболее активны в онлайне сети по продаже техники и электроники: Эльдорадо, Comfy и Foxtrot, который получил полный контроль над Sokol.ua. В категории «Одежда, обувь и аксессуары» также много успешных и сильных игроков: Интертоп, Carlo Pazolini, Helen Marlen (posh.ua). Компании вкладываются в развитие собственных интернет-магазинов, а также охотно сотрудничают с другими площадками в поисках своей аудитории (например, товары сети Интертоп можно найти на Rozetka.ua).

Для всех категорий, которые пока что не готовы строить свои интернет-магазины, существуют торговые площадки, такие отдельные платформы, которые могут стать хорошей отправной точкой для старта интернет-продаж.

Многие крупные сети (Metro Cash&Carry, Leroy Merlin) на сегодняшний день все еще используют свои сайты просто как каталог товаров.

Одним из новых трендов развития интернет-торговли на Украине являются Онлайн-покупки товаров недельного потребления такие как приобретении хлеба, пучка петрушки, средств гигиены и т.п. В этой нише работают Zakaz.ua, Gastronom.com.ua, Royalmarket.com.ua, Produktoff.com, Ambar.ua и т.п., которые предлагают весь ассортимент супермаркетов и магазинов «у дома». Потенциал этого сегмента рынка очень высок, так как количество людей, которые не хотят тратить время и силы на дорогу и очереди, с каждым годом растет.

Другим трендом развития интернет-торговли на Украине является «омниканальность». Относительно новое направление, о котором сейчас модно говорить — это построение омни-канальных продаж. Компания должна обеспечить единую цену, достоверную и актуальную информацию о своих товарах во всех каналах продаж, предоставить покупателю возможность выбрать наиболее удобный для него способ коммуникации и обеспечить возможность завершить сделку, независимо от канала коммуникации.

В октябре 2015 года состоялся E-Commerce Congress, который стал своеобразным подведением предварительных итогов деятельности на рынке электронной коммерции за год, а также помог определить проблемные вопросы и дальнейшие пути их решения. E-Commerce Congress - 2015, как, собственно, и предыдущие мероприятия, это коммуникационная площадка, где участники рынка могут обсудить направления и этапы своего развития, требования рынка, поделиться своим опытом друг с другом, найти пути решения существующих проблем и т.д. Это своего рода предварительный итог каждого года работы рынка e-commerce на Украине.

Что же касается информационного наполнения мероприятия, то в ходе панельных дискуссий обсуждались вопросы правового регулирования рынка, особенностей мобильной коммерции, построения стратегий развития, сбора и применения больших массивов данных,

финансовых сервисов, операционных моментов доставки и фулфилмента, инвестиций в бизнес, выхода больших розничных сетей в онлайн.

В 2015 году панельные дискуссии были рассчитаны, как на больших игроков рынка, так и средний и малый бизнес. То есть у игроков «разного калибра» была возможность поделиться опытом. Кроме того, участие в мероприятии приняли и представители больших ритейловых сетей, которые уже в своей работе используют отечественные наработки рынка e-commerce. В ходе панельных дискуссий был отслежен один из новых трендов для развития направления в ближайшем будущем. Речь идет об углублении сегментации рынка. Другими словами, это означает, что игроки рынка e-commerce одним из направлений развития определили своего рода отступление от универсальности и переход на более узкоспециализированные направления.

В настоящее время украинский рынок электронной коммерции переживает свой «золотой век». Причин этому множество. В первую очередь, это, конечно же, увеличение доверия потребителей. По сравнению с 2010 годом, уровень доверия населения к платежным картам вырос более, чем в 10 раз. Этому, в свою очередь, поспособствовало появление новых платежных сервисов, усовершенствование их систем безопасности, а также упрощение самой процедуры онлайн-покупок. Кроме того, увеличение проникновения Интернета в жизнь граждан тут же влияет на рост показателей рынка электронной коммерции.

Ежегодно, объем украинского рынка e-commerce увеличивается на 30-40%. Согласно данным Национального банка Украины, доля безналичных расчетов в 2015 году, по сравнению с 2014-м, возросла почти на 60% и составила 3 мдрд. долларов США. По данным регулятора, только во втором квартале 2015 года интернет-платежи с использованием платежных карт составили более 45 млрд. грн. Более 111 млн. операций на общую сумму почти 43 млрд. грн. было осуществлено на Украине, а в зарубежных интернет-магазинах — менее 2 млн. платежей на сумму 2,5 млрд. грн. Более того, аналитики уверенны, что тенденция развития рынка Интернет-торговли на Украине будет прослеживаться и далее, и в 2016 году безналичные расчеты во всемирной сети достигнут показателя 5 млрд. долларов США. Кроме того, по прогнозам экспертов, тенденция роста сохранится еще не менее пяти лет.

На Украине существуют многие составляющие для успешности дальнейшего расширения рынка. В первую очередь, есть интеллектуальный ресурс вобласти ИКТ. Также есть неограниченное количество технических возможностей. Украина готова предлагать своим потребителям качественный и безопасный продукт. Продукты постоянно проходят проверки на соответствие мировым стандартам.

На Украине принят закон «Об электронной коммерции». Нормы и положения его определяют организационно-правовые основы деятельности в сфере электронной коммерции на Украине, устанавливают порядок совершения электронных сделок и определяют права и обязанности участников. Это приведет к повышению доверия потребителей данных услуг, увеличит объем инвестиций в e-commerce, а также позитивно скажется на темпах развития украинского рынка электронной коммерции.

Данный Закон на законодательном уровне урегулировал вопрос использования электронной подписи в сделках. Не менее важным является признание самих сделок, заключенных в электронной форме, и приравнивание их к бумажным. Кроме того, в законе было утверждено распространение закона «О защите прав потребителей» на пользователей услугами e-commerce.

Эта норма обезопасит потребителей от недобросовестных игроков на рынке, а также предоставляет целый ряд инструментов для отстаивания интересов потребителей.

Также следует отметить следующую важную норму, которая говорит о том, что интернет-магазин или любой другой субъект электронной деятельности не имеет права требовать от потребителей больше данных, чем ему необходимо непосредственно для проведения сделки. Отказ потребителя предоставить такие данные не может быть причиной отказа в сделке. В документе предусмотрены практически все нюансы деятельности юридических лиц, а взаимодействие частных лиц этот закон не определяет. Также, в законе не упоминаются операторы доставки, которые являются полноценными участниками электронных сделок, так как в более 30% случаев именно они отвечают за прием оплаты заказа. По большей части, этот закон соответствует европейским и принципам, и стандартам.

В августе 2015 года НБУ принял два Постановления №480 и №481. Анализ этих документов, Интернет-ассоциациацией Украины показал, что эти нормативно-правовые акты создают дискриминационные условия для национальных платежных систем, а также прямо противоречат действующему законодательству Украины. Подобные прецеденты препятствуют приходу иностранных инвесторов в страну.

Вопросы организации трансграничной Интернет-торговли (e-commerce) были рассмотрены в 2015 году по инициативе компании Ukrainian E-commerce Expert в ходе Бизнес-встречи «Трансграничный e-commerce (импорт в Украину): перспективы, ограничения и провайдеры услуг». Мероприятие посетили около 200 участников. Спикерами стали 23 эксперта рынка (AIN).

Рынок трансграничного e-commerce на Украине растет с каждым годом. Так, согласно данным Сообщества трансграничной электронной коммерции (Cross-border eCommerce Community) в 2012 году международные интернет-продажи достигли объема 300 млрд. долларов США, а к концу 2015 года должны были превысить 1,4 трлн. долларов США.

Украинский рынок кросс-бордера тоже активно развивается. Согласно данным исследования GfK, в 2014 году 30% онлайн покупок украинцы совершали за рубежом. На данный момент определено более 19 млн. пользователей сети, из них 2,8 млн. - это интернет покупатели (исследование GfK).

На Бизнес-встречи отмечалось, что рынок электронной коммерции на Украине с 2013 года до 2015 год вырос более чем в 4 раза, трансграничных платежей – в 3 раза (по количеству транзакций), то есть с сотни тысяч до пары десятков миллионов. НБУ предложил разделить отчетность по e-commerce на статистику по платежам общей электронной торговли (B2C и B2B) и трансграничной части.

Были даны рекомендации по работе с логистическими компаниями и рассмотрена возможность оплаты биткоинами (ПриватБанк).

Отмечалось, что некоторые товары дешевле за границей на 20-30%, чем на Украине, особенно в период скидок. Основным международным «шоппер-регионом» является г.Киев и областные центры. В 2015 году на их долю приходится 76% от всей доли зарубежных заказов. 37% доставок на Украину из-за рубежа приходятся на долю Meest Group.

Участники Бизнес-встречи пришли к общему мнению, что сегмент трансграничного e-commerce перспективен с точки зрения возможностей роста и заработка. Во-первых, оплата в трансграничном сегменте происходит всегда по безналичному расчету. Это выгодно государству и

самим игрокам. Так как последние все больше предпочитают работать в формате предоплаты. Фактически, трансграничная торговля меняет стереотипы отечественного e-commerce. Трансграничный сегмент может дать толчок для систематизации и стандартизации рынка электронной торговли в целом в Украине. Данный вид бзнеса представляет собой открытую нишу, на которую бизнес может сейчас обратить свое внимание, пока мировые гиганты e-commerce не вышли на украинский рынок в полном объеме. Основная причина недостаточного присутствия – слабая покупательская способность населения.

В тоже время отмечалось, что в настоящее время рынок Украины не замечает угроз со стороны иностранных проектов. Хотя есть несколько фактов, которые свидетельствуют об обратной ситуации. Например, с каждым годом становится все меньше барьеров для оплаты покупок за рубежом. Кроме того, провайдеры сервисных услуг (логистические операторы и финансовые компании) с каждым годом создают удобные условия и новые продукты, тем самым формируя лояльность украинских покупателей к иностранным интернет-магазинам. Потребители перестали бояться заказывать в «далеких» магазинах и готовы покупать несмотря на большие сроки доставки».

7. Развитие человеческого капитала

Республика Азербайджан

Согласно результатам 2013 года, 70% населения Азербайджана являются пользователями Интернета, в том числе 50% от их числа — пользователями широкополосного Интернета. Стоимость Интернета снижается из года в год. Так, по сравнению с 2004 годом стоимость подключения к Интернету со скоростью 1 Мбит/с сократилась с 1200 до 10 манатов. По стране средняя стоимость подключения к широкополосным услугам составляет 3% среднемесячной заработной платы. Это означает достижение поставленной МТС цели о том, что к 2015 году в развивающихся странах данное соотношение должно быть меньше 5%.

Из года в год растет производство в Республике Азербайджан компьютерного и электронного оборудования, программной продукции. В течение последних 5 лет сектор информационно-коммуникационных технологий страны расширился почти в два раза, а среднегодовые темпы роста составили 17%.

Исходя из достигнутого развития, вопросы информационной безопасности представляют важное значение с точки зрения организации защиты созданной инфраструктуры, информационных систем, собранной информации, а также создания условий для свободного использования гражданами и другими пользователями этих возможностей, и постоянно находятся в центре внимания.

В целях усовершенствования деятельности в этой области, защиты информационных ресурсов и систем государственных органов от возможных угроз, повышения общенациональной подготовки и просвещения по кибербезопасности в стране функционируют Государственное агентство безопасности специальной связи и информации Особой службы государственной безопасности Республике Азербайджан и Центр электронной безопасности при Министерстве связи и высоких технологий Республики Азербайджан.

Для обеспечения устойчивости проводимой работы и усиления национального потенциала расширяется подготовка высококвалифицированных кадров в области ИКТ. В «Государственной

программе по обучению азербайджанской молодежи в зарубежных странах в 2007—2015 годах», утвержденной Распоряжением Президента Республики Азербайджан от 16 апреля 2007 года №2090, подготовка высококвалифицированных кадров в области ИКТ признана приоритетным направлением.

Поддержка подготовки специалистов по ИКТ осуществляется также посредством функционирующего при Министерстве связи и высоких технологий Азербайджанской Республики Фонда развития человеческих ресурсов.

Для расширения возможностей использования развития ИКТ в обществе в первую очередь были созданы возможности для повышения знаний населения по ИКТ, информирования граждан о проводимой работе и имеющихся возможностях, а также деятельности общественных центров, создающих условия для доступности информации, и приобретения компьютеров на льготных условиях.

Государственной программой по обучению азербайджанской молодежи за границей (2007-2015 гг.), предусмотрено решение следующих важных задач:

- выявление спроса и предложения на различные профессии и специальности;
- совершенствование подготовки кадров, конкурентоспособных на рынке труда;
- переориентация системы образования на потребности рынка труда, т.е. на требования работодателей к знаниям, навыкам и умениям выпускников.

Высшее профессиональное образования (ВПО) в Республике Азербайджан можно разделить на две группы: ИТ-профильные специальности (основные), предусматривающие углубленное изучение ИТ, и специальности, потенциально готовящие специалистов для этой отрасли (дополнительные). Исследование данных относительно специальностей ВПО в Азербайджане позволило выделить списки вузов с ИТ-профильными факультетами, предусматривающими непосредственную подготовку ИТ-специалистов по соответствующим специальностям, охватывающим области профессиональной деятельности, связанные с разработкой и внедрением ИТ, составляющие основную группу специальностей. Вторая дополнительная группа специальностей, косвенно охватывающих области профессиональной деятельности, связанные с разработкой и внедрением ИТ, представлена не ИТ-профильными факультетами университетов (технические вузы), выпускники которых при необходимости имеют потенциал для освоения ИТ и могут войти в эту сферу.

Проведенный опрос среды респондентов, работающих в качестве ИТ-специалистов, как в столице, так и в регионах Азербайджана, выявил, что большинство из них имеют высшее образование или же учатся в вузах страны.

В университетах предлагаются новые компьютерные классы и лаборатории, электронные библиотеки и соответствующая сетевая инфраструктура, прямой контакт с ведущими компаниями и изучение современных технологий. Между тем, в период с 2007 по 2015 годы более пяти тысяч студентов отправились в ведущие университеты Соединенных Штатов Америки, Европы и Азии для обучения профессиям, в том числе в сфере ИКТ. Через свой фонд людских ресурсов для развития ИКТ министерство финансирует обучение около 200 студентов в зарубежных университетах.

Особо надо отметить деятельность появившихся в последнее время различных учебных центров. Среди них особо выделяется BSTC - Бакинский научно-учебный центр. Он является научно-исследовательским и учебным комплексом в системе Государственного комитета по науке и технике Азербайджана. На базе этого центра создан Республиканский центр

развития компьютерных технологий UNESCO/UNDP с обучением на азербайджанском, русском и английском языках. Центр оснащен современным оборудованием и доступом в интернет. Он сертифицирован компанией CISCO и на его базе создана региональная академия (Кавказ и Средняя Азия) по проекту «Cisco Networking Academy Program». В обучении используются кейс- и интернет-технологии, действует система очной подготовки ИТ-специалистов.

Деятельность подобных центров нацелена на подготовку молодежи в области ИТ и развитие современных информационных коммуникаций в регионах Азербайджана. Создано несколько ИТ-центров в других городах страны (городах Сумгаите в 1996 году, Нахичевани в 1999 году, Гяндже в 2002 году и других).

Организации, связанные с ИТ-образованием в Республике Азербайджан

Наименование	URL
Национальная Академия наук Азербайджана	http://www.science.az/ru/
Бакинский Государственный Университет	http://bsu.in-baku.com/
Бакинский научно-учебный центр	http://www.bstc.az/
Программа IATP на Кавказе	http://www.iatp.aznet.org/
Институт Открытое Общество Азербайджан	http://www.sd.aznet.org/
Азербайджанский технический университет	http://www.aztu.org/rus/
Азербайджанская государственная нефтяная академия	http://www.adna.baku.az/
Компания «Cisco Systems»	http://www.cisco.com/
Computer System	http://www.cs-az.com/
STREAM Technologies	http://www.streamtech.net/
Computex	http://www.computex.ws/
Bakinity	http://www.bakinity.biz/
Кавказский Университет	http://www.qafqaz.edu.az/
Университет «Хазар»	http://www.khazar.org/
Нахичеванский Государственный Университет	http://www.ndu.edu.az/

В настоящее время в Азербайджане имеется около 50-ти высших учебных заведений, где проходят обучение почти сто тысяч студентов. К крупнейшим вузам страны относится Азербайджанский государственный университет им. Расулзаде (основан в 1919 году, около 11 тысяч студентов), Институт нефти и химии (основан в 1920 г., около 15 тысяч студентов), Азербайджанский технический университет, Азербайджанский педагогический институт русского языка и литературы им. М. В. Ахундова, Азербайджанский государственный институт иностранных языков, Азербайджанский медицинский университет им. Н.Нариманова, Государственный сельскохозяйственный институт в Гяндже, Азербайджанский государственный экономический университет (АГЭУ), Азербайджанская государственная нефтяная академия (АГНА) и другие. В этих вузах имеются подразделения и учебные центры для подготовки ИТ-специалистов различного уровня.

В последние годы в Азербайджане появились и негосударственные ВУЗы. К ним относится, например, открытый в 1991 году Хазарский университет с обучением на английском языке, Западный университет (одна тысяча студентов), Кавказский университет с обучением на турецком языке, и другие. В стране имеются филиалы Дагестанского и Днепропетровского университетов.

В стране пока еще недостаточно оснащены современной техникой школы, ВУЗы, научные и культурные учреждения, получающие финансирование из государственного бюджета.

Республика Армения

В рамках Концепции «Образования электронного общества в Республике Армения», принятой Решением Правительства Республики Армения 25 февраля 2010 года, отмечается необходимость создания Государственного органа по обеспечению информационной безопасности, в составе которого предусматривается формирование Национальной группы быстрого реагирования на компьютерные инциденты.

Одним из актуальных вопросов является создание отдельного учебного центра по подготовке высококвалифицированных специалистов в области ИКТ и информационной безопасности.

Реализация правительством Концепции развития сферы информационных технологий будет содействовать внедрению информационных и телекоммуникационных технологий в различных сферах экономики, обеспечит представление новейших и инновационных программных и технологических решений для автоматизации бизнеса, стимулирование развития различных сфер предпринимательства посредством внедрения современных технологий.

В 1998 году создана компания BEVER (BVR) по сборке ПК с привлечением специалистов НИИ математических машин. В настоящее время компания практикуется на современной и высокотехнологичной сборке компьютерной техники, поставке программно-аппаратных средств для автоматизации бизнес-процессов. В рамках компании был создан учебный центр BVR-training&consulting. При центре образована школа юного программиста, в которой на школьном уровне преподается операторское дело и начальное программирование.

С 2003 года при компании Arminco действует учебный центр по подготовке ИТ-специалистов, сертифицированный компанией Microsoft. В Ереванском государственном университете работает учебный ИТ-центр. При содействии Бременского университета здесь начато преподавание нового предмета — «индустриальная математика». В Российско-Армянском (Славянском) государственном университете при содействии американской компании «Интермек» создана лаборатория идентификации радиочастот и штрих-кодов. Лаборатория стоимостью примерно в 30 тыс. долларов США была подарена американцами. Курс обучения, по которому идет подготовка преподавателей в университете, предоставил Университет Огайо (США).

В 2001 году при поддержке компании LEDA Systems создана кафедра «Системы и схемы микроэлектроники» совместно с Государственным инженерным университетом Армении. В 2002 году американская компания Kaidens dissgn systems и LEDA Systems предоставили кафедре программный пакет по автоматическому проектированию стоимостью в 25 миллионов долларов США. В 2003 году на кафедре прошли подготовку несколько десятков студентов по

специальности «проектирование систем и схем микроэлектроники» и начато обучение специалистов программному обеспечению для проектировки полупроводниковых микросхем.

Вместе с тем, подготовка по техническим профессиям, имеющим спрос на рынке, пока не имеет достаточной аппаратурно-методической основы. Поэтому происходит совмещение учебной, исследовательской и коммерческой деятельности в различных организациях.

Научно-исследовательский институт компьютерной техники и информатики (в прошлом — НИИ «Алгоритм») в настоящее время занимается проектами по производству и экспорту компьютерной техники в страны СНГ. Используя международную сертификацию и связи компании-партнера CIP, НИИ ведет работу по экспорту информационных технологий в ряд регионов России, Казахстана, а также в Иран. Большинство местных ИТ-компаний действуют в качестве филиалов крупных иностранных компаний. Поскольку в Армении нет рынка сбыта для высокотехнологичного производства, почти весь объем работы исполняется для иностранных заказчиков.

Большая часть программ и проектов в области ИТ-образования Армении реализуется на средства доноров — международных организаций и фондов. Программа Развития ООН (UNDP) обеспечивает бесплатным доступом в интернет около 16 тысяч пользователей. Программа IATP бесплатно предоставляет интернет- услуги в г.Ереване и регионах страны. Project Harmony вместе с ACCELS на свои средства обеспечили более 80 школ компьютерами и подключением во Всемирную Сеть. На средства Госдепартамента США, Фонда гражданских исследований и развития США (NFSAT) создан Национальный фонд научных и прогрессивных технологий с уставным капиталом в 1,2 млн. долларов США. Он ориентирован на выдачу грантов по сотрудничеству в фундаментальных науках, поддержке молодых ученых и другое.

В настоящее время в Республике Армения создано достаточно много центров, занимающихся обучением в области ИТ, — от курсов компьютерной грамотности до языков программирования. Большинство из них, исключая действующие на гранты зарубежные организации, работают на платной основе. Тем не менее, развитие методов дистанционного образования на основе интернет-технологий, помимо проблем с телекоммуникационной сетью, сдерживается низким уровнем обеспечения ПК и компьютерной периферии.

По некоторым оценкам, в частном пользовании имеется только несколько тысяч ПК, а уровень обеспечения ими организаций и учреждений крайне низок. В Армении пока нет методик обучения на армянском языке, являющегося основным в учебных заведениях страны. Учебники по операционным системам и некоторым прикладным программам имеются в основном на русском и английском языках.

Республика Беларусь

Республика Беларусь активно участвует в выработке подходов к подготовке специалистов в области ИКТ.

В сентябре 2015 года в г. Минске состоялось 1-е заседание Совета по развитию людских ресурсов РСС. В работе заседания приняли участие представители Администраций связи: Азербайджанской Республики, Республики Армения (он-лайн) Республики Беларусь, Республики Казахстан, Кыргызской Республики, Республики Молдова (он-лайн), Российской Федерации,

Республики Таджикистан, а также участники Совета операторов электросвязи и инфокоммуникаций РСС: Руководитель РУП «Белтелеком» и «БелХуавэйТехнолоджис», участник Совета операторов почтовой связи: Руководитель РУП почтовой связи «Белпочта», Председатель Республиканского комитета Белорусского профсоюза работников связи и Исполкома РСС. В работе заседания приняли участие более 40 представителей от Администраций связи РСС и приглашенных лиц. В качестве приглашенных приняли участие представители: Исполкома РСС СНГ, Зонального отделения МСЭ для стран СНГ в г. Москве, АО «Национальный инфокоммуникационный Холдинг «Зерде» (Республика Казахстан), Таджикского национального университета (Республика Таджикистан), Вроцлавского технологического университета (Республика Польша), Университета г. Жилины (Словацкая Республика), НП "Учебный центр Хуавэй" (г. Москва), Учебный центр Алкатель – Лусент (г. Москва).

Совет открыл свою работу с обсуждения вопроса «О сотрудничестве в области образования, подготовке кадров и развитии людских ресурсов в странах участников РСС». Представитель Исполкома СНГ А.Н. Харченко ознакомила участников заседания с деятельностью Совета по сотрудничеству в области образования государств – участников СНГ. Также в рамках рассмотрения первого вопроса вниманию участников был представлен доклад ректора Высшего Государственного колледжа связи Республики Беларусь О.А. Зеневича – «Об инновационных решениях в области образования в Республике Беларусь». Далее участниками заседания был утвержден План работы Совета по развитию людских ресурсов РСС на 2015 – 2017 гг.

Вопрос о правовом обеспечении и регулировании вопросов кадровой политики в Администрациях связи РСС был рассмотрен в формате круглого стола, на котором представители Администраций связи РСС обменялись мнениями и опытом работы в данном направлении. Заместителем Председателя правления АО «Национальный инфокоммуникационный холдинг «Зерде» К.Б. Елеусизовой был представлен доклад - «Бакалавриат производственного направления» в системе высшего профессионального ИКТ-образования Республики Казахстан, в котором была предложена новая модель подготовки ИКТ - кадров.

В ходе заседания был рассмотрен вопрос о деятельности «Центра мастерства» МСЭ для стран СНГ в рамках новой Стратегии МСЭ о центрах мастерства, было заслушано выступление руководителя Зонального отделения МСЭ для стран СНГ О.Ж. Кайыкова и отчет Председателя Руководящего комитета Центров профессионального мастерства МСЭ для СНГ В.А. Каптура.

В рамках рассмотрения вопроса «О создании и деятельности Учебных центров на базе ВУЗов стран участников РСС» была заслушана информация:

- Заместителя Генерального директора Исполкома РСС Н.Е. Зоря - об открытии Регионального учебного центра ВПС для специалистов почтовой связи РСС;

- Заместителя директора ООО «Бел Хуавэй Технолоджис» Бондарева Максима Сергеевича - об участии компании HUAWEI в подготовке специалистов в области ИКТ стран участников РСС;
- Генерального директора «Учебный центр Алкатель - Лусент» - «Учебный Центр Алкатель-Лусент Г.Б. Буровой – «Развитие региональных образовательных площадок по подготовке специалистов в области ИКТ стран участников РСС»;

- Заместителя Генерального директора «ЭРИКССОН Трейнинг Центр» И. Б. Салтыковой «Обучение ИКТ в условиях экономического кризиса в странах-участниках РСС». Участники заседания ознакомились с опытом ВУЗов Восточной Европы по реализации программ

подготовки и повышения квалификации кадров, заслушав информацию профессора Вроцлавского технического университета (Республика Польша) Войцеха Криштофика и профессора Университета г. Жилины (Словацкая Республика) Милана Дадо.

В Республике Беларусь есть особая экономическая зона со специальным налогово-правовым режимом, для создания благоприятных условий для разработки программного обеспечения, информационно-коммуникационных технологий, направленных на повышение конкурентоспособности национальной экономики под названием Белорусский парк высоких технологий. Основной целью парка является создание условий для развития ИКТ-индустрии в целях ускоренного развития услуг в области информационных технологий в Республике Беларусь, привлечения заказов по разработке ИКТ-продукции, содействие росту валютных поступлений в Республику Беларусь.

Грузия

В 2000 году в соответствии с указом президента Грузии (№411) был утвержден Устав специальной Национальной комиссии по коммуникациям Грузии. Создание комиссии оказало позитивное влияние на развитие информационно-коммуникационных технологий в Грузии. Для рынка ИКТ характерен высокий уровень либерализации и в него вовлечено много компаний.

Организации, связанные с ИТ-образованием в Грузии

Наименование	URL
Организация CIT (Грузия)	http://www.prometric.ge/ru/
Центр дистанционного образования (Грузия)	http://edu.internet-academy.org.ge/
Многопрофильная академия им. Н.Николадзе	http://www.geo-plus.net/Gma/
Ассоциация современных научных исследований	http://www.amsi.ge/
Клуб молодых ученых INTELLECT (Грузия)	http://www.iberiapac.ge/
Фонд Открытое Общество Грузии	http://www.osgf.ge/
Prometric Testing Центр APTC GE1 (Грузия)	http://www.inspe.edu.ge/
Computer Educational Center ACS	http://acs.gol.ge/
Geotest (Professional IT Training and certification service)	http://www.certification.ge/
Internet Development Group-Georgia	http://idg-georgia.org.ge/
Mziuri International	http://mziuri.gol.ge/
Association of Professional Education Development	http://aped.gol.ge/
Distance Learning	http://edu.internet-academy.org.ge/
Institute of Mechanics of Machines	http://www.argosoft.com/mathsim/
Internet Academy	http://www.internet-academy.org.ge/
Security Systems in Georgia	http://general-security.ge/
ELITE-RC Co. LTD (Грузия)	http://www.elite-rc.com/
Компания Cerma (Грузия)	http://www.cerma.ge/
JULIA Ltd (Грузия)	http://www.julia.gol.ge/

Создание конкурентоспособной среды обеспечивает относительно низкие цены на пользование интернетом и начинает формировать рынок ИТ-специалистов в стране, стимулируя необходимость получения качественного образования. В Грузии все большее число учебных заведений оснащаются вычислительной техникой.

С 1997 года обучение в начальной школе Грузии длится 6 лет, после этого дети переходят в двухлетнюю базовую школу или профессионально-техническую школу (возраст учащихся 12–14 лет). Средняя трехлетняя школа делится на общеобразовательную,профессионально-техническую и специальную (возраст учащихся 14–17 лет). Преподавание предметов в большинстве школ ведется на грузинском языке. На русском языке обучение ведется примерно в двухстах школах Грузии.

Во многих ВУЗах Грузии создаются и работают отделения компьютеризации и информатики. В ряде из них созданы факультеты информационных и компьютерных наук. После 1990 года в Грузии появились частные учебные заведения и основанные на международном партнерстве новые институты — Европейская школа менеджмента и Институт государственного управления.

Организация CIT специализируется на продвижении профессионального образования и разработке информационных технологий в Грузии. A Prometric Testing Центр APTC GE1 занимаемся поддержкой профессионального образования и организацией дистанционной международной сертификации. Другой центр — Sylvan Prometric, авторизированный представитель в Грузии Sylvan Learning Systems Inc. — занимается тестированием в области информационных технологий, бизнеса и других сфер образования на базе интернет-технологий. Авторизированные Prometric Testing тесты кодируются и передаются в авторизированные центры индивидуально на каждого кандидата. Результаты тестов оцениваются, кодируются и передаются обратно в Sylvan Prometric.

В настоящее время государство не располагает достаточными средствами для поддержки учебных заведений и НИИ. Только благодаря помощи зарубежных организаций в стране проводятся актуальные исследования и налаживается сотрудничество с зарубежными институтами. Уровень заинтересованности грузинских организаций в высококвалифицированных и сертифицированных специалистах в области ИТ пока недостаточно высок.

По совместным программам НАТО, INTAS и OSGF была оказана помощь Академии наук Грузии в создании компьютерной сети с выходом в интернет. Фонд «Евразия» выделил несколько грантов для поддержки сетевых проектов. Благодаря деятельности международных организаций в Институте высоких энергий и Институте вычислительной математики Академии наук Грузии созданы некоммерческие интернет-центры, в которых ведется подготовка ИТ-специалистов.

В 2011-2012 годах в Грузии при поддержке МСЭ с целью совершенствования профессиональной подготовки и развития человеческого потенциала были созданы два «Интернет тренинг центра МСЭ – Cisco» (в г.Тбилиси и г. Батуми).

Республика Казахстан

Все больше и больше ИКТ проникают и в образование. Как заявляет Министр образования и науки Республики Казахстан: «Важный аспект, затрагивающий все уровни подготовки, – широкое внедрение электронного обучения – e-learning». E-learning – система электронного обучения при помощи информационных, электронных технологий. Развитие электронного обучения становится элементом политики государства. Организационной основой реализации государственной политики Республики Казахстан в сфере образования является Государственная программа развития образования Республики Казахстан на 2011-2020 годы, обеспечивающая продолжение модернизации казахстанского образования.

Нормативная правовая база системы электронного обучения разрабатывается на основе международных стандартов и технических регламентов эксплуатации системы электронного обучения.

Реализация проекта «E-learning» предусмотрена в два этапа. На 1 этапе более 50% организаций образования получат широкополосный доступ к сети Интернет (от 4-10 Мб/сек), будут иметь локальную сеть (свободный доступ к образовательному контенту) Wi-Fi, Wi-Max, будут обеспечены электронными библиотеками, не более 10 учащихся на 1 ПК.

На 2 этапе уже более 90% организаций образования получат все возможности к сети Интернет, иметь свободный доступ к образовательному контенту, не более 1 учащихся на 1 ПК.

В 2015 году планировалось охватить электронным обучением 50% организаций образования, а к 2020 году 90% будут охвачены электронным обучением все уровни подготовки. В дошкольном воспитании будут использоваться компьютерные программы, компьютерные обучающие игры, в средней школе – электронные учебники электронные пособия, в колледжах и профлицеях – виртуальные тренажеры, в вузах – электронные научно-исследовательские лаборатории. В соответствии с ним организации образования планируется обеспечить широкополосным Интернетом, приобретение порядка полумиллиона компьютеров и более восьми тысяч серверов, чтобы от сегодняшнего соотношения – один компьютер на 18 учащихся – перейти к соотношению 1:1, что соответствует уровню самых развитых стран. Кроме того, будут разработаны современные интерактивные обучающие и управляющие ресурсы, содержащие текст, графику, музыку, видео, анимации и различные мультимедийные технологии.

В Концепции системы электронного обучения на 2010-2015 годы определяются приоритеты по созданию единой информационной образовательной среды. В частности, требуется «сформировать основы единой системы информационного и научно-методического обеспечения развития образования и создать отраслевую информационную систему для эффективного управления объектами и процессами образования».

В Республике Казахстан на уровне государства проводится большая исследовательская и практическая работа по внедрению и развитию ИКТ. Такие преобразования касаются всех отраслей экономики, в том числе образования. Для развития и внедрения ИКТ возникает необходимость в высококвалифицированных кадрах.

Для решения этого вопроса по инициативе Президента страны Н. Назарбаева в 2009 г. был открыт первый в Республике Казахстан Международный университет информационных

технологий (МУИТ). Сегодня это отраслевой ВУЗ страны по ИТ технологиям, соответствующий мировым стандартам. Ключевым партнером университета в образовательном процессе является бизнес-школа iCarnegie (структурное подразделение университета Carnegie Mellon) с 10 образовательными модулями в области программного обеспечения. Кроме того, учреждение работает в тесном сотрудничестве с университетами Малайзии: University Tenaga Nasional (Uniten), Universiti Teknologi Mara (UiTM), Universiti Kuala Lumpur (UniKL) и Multimedia University, а также с Варнским свободным университетом (Болгария) и др. Мировой опыт позволяет подготовить универсальных сертифицированных ИТ-специалистов, способных соответствовать вызову отечественной Инновационной стратегии Казахстана по выходу в число высококонкурентных стран.

МУИТ имеет оснащенную материально-техническую базу. Открыты лаборатории облачных вычислений Huawei и Apple Training center. Профессорско-преподавательский состав вместе со студентами и магистрантами ведет научно-исследовательские работы по современным направлениям ИКТ. Это исследование облачных технологий; разработка и исследование моделей, методов и алгоритмов распознавания образов и принятия решений для интеллектуальных информационных технологий и систем; разработка математических моделей, численных методов и программных комплексов идентификации и распознавания синхронизированного потока звуковых и графических сигналов; компьютерная графика и искусственный интеллект, робототехника и др.

Разработка и развитие программ подготовки ИКТ-специалистов проводится в тесной связи с ведущими ИТ-компаниями Республики Казахстан, такими, как НИКХ «Зерде», которые помогают определить основные направления подготовки специалистов, перечень специальностей, востребованных на рынке ИКТ, гармонизировать учебные планы с современными мировыми стандартами в информационных технологиях. МИУТ постоянно обновляет и создает учебные программы, руководствуясь исследованиями и разработками в мире ИКТ.

Подготовка специалистов в области ИКТ является обязательным условием экономического роста государства. В ходе реформы образования, проводимой в настоящее время в Республике Казахстан, ищутся пути совершенствования подготовки таких специалистов. Такая необходимость обусловлена постоянно возрастающими требованиями к их квалификации, ростом потребности экономики в этих специалистах и тем, что эти требования в настоящее время приобретают международный характер.

Кыргызская Республика

Основой для современного образования в Киргизии является Советская система. После обретения независимости были проведены реформы в сфере образования.

Школьное образование расчитано на 11 лет, из них 9 обязательны. Начальная школа — с 1 по 4 класс, обучаются дети с 6-7 до 11 лет. В начальной школе детей обучают базовым знаниям, такими как письменность, литература, изучение языков, арифметика, уроки труда, этики и спорт. Средняя школа — с 5 по 9 класс, дети с 12 до 16 лет.

В средней школе начинают изучение научных предметов, математика, информационные технологии, углубленное изучение иностранных языков и другие.

Старшая школа — 10-11 класс. Несмотря на то, что 10-11 класс являются не обязательными, более 80 % школьников обучаются в старшей школе. Здесь ученики проходят те же предметы, что и в средней школе, начинается военное дело, а также выбирают будущие специальности, изучают предметы по своей будущей профессии и готовятся к поступлению в вузы. По окончании 11 класса, школьники сдают выпускные экзамены и Общереспубликанское тестирование (ОРТ), по результатам которого идет набор в университеты. В начале 90-х годов начали создаваться школы-гимназии с углубленным изучением отдельных предметов и специальностей.

В 2000 г. количество общеобразовательных государственных школ составило — 1975 школ. В настоящее время их уже более 2-х тысяч. В крупных городах открываются частные элитные школы.

В 1990 год в республике было только 9 вузов, где учились 58,8 тыс. студентов. К началу 2010-х годов число ВУЗов достигло 52, из которых 36 государственные. Число студентов также увеличилось и в начале 2010-х годов составило около 220 тыс. В республике функционируют международные «совместные» вузы: Кыргызско-Российский (Славянский) университет, Кыргызско-турецкий университет «Манас» и Кыргызско-турецкий университет «Ала-тоо», Американский университет в Центральной Азии.

В 2004 году создан Национальный центр информационных технологий (IT-Center KG) при содействии Японского Агентства Международного Сотрудничества (JICA) в ходе реализации совместного кыргызско - японского проекта «Развитие человеческих ресурсов в сфере IT-технологий в Кыргызской Республике». Решением Государственной инспекции по лицензированию и аттестации учреждений образования Национальный центр информационных технологий имеет право на ведение образовательной деятельности в сфере дополнительного образования (лицензия АШ № 2061) по следующим направлениям: системный анализ; управление проектами; базы данных; разработка программного обеспечения.

Решением Правительства Кыргызской Республики 3 декабря 2012 года образован наблюдательный совет Парка высоких технологий. Закон «О Парке высоких технологий» был принят в 2011 году, однако далее не последовало конкретных действий по реализации данного закона. Закон создает правовую основу государственной поддержки развития индустрии разработки ПО, а также функционирования Парка высоких технологий, его органов управления, резидентов, основные принципы формирования режима Парка высоких технологий, включая основные принципы налогообложения резидентов.

К 2012-му году была начата популяризация проекта «Кыргызская Википедия» По состоянию на 21 декабря 2012 года Киргизский раздел Википедии содержит 21 390 статей. Зарегистрировано 6572 участника, из них 103 наиболее активные. 5 участников имеют статус администратора. Общее число правок составляет 140 034. По числу статей проект занимает 105 место, а по числу правок только 164 место. Также создано мобильное приложение для планшетных компьютеров и смартфонов, позволяющее читать Википедию на кыргызком языке и использовать кыргызские словари.

На кыргызском рынке ИКТ, ИТ-специалисты, программисты, системные администраторы получают в среднем от 2 долларов США в час в государственных организациях, и от 15 до 80 долларов США в час в коммерческом секторе, который тесно связан с международным рынком

ИКТ. Для сравнения - в мире средняя цена одного часа работы программиста стоит от 1,5 долларов США, как в Индии, до 1500 долларов США, как в США.

С целью поддержки ЛОВЗ в 2012-м году стартовал обучающий проект как на своей активности заработать в социальных сетях. Проект планируется расширить и выйти на национальный уровень. Обязательным требованием успешности проекта остается наличие безлимитного Интернета. Сумма заработка будет варьироваться от 25 до 400 долларов. Проект реализуется при финансовой поддержке Фонда «Открытое общество» и Молодежной программы Фонда «Сорос–Кыргызстан».

Ряд экспертов выражают мнение, что при надлежащем отношении в рынку ИКТ, урегулированию законодательных вопросов и формировании национальной стратегии ИКТ, приближенной к реалиям кыргызскихИТ-компаний и потребностям пользователей можно добиться больших результатов. Политика государства с учетом менталитета страны является одним из ключевых факторов развития ИКТ-сектора. Для популяризации и поддержки ИКТ-сектора необходимы меры со стороны государства в виде декларирования стратегической важности развития отрасли ИКТ и создания условий для развития.

ИКТ-сектор остро ощущает не хватку кадров - технических и управленческих. Необходимо выстроить целый кластер: физмат или компьютерная школа - технический вуз/факультет – IT-компания разработчик ПО, IT- компания управляющая создание инфраструктуры Интернет и телекоммуникаций, IT-консалтинг, Интернет компания и т.д. по нарастающей.

В стране существует программа «Электронная школа», но компьютеризация на уровне «1 компьютер (1 планшет) - 1 ребёнок» присутствует не везде, равно как и бесперебойное электричество с Интернетом. Уровень образования не вполне соответствует международному уровню.

Через 54 высших учебных заведения республики проходят ежегодно около 240 тысяч человек. Но количество заведений - не показатель качества работы. Учёная степень есть только у 10% преподавателей. Из-за низкой зарплаты многие профессора и академики читают лекции в нескольких университетах, что сказывается на качестве преподаваемого материала. Учебный материал изрядно сокращён благодаря переходу Кыргызской Республики на двухуровневую Болонскую систему «бакалавр-магистр» с 1 сентября 2012 года. Предполагалось, что система сократит ненужные предметы и покроет потребности рынка труда. Однако по данным Минтруда Кыргызской Республики, трудоустроиться по-прежнему могут лишь около 10% выпускников вузов. В 2015 году 70% спроса на рынке труда составили заявки на рабочие профессии и специалистов в области сферы услуг: поваров, парикмахеров, водителей, работников СТО, строителей, официантов.

На 2015-2016 учебный год прекращён набор на непрофильные специальности и сокращены бюджетные места. В 2016-2017 годах внедрится принцип госзаказа на специалистов, будет проведён мониторинг эффективности вузов и по их итогам самые слабые закроют. Сильным обещают техническое оснащение и всяческую поддержку. В настоящее время, к сожалению, многие кыргызстанцы едут в Казахстан, Россию, США, Турцию, Китай, Малайзию за более качественным образованием.

В 2015 году Нарынском государственном университете им.С.Нааматова состоялся семинар по обсуждению роли вузов в продвижении открытых образовательных ресурсов (ООР).

Участниками мероприятия стали преподаватели, руководители факультетов НГУ им.С.Нааматова, студенты и библиотекари города Нарын. В программе семинара были представлены доклады о процессе разработки открытых электронных образовательных ресурсов, дистантном образовании в НГУ, электронной библиотеке http://www.kyrlibnet.kg/, открытых лицензиях Creative Commons. Нарынский государственный университет с сентября 2014 года реализует проект «Образовательный веб-портал Нарынского государственного университета» при финансовой поддержке программы «Свобода информации» Фонда «Сорос – Кыргызстан».

Ведущую роль в подготовке специалистов в области информационно-коммуникационных технологий в Кыргызской Республике играет Институт электроники и телекоммуникаций при Кыргызском государственном техническом университете имени И.Раззакова (http://iet.kg/).

Республика Молдова

В Республике Молдова (РМ) создана и действует законодательная база подготовки специалистов в области телекоммуникаций/ИКТ:

Президентская программа по внедрению ИКТ в системе образования «SALT», утвержденная постановлением Правительства РМ № 1424 от 22 декабря 2004 г. «О достижениях президентской программы SALT»;

Постановление Правительства РМ от 8 июня 2004 г. № 632 «Об утверждении политики создания информационного общества в РМ»;

Постановление Правительства РМ № 255 от 9 марта 2005 г. «О Национальной стратегии развития информационного общества «Электронная Молдова»;

Постановление Правительства РМ № 863 от 16 августа 2005 г. «Об утверждении Программы по модернизации системы образования в РМ», которое предусматривает актуализацию учебных планов для профессионально-технического, среднего специального и высшего образования в целях формирования у будущих выпускников способности пользоваться ИКТ;

Постановление Правительства РМ № 373 от 12 апреля 2006 г. «О реорганизации Центра новых информационных технологий»;

Постановление Правительства РМ № 270 от 13 апреля 2007 г. «Об утверждении Концепции информационной системы образования (ИСО)».

Государственная политика в области использования ИКТ в системе профессионального образования была определена постановлением Правительства № 632 от 8 июня 2004 г. «Об утверждении политики по созданию информационного общества в РМ». Этот документ ориентируется предусматривает поддержку компьютеризации учреждений системы образования и обеспечение их доступа к глобальной сети Интернет; внедрение ИКТ в воспитательный процесс, обеспечение постоянного обмена информацией по инновациям в области образования в целях развития и распространения современных технологий; развитие системы дистанционного образования как новой формы повышения квалификации специалистов; развитие научных исследований в области дистанционного образования и внедрения ИКТ в систему образования.

В целях реализации Указа Президента № 1743-III от 19 марта 2004 г. «О создании информационного общества в РМ» и постановления Правительства № 632 от 8 июня 2004 г. «Об утверждении политики по созданию информационного общества в РМ», Правительство утвердило Национальную стратегию по развитию информационного общества «Электронная Молдова». Главная цель Стратегии – установление принципа электронного образования (e-educatie) в системе общего образования и профессионально-технического образования (ПТО), т.е. использование ИКТ в целях повышения эффективности процесса преподавания и обучения, а также стимулирование навыков саморазвития на протяжении всей жизни. План действий по реализации Национальной стратегии предусматривал, что к 2015 г. 50% педагогических кадров будут пользоваться компьютерами, а 40% - будут использовать Интернет в своей дидактической деятельности на уроке. Кроме того, планировалось, что к 2015 г. 85% образовательных учреждений будут иметь свои веб-сайты.

Постановлением Правительства № 270 от 13 марта 2007 г. была утверждена Концепция информационной системы образования (ИСО). ИСО представляет собой набор средств программного обеспечения (software) и технического оборудования (hardware), информационных и организационных средств (включая вопросы инфраструктуры и персонала), систем передачи данных и технологий их обработки и использования, а также методов, законодательных норм, предназначенных для создания информационной базы для системы образования страны. В целях реализации Концепции была разработана техническая документация для двух подсистем ИСО: внедрение ИКТ в сфере образования и подготовка педагогических и менеджерских кадров.

В 2006 г. начал свою деятельность Центр информационных и коммуникационных технологий в системе образования (ЦИКТСО). Он осуществляет непрерывное профессиональное развитие всех преподавателей информатики, в том числе системы ПТО. Кроме того, Центр занимается научными разработками в данной области. Ежегодно Центр готовит около 465 преподавателей (локальных тренеров) для районов республики, свыше 200 учителей (в целях использования образовательного программного обеспечения), около 200 менеджеров и преподавателей информатики. Также в 2010 г. прошли обучение и сертифицированы в качестве инструкторов по внедрению платформ электронного обучения (e-Learning platforms) 35 преподавателей общеобразовательных, профессионально-технических и высших учебных заведений страны. По приказу Министра образования РМ были разработаны и утверждены требования по пилотному внедрению ИКТ в систему образования, инициированному в четырех теоретических лицеях и одном профессионально-техническом училище. В этих учреждениях было использовано образовательное ПО по четырем предметам: математика, физика, химия и биология. Также было дополнительно приобретено образовательное ПО по вышеназванным дисциплинам для обеспечения более чем 200 учебных заведений страны (в том числе 5 ПТУ). Планировалось расширить этот эксперимент по разработке и внедрению ПО по учебным дисциплинам для специальностей в сфере строительства и сельского хозяйства.

Приоритеты в области обеспечения равного доступа для различных групп пользователей к социально значимым образовательным сервисам были определены в Программе деятельности Правительства РМ «Европейская интеграция: свобода, демократия, благосостояние 2011–2014» и предполагают:

- развитие информационной культуры, обучение всего населения, нуждающегося в услугах информационного общества для работы и повседневной жизни;

- демократизацию в использовании информации в целях обеспечения прав граждан на свободный доступ к информационным ресурсам и информационным и коммуникационным средствам связи;
- внедрение и развитие информационной и коммуникационной инфраструктуры в сфере публичного управления для улучшения предоставляемых услуг по доступным ценам;
- рост доверия общественности к информационным системам за счет обеспечения безопасности, защиты личных данных и неприкосновенности частной жизни;
- обеспечение равного доступа всех граждан к информации, услугам и знаниям с учетом потребностей каждого.

В связи с этим в последние годы в результате программ по обеспечению равного доступа для различных групп пользователей к социально значимым образовательным сервисам Молдовы наблюдаются: рост плотности мобильной и фиксированной телефонной связи, расширение доступа к информационным ресурсам, улучшения в плане надежности предоставляемых оптоволоконных и спутниковых международных соединений, рост числа Интернет- провайдеров и пользователей данными услугами. Несмотря на это, степень использования населением преимуществ информационных технологий еще остается низкой.

Развитие дистанционного образования в качестве новой формы профессиональной подготовки и переподготовки специалистов было закреплено в постановлении Правительства от 8 июня 2004 г. № 632 «Политика создания информационного общества в РМ». В рамках программы «Темпус» Государственным институтом непрерывного образования (ГИНО) реализовывался проект «Внедрение модулей дистанционного обучения и электронных учебников в пилотных учреждениях высшего и непрерывного образования». В ГИНО была установлена и адаптирована к местным потребностям система MicroC@MPUS – программа дистанционного образования (ДО), которая соединила в себе возможности «классического» обучения с современными информационными технологиями, основанными на интерактивной работе преподавателя с обучающимися. В этом отношении ситуация в ПТО менее удовлетворительна. Первым серьезным шагом на пути развития данной сферы стало образование Республиканского центра развития профессионального образования, открытого по приказу Министерства образования РМ (приказ № 835 от 17 декабря 2008 г.) и при поддержке проекта технической помощи «Улучшение системы образования и профессиональной подготовки», внедренного Hifab International на базе Института педагогических наук. Центр призван обеспечить теоретическую и методологическую базу для системы профессионального образования в РМ, в том числе его деятельность направлена на создание условий для поэтапного перехода на новый уровень образования на базе ИКТ. Центр разработал и разместил на своем сайте три модульных учебных плана (curriculum) и материалы для модулей (для специальностей «Штукатур», «Сварщик» и «Повар»), учебник по предпринимательству, базу данных и модули для краткосрочных курсов по профессиональному обучению взрослых.

В начале 2010–2011 учебного года в системе ПТО было задействовано 2257 работников. В целях обеспечения их непрерывного профессионального развития Министерство образования РМ приняло определенные меры, в том числе открытие новых центров для повышения квалификации педагогических и руководящих кадров (на 2011г. насчитывалось 13 таких центров по всей республике). Преподаватели дисциплин по техническим специальностям и мастера

производственного обучения из системы специального профессионального образования (ССПО) проходят учебные курсы в Центре дополнительного образования Технического университета Молдовы. Аналитические программы, утвержденные Министерством образования для всех категорий педагогических кадров, содержат модули в области ИКТ. Согласно Приказу № 790 от 1 ноября 2010 г. «Об утверждении планов по непрерывному профессиональному образованию дидактических и менеджерских кадров системы образования на 2011 г.», ЦИКТСО организует курсы: Методика преподавания информатики, I уровень; Методика преподавания информатики, II уровень; Использование платформы электронного обучения, курс внедрения ИКТ; Основы использования ИКТ, вводный курс ИКТ; Адаптация и развитие образовательных ресурсов, промежуточный курс в области ИКТ. Преподавание ведется на румынском и русском языках.

Непрерывное профессиональное образование (в том числе дальнейшее развитие ИКТ-компетентности) педагогических и руководящих кадров в системе среднего профессионального образования регулируется Законом об образовании № 547-XIII от 21 июля 1995 г. и постановлением Правительства № 1224 от 9 ноября 2004 г.

На сегодняшний день в отношении среднего профессионального образования в РМ внедрение новых технологий в процесс обучения находится на начальном уровне развития, если для сравнения и за эталон принимать системы образования стран Западной Европы и США. Использование ИКТ еще не включено в процесс преподавания основных дисциплин ОУ ПТО, включая предметы по профессиональной подготовке. Несмотря на то, что практически все ремесленные училища имеют компьютерные классы, подключенные к Интернету, такая дисциплина как «Информационные и коммуникационные технологии» не входит в учебные планы. В большинстве профессионально-технических и ремесленных училищ учебные классы для общеобразовательных дисциплин и дисциплин по специальности не оснащены компьютерами.

К 2010 г. Министерством образования было оснащено компьютерами последнего поколения почти 10 % учреждений ПТО. Однако основная часть училищ обеспечивает себя компьютерной техникой за счет использования средств международных проектов, грантов, спонсорских вложений, а так же из собственных внебюджетных средств. Исходя из имеющихся данных, можно сказать, что каждый ученик ПТО имеет доступ к компьютеру раз в неделю на время не более 20 минут. Все учреждения ПТО подключены к Интернету, используя в основном широкополосные соединения (более 256 Кбит/с). Каждое второе образовательное учреждение имеет свой веб-сайт.

В Молдове открылась современная лаборатория по подготовке специалистов в области информационных технологий. Лаборатория разместилась в индустриально-педагогическом колледже г. Кагул. Лаборатория создана при финансовой поддержке Австрии, посредством Австрийского агентства по развитию в рамках проекта «Повышение качества профессионально-технического образования в области информационных технологий и коммуникаций. В лаборатории установлено современное оборудование, которое позволит ученикам с легкостью изучить на практике пройденные материалы. Ранее лаборатории были открыты в политехническом колледже в г.Кишиневе и профтехучилище г. Бельцах. Планировалось, что в 2015 г. около 70 учащихся последнего года обучения пройдут практику в 10 ИТ-компаниях. Стоимость лаборатории — 140 тыс. евро. Проект реализуется в Молдове с 1 декабря 2012 г. и завершается 31 мая 2015 г. Он осуществляется Образовательным центром PRO DIDACTICA и Национальной ассоциации ИТ-компаний в сотрудничестве с министерством просвещения РМ при поддержке Австрийского агентства по развитию. Общий бюджет проекта — 500 тыс. евро.

Российская Федерация

Информационные технологии проникли почти во все сферы нашей жизни. Совсем скоро объемы информации будут измеряться зеттабайтами (это 10 в 21 степени), и крайне важно будет этими объёмами информации управлять.

Основные университеты в российской Федерации, где готовят специалистов по ИКТ: МГТУ им. Н.Э. Баумана; Факультет ВМК МГУ им. Ломоносова**;** МФТИ**;** МИФИ**;** МЭСИ; Иннополис; МТУСИ. Также отметим факультет бизнес-информатики НИУ ВШЭ; МИРЭА и СПбГУ (факультет прикладной математики – процессов управления); НИУ ИТМО. Из региональных вузов эксперты выделяют Казанский (Приволжский) и Южный федеральные университеты, Новосибирский, Томский и Нижегородский государственные университеты. Во все вузы без экзаменов принимают победителей и призеров заключительного этапа Всероссийской олимпиады школьников по профильным предметам и членов Международных сборных предметных олимпиад.

Рынок труда формирует потребность в специалистах в области информационно-коммуникационных технологий (ИКТ) широкого профиля, которая в полной мере не покрывается выпускниками вузов. Существующие государственные образовательные стандарты по направлению подготовки специалистов в области ИКТ в целом соответствует потребностям подготовки специалистов данного профиля. Вместе с тем, бурное развитие информационно-коммуникационных технологий вызывает необходимость внесения изменений как в содержание ГОСов, так и в формирование структуры типовых учебных планов. В частности высокая динамика инноваций в области ИКТ обусловливает с одной стороны усиление фундаментальности подготовки специалистов, а с другой стороны развитие принципов элективности курсов обучения в соответствии с региональными потребностями и личными предпочтениями обучающихся.

Анализ зарубежных учебных планов в области ИКТ показал большую профессиональную ориентацию подготовки специалистов. В учебных планах практически нет курсов, связанных с общекультурным развитием личности, но есть курсы, ориентированные на адаптацию человека в профессиональной среде, например, курсы психологии делового общения, умения работы в профессиональном коллективе и др.

Профессиональная подготовка разбивается на три составляющие: общепрофессиональные дисциплины для всех ИКТ-специальностей; специальные дисциплины, обязательные для конкретной специальности; элективные курсы специализаций. В принципе такая же структура подготовки специалистов по ИКТ характерна и для российских ГОСов и учебных планов.

Вместе с тем, учебные программы общепрофессиональных дисциплин разных ИКТ-специальностей построены не одинаково и с разной степенью детальности, что снижает требования к их фундаментальности. Содержание специальных дисциплин в силу сложности внесения изменений в существующие стандарты не всегда соответствует сегодняшнему состоянию информационно-коммуникационных технологий. Дисциплины специализаций также мало адаптируются к изменениям на рынке труда и не предоставляют должной свободы обучающимся в построении индивидуальной траектории обучения.

Перечисленные соображения вызывают необходимость проведения серьезной работы по изменению существующих государственных образовательных стандартов, как на содержательном,

так и на организационном уровнях. В части содержательных аспектов ГОСов, прежде всего, требуется уточнение компетентностных характеристик профиля подготовки специалистов по ИКТ, которые откорректируют и содержание разделов специальных дисциплин.

С точки зрения организации построения учебных планов имело бы смысл сократить общее число дисциплин до 20-30, которые были бы нацелены на более глубокое освоение специальности. Для обеспечения большей гибкости построения учебных планов имело бы смысл сократить федеральную компоненту обучения до 40-50 %, предоставив вузам право формирования дисциплин с учетом особенностей рынка труда в конкретном регионе.

Государственные образовательные стандарты третьего поколения должны в большей части соответствовать международным стандартам в области ИКТ образования, в частности основным требованиям Computing Curricula 2005. Причем базовые модули общепрофессиональных дисциплин должны совпадать по всем направлениям и специальностям в области ИКТ.

Среди профессий, связанных с ИКТ, наиболее востребованными являются профессии, нацеленные на системный анализ предметной области, проектирование информационных систем, проектный и информационный менеджмент. Подготовка профессионалов по проектированию, внедрению и сопровождению информационных систем ведется в частности и по направлению «Прикладная информатика». В рейтинге самых престижных ИТ-специальностей можно отметить следующие:

- «Датасаентист» - и специалист по работе с большими объемами данными. Big data – популярное и перспективное направление в информатике. Data scientist – это человек, который в идеале имеет техническое образование, он может быть программистом, аналитиком, бизнес-архитектором. Также он имеет научный опыт, навыки и способности к анализу информации и выдвижению гипотез»;
- Специалист по облачным вычислениям. Облачные хранилища данных – это мощные виртуальные серверы, на которых хранятся данные пользователей. Благодаря тому, что данные сохраняются в так называемых «облаках», они не прикреплены к конкретному ПК и могут извлекаться с менее мощных, чем сервер, устройств;
- Разработчик мобильных приложений**.** Смартфон = мобильные приложения. Каждое новое приложение интереснее и сложнее предыдущего, появляются новые специализации в этой сфере. Например, программисты под определенную платформу, специалисты по графическим интерфейсам, тестировщики мобильных приложений;
- Специалист по робототехнике. Относительно новое направление в ИТ, но сейчас оно стремительно набирает обороты. Сфера очень сложная, здесь и электроника, и механика, и информатика;
- Специалист по информационной безопасности. Очень широкая сфера со множеством ответвлений. Здесь и разработка антивирусов, и защита систем электронных платежей –все, что поможет информации быть под защитой;
- Комплексная автоматизация бизнес-процессов. Автоматизация нужна, чтобы быстрее решать различные бизнес-задачи. С помощью ИТ-решений можно ускорить практически любые бизнес-процессы: от привлечения новых клиентов до расчета зарплаты. Но все

процессы в бизнесе связаны между собой, поэтому комплексная автоматизация эффективнее и проще.

Также отметим междисциплинарные направления, например биоинформатику.

Подготовку специалистов в области информационных систем представляется целесообразным усилить обучением студентов в части:

- широты подготовки специалистов в области знания предметных областей (экономика, менеджмент, юриспруденция и др.);
- способности работы специалистов на различных стадиях жизненного цикла создания и эксплуатации информационной системы;
- способности работы специалистов, как в организациях, разрабатывающих информационные технологии, так и в организациях, внедряющих и эксплуатирующих ИКТ.

Большое значение в подготовке специалистов по ИКТ специальностям должны сыграть современные инновационные технологии, прежде всего, на базе средств e-Learning, которые призваны повысить адаптивность учебных программ к современным требованиям экономического развития.

Профессиональная переподготовка и повышение квалификации специалистов в области ИКТ осуществляются в рамках государственного заказа, государственного плана, а также в рамках отраслевой системы высшего и среднего профессионального образования. Распоряжением Правительства Российской Федерации от 6 марта 2015 г. № 370-р Россвязи утверждён госзаказ на 2015 год в объёме средств, предусмотренных в федеральном бюджете, — 53,3 тыс. руб. на повышение квалификации 11 гражданских служащих. План повышения квалификации государственных служащих Федерального агентства связи на 2015 год утверждён руководителем Россвязи 20 марта 2015 года. В 2015 году проведено повышение квалификации 39 федеральных государственных граждански служащих Россвязи, в том числе:

- в соответствии с Планом повышения квалификации федеральных государственных гражданских служащих Федерального агентства связи на 2015 год — 11 человек;
- за счёт средств федерального бюджета, предусмотренных Минтруду России, — 17 человек;
- за счёт средств Россвязи — 7 человек;
- за счёт средств Минобороны России — 4 человека.

Для предприятий отрасли подготовку специалистов по 16 направлениям и 3 специальностям высшего образования и по 4 специальностям среднего профессионального образования осуществляют 4 подведомственных высших учебных заведения и 9 структурных подразделений вузов связи. Контингент студентов в подведомственных учебных заведениях составляет 36150 человек, в том числе обучающихся по программам высшего образования — 27850 человек, по программам среднего профессионального образования — 8300 человек. Подготовка специалистов высшей квалификации осуществляется в аспирантуре и докторантуре вузов связи по 5 направлениям. Общая численность аспирантов и докторантов в вузах связи составляет 700 человек. В 2015 году подведомственными учебными заведениями подготовлено 8807 специалистов, в том числе 7189 человек с высшим профессиональным образованием и 1 618 человек со средним профессиональным образованием.

Из них около 80% — это специалисты в области телекоммуникационных и информационных технологий. Около 75% выпускников трудоустроено на предприятия связи и информатизации. Около 90% направлений (специальностей) подготовки в отраслевых учебных заведениях соответствуют потребностям предприятий отрасли в подготавливаемых специалистах и только 10% открыты для получения дополнительных доходов от обучения на платной основе в соответствии с потребностями региональных рынков труда в данных специалистах. Кроме подготовки специалистов отраслевые учебные заведения связи проводят повышение квалификации и профессиональную переподготовку специалистов в области ИКТ, а также в области экономики, менеджмента и управления персоналом. По заявкам предприятий отрасли учебные заведения готовы открывать новые направления повышения квалификации и переподготовки специалистов в области ИКТ. Ежегодно на базе подведомственных учебных заведений, а также в 18 учебных центрах, созданных на базе вузов с участием ведущих мировых компаний связи, проходят повышение квалификации и про- фессиональную переподготовку около 10 000 специалистов предприятий отрасли.

В 2015 году на базе СПбГУТ и Центрального музея связи имени А.С. Попова проведён конкурс профессионального мастерства среди студентов вузов Россвязи «Телесфера-2015». На первом этапе в Конкурсе приняли участие около 3000 студентов подведомственных учебных заведений. В финальной части конкурса участвовало 33 студента.

В Россвязи разработаны и направлены в Минкомсвязь России предложения по контрольным цифрам приёма (КЦП) в 2015 году для вузов Федерального агентства связи по ИТ специальностям. В вузах Россвязи разработаны меры по содействию трудоустройства выпускников 2015 года, информация о которых направлена в Минобрнауки России.

В 2015 года проведена работа с Минобрнауки России и подведомственными вузами по приёму иностранных граждан из дальнего зарубежья и стран СНГ. В Россотрудничество направлены предложения по приёму иностранных граждан, лиц без гражданства, в т. ч. соотечественни- ков, проживающих за рубежом, на обучение в вузы Россвязи в 2016 году. Продолжена работа с Минобороны России по приёму и обучению в 2015 году на военных кафедрах в СПбГУТ и СибГУТИ.

Постоянно ведётся работа по совершенствованию деятельности отделения Центра мастерства МСЭ для стран СНГ. Центр состоит из 4 узловых центров: белорусский узел (на базе Высшего колледжа связи в Минске); казахский узел, (Казахская Академия Инфокоммуникаций); российский узел (на базе МТУСИ); украинский узел (Одесская национальная академия связи им. А.С.Попова).

Большую работу по повышению квалификации и переподготовке специалистов в области информационно-коммуникационных технологий проводит Национальное агентство развития квалификаций (НАРК) Российского союза промышленников и предпринимателей (http://nark.ru/). При участии НАРК РСПП разработаны и утверждены Минтруда России уровни квалификации, которые используются при разработке профессиональных стандартов, в том числе – в области ИКТ (Приложения 1-5). При поддержке РСПП созданы виртуальная Академия современных инфокоммуникационных технологий (http://АСИКТ.РФ) и Научно-образовательный центр «Инфокоммуникации и информационные технологии» ВШБИ НИУ «Высшая школа экономики», в которых особое внимание уделяется повышению профессиональных знаний специалистов в области информационной безопасности и защиты информации. Гармонизация требований к

специалистам в области ИКТ в странах СНГ будет содействовать укреплению доверия и безопастости при использовании ИКТ.

На Расширенной коллегии Министерства связи и массовых коммуникаций Российской Федерации в 2015 году особое внимание было уделено обеспечению дальнейшей поддержки ИТ-образования. В настоящее время в России системный дефицит кадров в ИКТ-отрасли. Минобрнауки ежегодно увеличивает объем госзаказа на ИТ-специалистов. Контрольные цифры приема по ИТ-специальностям на 2016–2017 учебный год увеличились на 31% по сравнению с предыдущим учебным годом и на 70% за последние два года.

Для решения проблемы кадрового дефицита в ИТ-отрасли в 2015 году вместе с субъектами РФ Минкомсвязи России инициировало включение ИТ-специальностей в финансируемые государством региональные программы переквалификации высвобождающихся специалистов из других отраслей. Выделяются соответствующие субсидии, эта программа реализуется.

Отдельного следует отметить образовательную акцию в области ИТ «Час кода». Она проходит полномасштабно уже второй год (2014-2015гг.). В ней принимает участие около 8 млн. школьников.

В конце 2014 года Минкомсвязи России завершило основную фазу строительства технопарков. Программа реализовывалась по принципу субсидий. Выручка этих компаний составила более 50 млрд. рублей, около 900 компаний-резидентов, около 20 тысяч рабочих мест. Средний возраст сотрудников в технопарках — около 27 лет. Объем софинансирования со стороны субъектов значительно превысил объем федеральных субсидий.

В 2015 году фактически завершилось строительство целого небольшого города в области высоких технологий — города Иннополис, который Минкомсвязи России реализовало совместно с Министерством экономического развития. Основной объем финансирования пришелся на программу «Особых экономических зон». Город построен по принципу «живи-учись-работай-отдыхай», и смысл в том, что это целостная экосистема, которая позволяет развиваться инновационным компаниям принципиально нового типа. Там создано и жилье, и соответствующая

социальная инфраструктура, технопарк, и создан достаточно необычный пример университета, который целиком сфокусирован на разных сферах обучения в области ИТ. Сегодня он не является получателем какого бы то ни было базового бюджетного финансирования по линии Минобрнауки или любого другого вуза и финансируется за счет взносов тех или иных ИТ-компаний. Сегодня там обучаются уже более 200 бакалавров, 70 магистров и в 2015 году еще почти 300 новых бакалавров и магистров планируют туда поступить.

Республика Таджикистан

В настоящее время специалистов в сфере ИКТ готовят в основном два вуза страны: Технологический университет Таджикистана и Таджикский технический университет имени академика М.С. Осими.

Технологический университет Таджикистана (ТУТ) образован на базе Таджикского высшего технологического колледжа, созданного Постановлением Совета Министров Республики 20 сентября 1990 года. Для эффективного внедрения новых моделей и технологий обучения в Технологическом университете Таджикистана созданы все условия, то есть имеются: современная электронная библиотека, Центр Регистратора, Единый Тестовый Центр и другие атрибуты, обеспечивающие общую результативность и эффективность функционирования ВУЗа. ТУТ является ведущим ВУЗом Республики Таджикистан, который осуществляет подготовку высококвалифицированных специалистов в области информационно-коммуникационных технологий последние десять лет. Выпускники ИКТ-специальностей ТУТ считаются весьма востребованными на рынке информационных услуг как Республики Таджикистан, так и за ее пределами.

Подготовку специалистов в области ИКТ в университете осуществляют три факультета:

- Факультет информационных и компьютерных технологий;
- Факультет отраслевых информационных систем и технологий;
- Совместный таджикско-украинский факультет.

В целом, систему подготовки ИКТ-специалистов в Таджикистане можно охарактеризовать как неориентированную на рынок. Изменения в государственных программах подготовки ИКТ-специалистов заметно отстают от изменений на рынке труда и технического прогресса как такового. Хотя значительную роль в качестве образования играет недостаток финансирования, основной причиной проблем для развития является почти полное отсутствие частных ВУЗов, которые бы готовили ИКТ-специалистов и очень слабая конкуренция даже между существующими государственными ВУЗами.

Общественная организация «Центр Информационно-Коммуникационных Технологий» (Центр ИКТ) г.Душанбе ведет свою деятельность в области развития человеческих ресурсов в сфере Информационных Технологий (ИТ), которая готовит будущих ИТ-специалистов по новейшим программам обучения. В рамках своих программ Центр ИКТ занимается информационно-образовательной деятельностью и работает с ВУЗами, некоммерческими, коммерческими и государственными организациями. Основные обучающие курсы проводятся на основе лицензии Министерства образования и науки Республики Таджикистан.

10 октября 2015 года Центр ИКТ объявил о начале нового образовательного проекта «Продвижение и развитие открытых образовательных ресурсов (ООР) с использованием современных технологий, методики и системы дистанционного обучения», который реализуется при финансовой поддержке Отделения Международной Организации Института «Открытое Общество» — Фонд Содействия в Таджикистане. Партнерами проекта являются Министерство образования и науки Республики Таджикистан и компания Tcell. Планируется, что в рамках проекта Центр ИКТ проведет ряд мероприятий для вузов с целью увеличения учебных и научных материалов в открытом доступе в сети Интернет и их последующей интеграции в систему дистанционного образования. Основными участниками данного проекта являются преподаватели и специалисты учебных заведений, которые примут участие на презентациях, мастер-классах, конкурсах и тренингах по созданию и развитию открытых образовательных ресурсов.

Конкурс «Интернет для открытых образовательных ресурсов» проводится для достижения высокого уровня качества учебных ресурсов в сети и повышения заинтересованности преподавателей. По завершении конкурса Центр ИКТ продолжит совместную работу с целевыми вузами проекта, которым будет оказана техническая помощь в создании сайтов с учебными ресурсами. Также будет создан единый образовательный портал для быстрого доступа к внутренним и внешним научно-образовательным материалам.

Республика Узбекистан

Информационные технологии составляют основу любой развитой экономики. Знания ИТ-специалистов, их работа в цифровом пространстве очень важны для интеллектуального потенциала общества. Специалисты, имеющие отношение к ИТ, способны оказывать серьезное влияние на экономику и соответственно потребность к сотрудникам в области ИТ неуклонно возрастает.

Университет Инха в г.Ташкенте(IUT) был создан в соответствии с Постановлением Президента Республики Узбекистан от 24 марта 2014 г. и начал свою деятельность со 2 октября 2014 г. по двум направлениям образования: «Компьютерный инжиниринг» (ICE) и «Программный инжиниринг» (CSE). На сегодняшний день для работы в университете привлечены 11 высококвалифицированных зарубежных специалистов. В будущем планируется открытие новых востребованных направлений обучения, таких как логистика, менеджмент в сфере ИКТ и электронная коммерция, а также открытие магистратуры.

В начале 2015 года в Университете Инха в г.Ташкенте обучалось 115 студентов, из них половина из регионов республики. 10 лучших студентов по итогам вступительных экзаменов обучаются на грантовой основе с обязательством отработать не менее 5 лет после завершения учебы в одной из организаций-учредителей. Также для дополнительного стимулирования и поощрения 10 студентов, получивших наивысшие оценки по окончании семестра, освобождаются от полной либо частичной оплаты за обучение на следующий семестр. В 2015-2016 учебном году Университет принял 250 студентов, из них 120 по направлению компьютерный инжиниринг и 130 по направлению программный инжиниринг.

Эффективность развития информационно-коммуникационной системы необходимо дополнять повышением уровня знаний по ИКТ специалистов различных сфер деятельности. В этих целях при Ташкентском университете информационных технологий (ТУИТ) был учрежден

учебный центр электронного правительства, где налажено обучение руководителей и сотрудников государственных и хозяйствующих органов и местных органов управления. На сегодняшний день обучение прошли более 16 тыс. сотрудников 63 учреждений.

Ташкентский университет информационных технологий имеет 5 филиалов в городах Карши, Нукус, Самарканд, Ургенч и Фергана. В составе университета и его региональных филиалов действуют 13 факультетов, 57 кафедр и ведется подготовка кадров по 25 направлениям образования. В университете и его региональных филиалах обучаются 10 508 студентов.

Также были организованы 12 учебных центров на базе высших учебных заведений при Комплексах Кабинета Министров Республики Узбекистан. На специализированных курсах этих центров были обучены 844 сотрудника различных ведомств. На данный момент ведется обучение еще более 8 200 сотрудников.

В соответствии с Постановлением Президента Республики Узбекистан от 26 марта 2013 года №ПП-1942 года «О мерах по дальнейшему совершенствованию системы подготовки кадров в области информационно-коммуникационных технологий» в течение 2014 года более 60 молодых и перспективных преподавателей ТУИТ и его филиалов прошли обучение на курсах в Южной Корее и Германии. Это будет способствовать обеспечению качественной, на уровне международных стандартов, подготовки и повышения квалификации высококвалифицированных специалистов в сфере информационно-коммуникационных технологий.

Украина

На Украине создана законодательная база подготовки специалистов в области телекоммуникаций/ИКТ:

Закон Украины № 537-V от 9 января 2007 г. «Об Основных принципах развития информационного общества в Украине и на 2007-2015 годы» определяет основные стратегические цели и направления развития информационного общества на Украине. Закон предусматривает следующие основные приоритеты:

- развитие национального научно-образовательного пространства на базе информационно-коммуникационных систем;
- разработку методологического обеспечения использования компьютерных мультимедийных технологий во время преподавания школьных предметов, обучения студентов;
- обеспечение приоритетности подготовки специалистов по ИКТ;
- усовершенствование учебных планов, открытие новых специальностей по новейшим ИКТ;
- создание системы дистанционного обучения на основе ИКТ;
- обеспечение учебных заведений и научных учреждений современными средствами ИКТ и необходимыми информационными ресурсами;
- обеспечение свободного доступа к средствам ИКТ и информационным ресурсам, особенно в сельской местности и труднодоступных населенных пунктах;

- повышение компьютерной грамотности населения;

Постановление Кабинета министров Украины «О Государственной национальной программе «Образование» (Украина XXI столетие)» от 01.11.1993 г.;

Указ Президента Украины «Об основных направлениях реформирования высшего образования Украины» от 12.09.1995 г.;

Указ Президента Украины «Об основных направлениях реформирования высшего образования Украины» от 09.10.2001 г. № 941/2001;

Приказ Министерства образования Украины от 02.06.1993 г. об утверждении «Положения об организации учебного процесса в высших учебных заведениях Украины»;

Постановления Кабинета Министров Украины от 15 сентября 1999 г. № 1697 «Национальная программа патриотичного воспитания населения, формирование здорового образа жизни, развития духовности и укрепления моральных основ общества»;

Приказ Министерства образования и науки Украины от 08.12.95 № 340 «Об утверждении Положения об организации экстерната в вузах Украины»;

Концепция национального воспитания, одобренная Всеукраинским педагогическим советом работников образования Украины 30 июня 1994 г.;

Приказ Министерства связи Украины от 22.05.1995 г. о создании Ведомственного наставительно-научно-производственного комплекса «Связь» на базе Украинской государственной академии связи;

Указ президента «О дополнительных мерах относительно усиления борьбы с коррупцией, другими противоправными действиями в социально-экономической сфере и обеспечения экономного расходования государственного средства» от 16.11.2000 г. за № 1241/2000;

«Концепция подготовки, переподготовки и повышения квалификации специалистов для области связи и сферы информатизации до 2007 года» № 19 от 03.02.2003 г.

Количество ВУЗов Украины, готовящих специалистов по ИКТ-специальностям

Специальность	**Количествово вузов**
Информационные системы и технологии	25
Программное обеспечение информационных систем	23
Прикладная математика	22
Электронные системы	11
Информационные технологии проектирования	9
Производство электронных средств	9
Компьютерно-интегрированные технологические процессы и производства	8
Микроэлектроника и полупроводниковые устройства	8
Телекоммуникационные системы и сети	7
Системное программирование	6

Технологии и средства телекоммуникаций	6
Электронные приборы и устройства	6
Робототехнические системы и комплексы	4
Информационная безопасность	3
Проектный менеджмент	3

Проведённые украинскими специалистами исследования показывают следующий рейтинг университетов на Украине в области ИКТ.

Рейтинг	**Вуз**	**Город**
1	ГУТ	Киев
2	СумГУ	Сумы
3	ХНУ им. Каразина	Харьков
4	ХНУРЭ	Харьков
5	КНУ им. Шевченко	Киев
6	ХАИ им. Жуковского	Харьков

Проведённые опросы показывают, что к слабым сторонам ВУЗов Украины, в которых изучаются ИКТ, относятся: слабый студентческий состав; устаревшие программы обучения; Вуз не мотивирует учиться; отсутствие современного учебного оборудования; отсутствие сотрудничества с работодателями. В тоже время, «сильные» ВУЗы характеризуются такими показателями как: наличие опытеных преподавателей, владеющих пониманием основных тенденций развития ИКТ; престижность и котируемость диплома; изучаемые предметы и программы обучения соответствуют современному уровню развития ИКТ; в ВУЗе хорошо налажена культурная жизнь; ВУЗ имеет прочные постоянные связи с работодателями.

Можно сделать вывод, что к настоящему времени в ВУЗах Украины ещё сохранился достаточно сильный профессорско-преподавательский состав, но преподаваемые ими учебные программы начинают всё больше и больше устаревать. Только 20% выпускников и студентов ВУЗов Украины считают, что им читали актуальные предметы и давали знания в достаточном объеме. Ни один из передовых украинских технических вузов не может похвастаться современным техническим оборудованием. При этом 60% студентов сталкивались с коррупцией.

Подготовка специалистов с высшим образованием в области информационной безопасности (ИБ) начата на Украине в 1997 году, является самой новой и самой динамичной.

Проведение сравнительного анализа систем подготовки специалистов ИБ не может быть полным без учета, кроме подготовки сугубо гражданских специалистов, несколько специфических систем подготовки специалистов ИБ для силовых министерств и ведомств, которые были созданы первыми и сохраняют координирующую роль в общей системе. Опыт показывает, что обе категории специалистов должны иметь преимущественно родственную по содержанию подготовку и реализуют себя на родственных объектах деятельности.

Для сравнительного анализа определим несколько составляющих возможной структуры системы подготовки специалистов ИБ:

- подготовка специалистов в области информационной безопасности (как для выявления и нейтрализации информационно-технических угроз инфо-сферы машинно-технических систем, другим объектам информационной инфраструктуры страны, так и угроз в гуманитарной сфере);
- подготовка специалистов для структур информационной безопасности и информационной борьбы вооруженных сил и некоторых других министерств и ведомств;
- специальная подготовка (переподготовка, повышение квалификации) по вопросам информационной безопасности органов государственного (военного, корпоративного) управления определенных стран;
- общая подготовка населения страны (адаптация к условиям жизни в информационном обществе).

Подготовка специалистов по ИБ была начата с совместного приказа Государственной службы Украины по вопросам технической защиты информации и Министерства образования Украины от 28 декабря 1995 г. № 66/358 «О сотрудничестве между Министерством образования Украины и Государственной службой Украины по вопросам технической защиты информации».

Также был подготовлен «Перечень направлений и специальностей, по которым осуществляется подготовка специалистов в высших учебных заведениях за соответствующими образовательно-квалификационными уровнями», который был утвержден Постановлением Кабинета Министров Украины от 24 мая 1997 г. № 507, и в который было внесено направление 1701 «Информационная безопасность» в составе пяти специальностей.

С 2007 года согласно постановлению Кабинета Министров Украины от 13 декабря 2006 г. № 1719 «О перечне направлений, по которым осуществляется подготовка специалистов в высших учебных заведениях по образовательно-квалификационному уровню бакалавра» система подготовки специалистов по информационной безопасности на Украине включает несколько групп стандартов системы высшего образования отрасли знаний такие как: 1701 «Информационная безопасность» (направления: безопасность информационных и коммуникационных систем; системы технической защиты информации; управление информационной безопасностью); 0501 «Информатика и вычислительная техника (компьютерные науки, компьютерная инженерия, программная инженерия)»; 0502 «Автоматика и управление (системная инженерия)»; 0509 «Радиотехника, радиоэлектронные аппараты и связь (радиотехника, телекоммуникации)»; 0403 «Системные науки и кибернетика (прикладная математика, информатика)»; 1601 «Военные науки, национальная безопасность» и некоторые другие.

В стране действует система соответствующих государственных и коммерческих курсов повышения квалификации.

Ведущие вузы Украины по подготовке специалистов направления 1701 «Информационная безопасность»

№пп	Наименование вуза
1	Национальный авиационный университет
2	Национальный технический университет Украины (НТУУ «КРУГОВ»)
3	Национальная академия Службы безопасности Украины

4	Киевский национальный университет имени Т. Г. Шевченко
5	Государственный университет информационно-коммуникационных технологий (г.Киев)
6	Харьковский национальный университет радиоэлектроники
7	Национальный горный университет (г.Днепропетровск)
8	Запорожский национальный технический университет
9	Национальный университет внутренних дел (г.Харьков)

Специалисты отмечают, что объемы подготовки специалистов по ИБ на Украине, по сравнению с общими объемами подготовки специалистов, в настоящее время недостаточны. Особенностью подготовки специалистов ИБ является динамичное развитие объекта деятельности, а следовательно, и содержания обучения. Эта проблема должна решаться своевременным обновлением содержания и интеграцией базового и вариативного курсов подготовки. Учитывая это, негативными факторами являются:

- недостаточные объемы переподготовки и своевременного повышения квалификации научно-педагогических работников, обеспечивающих учебный процесс;
- недостаточный уровень модернизации учебно-лабораторной базы университетов по соответствующим направлениям и специальностям;
- недостаточные объемы привлечения к переподготовке и повышению квалификации по вопросам ИБ государственных служащих и специалистов органов государственного (корпоративного) управления, особенно среднего и старшего возраста;
- недостаточный уровень взаимодействия между министерствами и ведомствами по вопросам подготовки специалистов ИБ, обмена программами подготовки;
- чрезмерная коммерциализация курсов по ИБ. Значительная часть коммерческого сегмента курсов является фактически представительствами иностранных компаний-производителей программного продукта, что не уменьшает информационную зависимость Украины и не способствует повышению степени контролируемости заимствованных информационных технологий, внедренных в различные сферы государственного и корпоративного управления, обеспечения жизнедеятельности страны.

В целом можно сказать, что на Украине завершен первый этап - создание системы подготовки специалистов по ИБ. Но в контексте мирового опыта, современных и перспективных угроз в информационной сфере эта система требует дальнейшего существенного развития в структурном и содержательном плане, а также улучшение кадрового и материально-технического обеспечения.

8. Рекомендации в части реализации Региональной инициативы

1. Поддержать курс на усиление роли мирового сообщества, в лице Международного союза элетросвязи. в управлении интернетом и разработку глобальной политики в этой области, основывающейся на принципах неприменения силы, уважения государственного суверинитета, невмешательства в дела других государств и соблюдения основных прав и свобод человека.
2. Поддерживать процесс гармонизации законодательства и нормативно-технической базы в области ИКТ государств - участников СНГ.
3. Поощрять активное участие всех заинтересованных сторон и, при необходимости, принимать соответствующие меры по поддержке проводимой Международным союзом электросвязи деятельности по укреплению доверия и безопасности при использовании ИКТ.
4. В рамках компетенций продолжить работы по совершенствованию механизмов взаимодействия государств - участников СНГ по развитию рынка в сфере ИКТ.
5. Принимать необходимые меры и соответствующие действия, на национальном и международном уровнях по защите детей в информационном пространстве.
6. Подготовить рекомендации Администрациям связи государств - участников СНГ и Грузии по возможности ратификации Конвенции ООН о правах инвалидов. Провести сравнительно-правовой анализ на соответствие действующего законодательства в области использования ИКТ требованиям Конвенции ООН о правах инвалидов, внести соответствующие изменения и дополнения в нормативно-правовые акты.
7. Поддержать и активно содействовать реализации предложений РСС от 2014 года по выработке взаимоприемлемых подходов для построения трансграничного пространства доверия на основе сети Интернет государств - участников СНГ.
8. Поощрять проведение на национальном уровне оценки внутреннего законодательства с целью ликвидации препятствий для эффективного использования документов и осуществления сделок в электронной форме, в том числе использования электронных методов аутентификации.
9. Рассмотреть возможность разработки и утверждения в рамках СНГ (в том числе в рамках модельного закона, предложенного РСС) унифицированный механизм электронной цифровой подписи с целью легитимизации всех видов электронной коммерции, как в случае операций внутри страны, так и в ситуации, когда покупатель и продавец – граждане различных стран, в том числе для сделок, предусматривающих переуступку прав требования.
10. Поддержать и активно способствовать реализации предложений, выдвинутых в рамках реализации региональной инициативы стран СНГ «Разработка рекомендаций и создание пилотного фрагмента системы электросвязи / ИКТ для поддержки защищенных удаленных розничных платежей и управления банковскими счетами на основе беспроводных сетей связи», принятой на Всемирной конференции по развитию электросвязи 2010 года (Хайдарабад, Индия) при поддержке ЗАО «Интервэйл» (Российская Федерация) и Одесской национальной академии связи им. А.С. Попова

(Украина), в части формирования правовой основы и координации усилий по борьбе с преступлениями в области электронной коммерции. Рассмотреть возможность создания в рамках СНГ механизма обмена информацией по вопросам обеспечения безопасности и тихнологиям совершаемых преступных действияй в области электронной коммерции в виде постоянно действующего органа и специализированного форума для взаимодействия участников рынка различных стран.

11. Продолжить совместные усилия по развитию человеческого капитала в области ИКТ государств - участников СНГ.
12. Представляется целесообразным и актуальным организовать в рамках СНГ выработку единых принципов оценки профессиональной подготовки специалистов в области ИКТ и предусмотреть формирование гармонизированных в рамках СНГ национальных систем профессиональных квалификаций, включая механизм независимой оценки профессионального уровня квалификации работников.
13. Предусмотреть, с участием объединений работодателей и профессиональных сообществ, подготовку предложений по формированию сети независимых центров сертификации квалификации, в том числе по определению механизмов аккредитации таких центров и установлению процедуры подтверждения квалификации.
14. Предпринимать меры по адаптации системы профессиональных стандартов для специалистов в области ИКТ в государствах - участниках СНГ в систему существующих требований к их уровню квалификации.
15. Рассмотреть возможность и подготовить предложения по международной аккредитации, в рамках СНГ, национальных центров сертификации квалификации специалистов в области ИКТ.
16. В рамках компетенций продолжить проводимую в государствах-участниках СНГ работу по обучению пользователей и повышению их осведомленности относительно неукоснительного соблюдения законодательства в области ИКТ и борьбы с преступлениями в сфере компьютерных преступлений, неприкосновенности частной жизни при работе в онлайновом режиме и способов их защиты.
17. Продолжить и поощрять ведущиеся в государствах - участниках СНГ работы по предупреждению и обнаружению проявлений ненадлежащего использования ИКТ и нарушений информационной безопасности. При необходимости разработать соответствующие руководящие документы и рекомендации, согласованные в рамках СНГ.
18. Принимать необходимые меры по расширению возможности доступа к «открытым данным» государственных министерств и ведомств, а также коммерческих организаций с целью укрепления доверия со стороны граждан при использовании государственных услуг в электронном виде и другом использовании ИКТ.
19. При необходимости подготовить предложения о взаимодействии систем мониторинга ресурсов национальных сегментов Интернета государств - участников СНГ в целях своевременного выявления проблем и угроз, а также поиска оптимальных средств их решения и нейтрализации

20. Наладить постоянный обмен опытом в области обеспечения информационной безопасности и защиты информации и поощрять его использование всеми заинтересованными сторонами.
21. Продолжать положительную практику государств-участников СНГ по укреплению доверия и безопасности с помощью взаимодополняющих и взаимоусиливающих инициатив в сфере безопасности при использовании ИКТ и инициатив или руководящих принципов в отношении прав на неприкосновенность частной жизни, защиту персональных данных и прав граждан.

Основные термины и сокращения

ИКТ - информационно-коммуникационные технологии.

МСЭ - Международный Союз Электросвязи при ООН.

Информация - сведения о фактах, событиях, явлениях, процессах независимо от физической формы их представления, используемые в целях сохранения и получения знаний, принятия решений, обеспечения функционирования общества на основе их естественной и (или) машинной обработки. Совокупность знаний о фактических данных и зависимостях между ними. Является объектом собственности и одним из видов ресурсов, используемых человеком в трудовой деятельности и в быту с целью самосовершенствования, саморазвития.

Информатизация - формирование и использование информационных систем, основанных преимущественно на новых информационных технологиях, средствах вычислительной техники и связи, применение их для обеспечения всех структур общества и граждан информацией.

Ресурсы информатизации - технологии, программные и информационные продукции, техника, инфраструктура (информационные системы, комплексы информационных систем и передачи информации).

Информационные системы - системы, выполняющие, в основном, автоматизированную обработку массивов официальной документированной информации, формируемых по организационно-структурному, тематическому, технологическому и другим признакам в целях удовлетворения потребностей граждан, организаций.

Защита информации - предотвращение или существенное затруднение нанесения ущерба интересам собственников информации (данных) и информационных систем, а также другим заинтересованным лицам, осуществляемые с помощью совокупности организационных мер, программно-технических средств и правовых норм, а также система ответственности виновных в нарушении установленных правил защиты информации.

Обработка информации (данных) - вся совокупность операций (сбор, накопление, ввод, вывод, передача, прием, запись, воспроизведение, преобразование, чтение, хранение, уничтожение, регистрация), осуществляемых с использованием естественных, технических и программных средств.

Индекс развития электронного правительства (The UN Global E-Government Development Index) Организации Объединённых Наций (ООН) — это комплексный показатель, который

оценивает готовность и возможности национальных государственных структур в использовании информационно-коммуникационных технологий (ИКТ) для предоставления гражданам государственных услуг. Выпускается раз в два года.

Исследование содержит данные об уровне развития электронного правительства в различных странах, а также системную оценку тенденций в использовании ИКТ государственными структурами. Все страны, охваченные данным исследованием, ранжируются в рейтинге на основе взвешенного индекса оценок по трем основным составляющим:

- Степень охвата и качество интернет-услуг.

- Уровень развития ИКТ-инфраструктуры.

- Человеческий капитал.

Индекс развития информационно-коммуникационных технологий (ICT Development Index) — это комбинированный показатель, характеризующий достижения стран мира с точки зрения развития информационно-коммуникационных технологий (ИКТ).

Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года (далее – Стратегия) представляет собой совокупность согласованных взглядов государств – участников Содружества Независимых Государств (далее – СНГ, Содружество), отражающих их общее видение путей формирования информационного общества.

ПТО - профессионально-техническое образование.

РСС - Региональное содружество в области связи.

ИСО - Международная организация по стандартизации.

ЦИКТСО - Центр информационных и коммуникационных технологий в системе образования.

ИМЦ - информационно-маркетинговых центров.

КСИРСС - Координационного совета государств-участников СНГ по информатизации при РСС.

ВВУИО - Встреча на высшем уровне по вопросам информационного общества.

ООН - Организация Объединенных Наций

СНГ - Содружество Независимых Государств

ШПД (ШД) - Широкополосный или высокоскоростной доступ в Интернет

CDMA - Code Division Multiple Access

GSM - Global System for Mobile Communications

UMTS - Universal Mobile Telecommunications System

Список источников

Печатные источники

1. Жаманкарин, М. М. Развитие информационно-коммуникационных технологий в Казахстане [Текст] / М. М. Жаманкарин, М. Х. Макенова // Молодой ученый. — 2015. — №4. — С. 175-176.
2. Саморукова, И. Доверие и безопасность – основные тенденции в развитии сотрудничества в РСС [Текст]/ И. Саморукова, Н. Мухитдинов// Information Security/ Информационная безопасность - 2010 – №2. – С. 8 – 10.
3. Продвижение использования информационных и коммуникационных технологий в техническом и профессиональном образовании и обучении в странах СНГ [Текст]: аналитический отчет / ООН по вопросам образования, науки и культуры, Ин-т ЮНЕСКО по информ. технологиям в образовании, Междунар. фонд гуманитарного сотрудничества государств - участников СНГ. - Москва : Ин-т ЮНЕСКО по информационным технологиям в образовании, 2012. - 127 с.
4. Дзюба, Н. И. Дети и Интернет: украинский подход к безопасному киберпространству [Текст]/ Н. И. Дзюба, В. М. Красножон // Школьная библиотека. - 2012. - № 6/7. - С. 101-103.
5. Асланов Рамиль Махир оглы Правовая база создания информационного общества в Азербайджанской Республике [Текст]/ Асланов Рамиль Махир оглы// Правовая информатика. – 2012. - № 1. – С. 22-25.
6. Агаев, Т.А. Подготовка в Азербайджане специалистов в области информационных технологий [Текст] / Т. А. Агаев, З. Г. Джабраилова, М. Г. Мамедова // Открытое образование. - 2010. - N 1. - С. 85-96.
7. Петрова, О.М. Информационное законодательство в республике Молдова [Текст]/ О,М. Петрова// Информационное право. -2010. - №2. – С. 26-29.

Электронные источники

8. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Азербайджанской Республики от 03 апреля 1998 г. №460- IQ. – Режим доступа: http://www.eos.ru/pk6/documents/detail.php?ID=9536&SECTION_ID=680. – (Дата обращения: 25.12.2015).
9. Министерство связи и высоких технологий Азербайджанской республики [Электронный ресурс]: – Режим доступа: http://www.mincom.gov.az. – Заглавие с экрана. – (Дата обращения: 25.12.2015).
10. Научная электронная библиотека «Киберлиника» [Электронный ресурс]: – Режим доступа: http://www. cyberleninka.ru . – Заглавие с экрана. – (Дата обращения: 25.12.2015).
11. О государственной и служебной тайне [Электронный ресурс]: Закон Республики Армения от 03 декабря 1996 г. (с изменениями и дополнениями на 18.04.2002г.) – Режим доступа: http://online.zakon.kz/Document/?doc_id=31419010. – (Дата обращения: 25.12.2015).
12. О свободе информации [Электронный ресурс]: Закон Республики Армения от 11 октября 2003 г. № ЗР-11 – Режим доступа: http://online.zakon.kz/Document/?doc_id=31423967. - (Дата обращения: 25.12.2015).

13. Об электронном документе и электронной цифровой подписи [Электронный ресурс]: Закон Республики Армения от 15 января 2005 г. № НО-40 – Режим доступа: http://online.zakon.kz/Document/?doc_id=31423952. - (Дата обращения: 25.12.2015).
14. Об электронной связи [Электронный ресурс]: Закон Республики Армения от 13 августа 2005 г. № ЗР-176 – Режим доступа: http://online.zakon.kz/Document/?doc_id=31422228. - (Дата обращения: 25.12.2015).
15. Об архивном деле [Электронный ресурс]: Закон Республики Армения от 01 июля 2004 г. № ЗР-88 – Режим доступа: http://base.spinform.ru/show_doc.fwx?rgn=26064. - (Дата обращения: 25.12.2015).
16. Уголовный кодекс Республики Армения [Электронный ресурс]: Текст кодекса приводится по состоянию на 18.04.2003 г. – Режим доступа: http://www.crime.vl.ru/index.php?c=1&more=1&p=1319&pb=1&tb=1. - (Дата обращения: 25.12.2015).
17. Гражданский кодекс Республики Армения [Электронный ресурс] – Режим доступа: http://www.competition.am/uploads/resources/qorensgirkRUS.pdf. - (Дата обращения: 25.12.2015).
18. Информационная безопасность в Армении vs хакеры: угрозы и вызовы в преддверии 24 апреля [Электронный ресурс]: Данные компаний АрменТел и Viva Cell . – Режим доступа: http://telecom.arka.am/ru/news/internet/informatsionnaya_bezopasnost_v_armenii_vs_khakery_ugrozy_i_vyzovy_v_preddverii_24_aprelya/. – Заглавие с экрана. – (Дата обращения: 25.12.2015).
19. Мартиросян, С. Цензура в интернете: Запад не отстает от Востока [Электронный ресурс] / С. Мартиросян// CNews.Ru. -2006. - Режим доступа: http://www.cnews.ru/reviews/index.shtml?2006/02/16/196225_1
20. Очередная встреча лидеров IT посвящена проблемам электронной торговли [Электронный ресурс] – Режим доступа: http://www.panorama.am/ru/news/2010/12/15/it/1014916. - Заглавие с экрана. - (Дата обращения: 25.12.2015).
21. Руководящие указания для директивных органов по защите ребёнка в онлайновой среде [Электронный ресурс] – Режим доступа: http://www.un.org/ru/ecosoc/itu/guidelines_for_policymakers.pdf - (Дата обращения: 25.12.2015).
22. Касперский получил премию президента Армении Global IT Award из рук главы государства [Электронный ресурс] // HayastanNews.com/. -2015. - Режим доступа: http://hayastannews.com/news/104089.html.
23. Национальная программа ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы [Электронный ресурс]: Постановление Совета Министров Республики Беларусь от 28.03.2011 № 384 – Режим доступа: http://e-gov.by/programma-elektronnaya-belarus/nacionalnaya-programma-uskorennogo-razvitiya-uslug-v-sfere-informacionno-kommunikacionnyx-texnologij-na-20112015-gody. - (Дата обращения: 25.12.2015).
24. В Белоруси появится возрастная маркировка информационной продукции [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь pravo.by/. -2015. - Режим доступа: http://www.pravo.by/main.aspx?guid=192353.
25. Национальный ИКТ-профайл Грузии [Электронный ресурс] // Режим доступа: http://digital.report/gruziya-natsionalnyiy-ikt-profayl/

26. Часть 3: Фиксированная, мобильная и международная связь. Национальный ИКТ-профайл Грузии [Электронный ресурс]// Режим доступа: http://digital.report/gruziya-svyaz. - Заглавие с экрана.
27. Часть 4: Доступ в интренет и интернет-услуги. Национальный ИКТ-профайл Грузии [Электронный ресурс]// Режим доступа: http://digital.report/gruziya-dostup-v-internet/ - Заглавие с экрана.
28. Реализация региональных инициатив СНГ Дубайский план действий (ВКРЭ-14) и региональные инициативы (2015-2018 гг.) // Режим доступа: http://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/Regional%20Initiatives/RI5%20confidence%20in%20ICT/%D0%A0%D0%B5%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F%20%D0%A0%D0%98%20CIS5.pdf
29. Электронное правительство в странах бывшего Советского Союза [Электронный ресурс]// e-event.kz /. -2014. - Режим доступа: http://www.e-event.kz/elektronnoe-pravitelstvo-v-stranax-byvshego-sovetskogo-soyuza/.
30. Опыт Грузии во внедрении электронного правительства [Электронный ресурс]. - Режим доступа: http://infocom.uz/2015/07/08/opyt-gruzii-vo-vnedrenii-elektronnogo-pravitelstva/.
31. Официальный сайт МСЭ в регионе СНГ [Электронный ресурс]. - Режим доступа: http://www.itu.int/ru/ITU-D/Regional-presence/CIS/Pages/default.aspx - Заглавие с экрана.
32. Орозобек Кайыков: Руководитель Зонального отделения МСЭ для стран СНГ. Реализация Хайдарабадского плана действий (HAP) 2011-2014 годы [Электронный ресурс]. - Режим доступа: http://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2015/02_Moscow/Session_1_Kaiykov.pdf
33. Сайт регионального содружества в области связи [Электронный ресурс]. - Режим доступа: http://www.rcc.org.ru/ - Заглавие с экрана.
34. Региональный форум по вопросам развития для стран СНГ/РСС “Широкополосная связь в интересах устойчивого развития” Кишинев, Республика Молдова, 31 марта−1 апреля 2015 года. Заключительный отчет Электронный ресурс]. - Режим доступа: http://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2015/03_Chisinau/%D0%9E%D1%82%D1%87%D0%B5%D1%82.pdf.
35. Справка о ходе выполнения Стратегии сотрудничества государств - участников СНГ в построении и развитии информационного общества и Плана действий по ее реализации на период до 2015 года связи [Электронный ресурс]. - Режим доступа: www.minsvyaz.ru/uploaded/files/17s50217strategiya.doc
36. О проекте Стратегии сотрудничества государств - участников СНГ в построении и развитии информационного общества и Плана действий по ее реализации на период до 2025 года [Электронный ресурс]. - Режим доступа: www.minsvyaz.ru/uploaded/files/20p502172proekt-strategii-do-2025-g-70415.doc
37. Костров, Д. Киберзащита конЦЕНТРируется [Электронный ресурс] / Дмитрий Костров// ИКС-Медиа: журн. – 2013.-№3.- Режим доступа: http://www.iksmedia.ru/articles/4808665-Kiberzashhita-konCENTRiruetsya.html
38. Электронное правительство Республики Казахстан [Электронный ресурс]. -Режим доступа: http://egov.kz/wps/portal/Content?contentPath=/egovcontent/basic&lang=ru.

39. Государственная программа «Информационный Казахстан – 2020 [Электронный ресурс]// Электронное правительство Республики Казахстан. - Режим доступа: http://egov.kz/wps/portal/Content?contentPath=/egovcontent/transports/communications/article/gp_inf_kaz_2020&lang=ru#6.
40. Об утверждении Правил присоединения и взаимодействия сетей телекоммуникаций, включая пропуск трафика и порядок взаиморасчетов [Электронный ресурс]: Утверждено правительством Республики Казахстан от 30 декабря 2011 г. № 1694с. - Режим доступа: www.tengrinews.kz/zakon/pravitelstvo_respubliki_kazahstan_premer_ministr_rk/svyaz/id-P1100001694/. - (Дата обращения 09.11.2015).
41. Ускенбаева, Р. К. Перспективы развития ИКТ-образования в Казахстане [Электронный ресурс]/ Р.К. Ускенбаева // Вестник промышленности, бизнеса и финансов 365-tv.ru, журн.-2010.-Режим доступа: http://365-tv.ru/index.php/analitika/kazakhstan/278-perspektivy-razvitiya-ikt-obrazovaniya-v-kazakhstane. - (Дата обращения 27.10.15).
42. Оспанов, С. Электронная коммерция в Казахстане готовится к большому скачку [Элеткронный ресурс]/ С. Оспанов// Информационное агентство zakon.kz. –Режим доступа: http://www.zakon.kz/4449726-jelektronnaja-kommercija-v-kazakhstane.html. - (Дата обращения 27.10.15).
43. Укрепление доверия и безопасности при использовании информационно-коммуникационных технологий [Электронный Ресурс]// ITU NEWS. – 2010.- №10. – Режим доступа: https://itunews.itu.int/Ru/Note.aspx?Note=664. - (Дата обращения 27.10.15).
44. Обзор тенденций в телекоммуникационной отрасли. Банк развития Казахстана, БРК Аналитика. [Электронный ресурс]. – Режим доступа: http://www.kdb.kz/upload/files/view-IT.pdf. - (Дата обращения: 4.11.2015).
45. ИКТ в Казахстане: итоги 2013 года [Электронный ресурс]/ Портал о казахстанском рынке информационных технологий. – Режим доступа: http://profit.kz/news/16736/IKT-v-Kazahstane-itogi-2013-goda. - (Дата обращения: 4.11.2015).
46. «Электронное Правительство» в Казахстане – реальность? [Электронный ресурс]/ Портал о казахстанском рынке информационных технологий. – Режим доступа: http://profit.kz/articles/1865/Elektronnoe-Pravitelstvo-v-Kazahstane-realnost/. - (Дата обращения: 4.11.2015).
47. Проект закона республики Казахстан о «О защите детей от информации, причиняющий вред их здоровью и развитию» [Электронный ресурс]. – Режим доступа: http://www.adilsoz.kz/upload/Bill/bill_16_1.pdf. - (Дата обращения: 04.11.2015).
48. Накипова, Ж. МТСНЗ совместно с АСИ разрабатывает электронные госуслуги для инвалидов [Электронный ресурс]/Жанна Накипова// bnews.kz. – 2014. – Режим доступа: http://bnews.kz/ru/news/post/199699/. - (Дата обращения: 04.11.2015).
49. Портал инвалидов Казахстана. [Интернет-портал]. – Режим доступа: http://www.invalid.kz/. - (Дата обращения: 04.11.2015).
50. К вопросу по обеспечению информационной безопасности KZ-CERT. Служба реагирования на компьютерные инциденты [Электронный ресурс]. – Режим доступа: http://kz-cert.kz/ru/publication/?doc=7. - (Дата обращения: 13.11.2015).
51. Тумашова, Е. Обороты e-commerce [Электронный ресурс]/ Е. Тумашова// Информационное агентство «Деловой Казахстан». - 2013.- Режим доступа: http://dknews.kz/oboroty-e-commerce/. - (Дата обращения: 06.11.2015).

52. 4 проблемы e-commerce в Казнете [Электронный ресурс]: Сообщество «Интернет коммерция». – Режим доступа: http://yvision.kz/post/112959. - (Дата обращения: 06.11.2015).
53. Бейсенбаева, Ж. Логистика для e-commerce и трансграничная торговля [Электронный ресурс] / Жаннель Бейсенбаева // Центр деловой информации «КАПИТАЛ». – 2015. – Режим доступа: http://kapital.kz/business/37855/logistika-dlya-e-commerce-i-transgranichnaya-torgovlya.html. - (Дата обращения: 10.11.2015)
54. Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии [Электронный ресурс]/ Международный Союз Электросвязи (МСЭ). – Режим доступа: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf. - (Дата обращения: 14.11.2015).
55. Саморукова, И. Доверие и безопасность - основные тенденции в развитии сотрудничества в РСС [Электронный ресурс] / И. Саморукова, Н. Мухитдинов // Информационная безопасность «InformationSecurity». – Режим доступа: http://www.itsec.ru/articles2/focus/doverie-i-bezopasn-osnovn-tendenc-v-razvitii-sotrudnich-v-rss. - (Дата обращения: 08.11.2015).
56. Кыргызская Республика [Электронный ресурс]. – Режим доступа: Информационно-аналитический портал Центр гуманитарных технологий http://gtmarket.ru/countries/kyrgyzstan/kyrgyzstan-info. - Заглавие с экрана.
57. Проект стратегии по внедрению электронного управления в государственных органахисполнительной власти и органах местного самоуправления Кыргызской Республики на 2014 - 2017 годы (Окончательная версия со стороны ЮМ от 29 января 2014 года) [Электронный ресурс]/ Министерство экономики Кыргызской Республики. – Режим доступа: http://mineconom.gov.kg/Docs/antimonopol/e_upravlenie.pdf.
58. Стратегия сотрудничества государств – участников Содружества Независимых Государств в построении и развитии информационного общества на период до 2025 года [Электронный ресурс]/ Официальный сайт Минкомсвязь России. – Режим доступа: www.minsvyaz.ru/uploaded/files/20p502172proekt-strategii-do-2025-g-70415.doc
59. Региональная инициатива, утвержденная ВКРЭ-14 «Укрепление доверия и безопасности при использовании ИКТ» [Электронный ресурс]. – Режим доступа: http://www.itu.int/ru/ITU-D/Regional-Presence/CIS/Pages/Regional%20Initiatives/Confidence%20in%20ICT/Confidence-in-ICT.aspx.
60. Централизованный банк данных правовой информации Кыргызской Республики [Электронный ресурс]. – Режим доступа: http://cbd.minjust.gov.kg/. – Заглавие с экрана.
61. World Economic Forum [Электронный ресурс]. – Режим доступа: http://reports.weforum.org/global-information-technology-report-2015/analysis-and-key-findings/. – Заглавие с экрана.
62. «e-Услуги» для бизнеса [Электронный ресурс]/ Mybusiness.md: онлайн-журнал. – 2014. – Режим доступа: http://mybusiness.md/categories/item/1513-e-uslugi-dlja-biznesa.
63. Кодекс телевидения и радио Республики Молдова от 27 июля 2006 года 260-XVI [Электронный ресурс]. – Режим доступа: http://lex.justice.md/document_rus.php?id=7C2C8A51:51D0B3BF.
64. О социальной интеграции лиц с ограниченными возможностями [Электронный ресурс]: Закон Республики Молдова от 30 марта 2012 года №60. – Режим доступа: http://www.allmoldova.com/news/v-moldove-otkrylas-laboratoriya-po-podgotovke-specialistov-v-oblasti-it/.

65. Формирование Электронного правительства Молдовы [Электронный ресурс]: Новости интернет-ресурса «Открытое правительство». – 2013. – Режим доступа: http://open.gov.ru/events/5511614/.
66. Инвестиционные возможности сектора ИКТ Молдовы [Электронный ресурс]: Новости официального сайта Министерства информационных технологий и связи Молдовы. – 2015. – Режим доступа: http://www.mtic.gov.md/ru/news/investicionnye-vozmozhnosti-sektora-ikt-moldovy-predstavleny-na-ekspo-2015-v-milane .
67. Об утверждении Стратегии защиты ребенка на 2014-2020 годы [Электронный ресурс]: Постановление Правительства Республики Молдова от 10 июня 2014 года №434. – Режим доступа: http://lex.justice.md/index.php?action=view&id=353459&lang=2&view=doc
68. Стратегическое направление деятельность Совета операторов электросвязи и инфокоммуникаций Регионального содружества в области связи – утверждено Решением 49/12.1 Совета глав АС РСС [Электронный ресурс]. – Режим доступа: http://rcc.org.ru/about/rabochie_organi/sovet_operatorov/zapravlenie_deyatelnocti.
69. Об электронных коммуникациях [Электронный ресурс]: Закон республики Молдова от 14.11.2007 №241. – Режим доступа: http://ru.anrceti.md/fileupload/1.
70. Стратегия сотрудничества государств – участников Содружества Независимых Государств в построении и развитии информационного общества на период до 2025 года [Электронный ресурс]. – Режим доступа: http://www.e-cis.info.
71. О реализации решений Совета глав государств СНГ и Совета глав правительств СНГ по вопросам дальнейшего сотрудничества в области ИКТ [Электронный ресурс]. – Режим доступа: http://www.old.rcc.org.ru/index.php?option=com_content&view=article&id=74&Itemid=399.
72. Отчет о проведении семинара МСЭ «Переход с IPv4 на IPv6: регуляторные и технические аспекты», Кишинев, Республика Молдова, 24-25 мая 2012 года [Электронный ресурс]. – Режим доступа: http://www.itu.int/ru.
73. Разработанная ВВУИО+10 концепция ВВУИО на период после 2015 года. [Электронный ресурс]. – Режим доступа: http://www.itu.int/ru.
74. Костров Д.В. Интегрирование в мировое киберпространство — единственный выход [Электронный ресурс]. - 2015. – Режим доступа: http://aciso.ru/news/3593/. - (Дата обращения: 02.11.2015).
75. Анализ состояния и перспектив развития российского рынка телекоммуникационных услуг в сегментах B2C, B2B и B2G [Электронный ресурс]. - 2014. – Режим доступа: http://www.mobilecomm.ru/analiz-sostoyaniya-i-perspektiv-razvitiya-rossiyskogo-rinka-telekommunikatsionnich-uslug-v-segmentach-b2c-b2b-b2g. - (Дата обращения: 05.11.2015).
76. Мобильные технологии-2015: [Электронный ресурс]. - 2015. – Режим доступа: http://ingvarr.net.ru/publ/5-1-0-15314. - (Дата обращения: 06.11.2015).
77. Гайдарева, И.Н. Правовое обеспечение информационной безопасности в России [Электронный ресурс]. - 2014. – Режим доступа: http://cyberleninka.ru/article/n/pravovoe-obespechenie-informatsionnoy-bezopasnosti-v-rossii. - (Дата обращения: 07.11.2015).
78. Единый портал государственных услуг (ЕПГУ) [Электронный ресурс]. - 2015. - Режим доступа: http://www.minsvyaz.ru/ru/activity/directions/7/. - (Дата обращения: 07.11.2015).
79. Безопасность детей в интернете - Лаборатория Касперского [Электронный ресурс]. - 2014. – Режим доступа: http://www.kaspersky.ru/internet-security-center/internet-safety/kids-online-safety. - (Дата обращения: 08.11.2015).

80. Меритт, Мэриан 10 советов по защите детей в интернете [Электронный ресурс] / Мэриан Меритт// Norton: официальный сайт - 2014. – Режим доступа: http://ru.norton.com/kids-safe/article. - (Дата обращения: 08.11.2015).
81. Мобильные и ИКТ технологии в помощь пожилым и слабослышащим людям [Электронный ресурс]. - 2015. – Режим доступа: http://expert.ru/2015/05/22/mobilnyie-i-ikt-tehnologii-v-pomosch-pozhilyim-lyudyam-i-lyudyam-s-ogranichennyimi-vozmozhnostyami/?ny. - (Дата обращения: 09.11.2015).
82. Меморандум о взаимодействии операторов электросвязи и инфокоммуникаций стран участников РСС в сфере обеспечения информационной безопасности [Электронный ресурс]. - 2014. – Режим доступа: http://www.gosbook.ru/node/66086. - (Дата обращения: 09.11.2015).
83. Третьяков, А. Угрозы и перспективы интернет-торговли [Электронный ресурс]/ А. Третьяков// Эксперт OnLine. - 2014. – Режим доступа: http://expert.ru/northwest/2014/19/ugrozyi-i-perspektivyi-internet-torgovli/. - (Дата обращения: 10.11.2015).
84. Количество пользователей мобильной связи в Украине достигло 58,63 млн. [Электронный ресурс]. – Режим доступа: http://itexpert.org.ua/rubrikator/item/24657-kolichestvo-polzovatelej-mobilnoj-svyazi-v-ukraine-dostiglo-5863-mln.html.
85. Киевстар официальный сайт [Электронный ресурс]. – Режим доступа: http://www.kyivstar.ua.
86. МТС Украина официальный сайт [Электронный ресурс]. – Режим доступа: http://www.mts.ua.
87. Life:) официальный сайт [Электронный ресурс]. – Режим доступа: http://www.life.ua/ru/.
88. Интертелеком официальный сайт [Электронный ресурс]. – Режим доступа: http://www.intertelecom.ua/.
89. Akamai. The State of the Internet Report. AMERICAS HIGHLIGHTS – FIRST QUARTER, 2014. – Режим доступа: https://www.akamai.com/us/en/about/news/press/2014-press/akamai-first-quarter-2014-state-of-the-internet-report.jsp.
90. Рейтинг интернет-провайдеров по итогам 1-го квартала 2015 года [Электронный ресурс]/ Expert & Consulting (E&C). – Режим доступа: http://www.encint.com/ratings/broadband1q2015.
91. Измерение информационного общества. Международный союз электросвязи [Электронный ресурс]. - 2012. – Режим доступа: http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2012-SUM-PDF-R.pdf.
92. Измерение информационного общества. Международный союз электросвязи [Электронный ресурс]. - 2014. – Режим доступа: http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2014-SUM-PDF-R.pdf.
93. iKS-Consulting: украинский рынок широкополосного доступа в интернет (IV квартал 2014 года) [Электронный ресурс]. – 2015. – Режим доступа: http://itc.ua/news/iks-consulting-ryinok-shirokopolosnogo-dostupa-v-internet-ukrainyi-iv-kvartal-2014-goda/.
94. Кабмин одобрил законопроект «Об основных мерах кибербезопасности» [Электронный ресурс] – Режим доступа: http://112.ua/politika/kabmin-odobril-zakonoproekt-o-merah-kiberbezopasnosti-141151.html.
95. О Стратегии сотрудничества государств-участников СНГ в построении и развитии информационного общества и Плане действий по ее реализации на период до 2015 года от

28 сентября 2012 года [Электронный ресурс]. – Режим доступа: http://www.e-cis.info/page.php?id=22902.

96. Единый портал госуслуг Украины [Электронный ресурс]. – Режим доступа: http://poslugy.gov.ua/.
97. Система электронных обращений граждан [Электронный ресурс]. – Режим доступа: http://z.gov.ua.
98. МСЭ-D 1-я Исследовательская комиссия. ВОПРОС 20/1: Доступ к услугам электросвязи для лиц с ограниченными возможностями [Электронный ресурс]. – Режим доступа: http://www.itu.int/ru/Pages/default.aspx.
99. Зелинский, С. Системные проблемы мешают ИТ-образованию на Украине [Электронный ресурс]/ С. Зелинский// CNews: интернет-издание. – Режим доступа: http://corp.cnews.ru/reviews/free/edu2004/cis/ukraine.shtml.
100. Клюка, А. Исследование рынка электронной коммерции в Украине [Электронный ресурс]/ А. Клюка// AIN.UA: интернет-журнал. - 2013. – Режим доступа: http://ain.ua/2013/04/11/120835.
101. Инфографика: чем торгует украинский бизнес за рубежом [Электронный ресурс]/ Forbes Украина: интернет-журнал. - Режим доступа: http://forbes.net.ua/business/1401872-infografika-chem-torguet-ukrainskij-biznes-za-rubezhom.
102. Укрепление доверия и безопасности при использовании информационно-коммуникационных технологий [Электронный ресурс]/ официальный сайт МСЭ. – Режим доступа: https://www.itu.int/net/itunews/issues/2010/10/pdf/201010_39-ru.pdf.
103. Новости Азербайджана и мировые новости [Электронный ресурс]. – Режим доступа: http://minval.az. – Заголовок с экрана.
104. РБК-новости [Электронный ресурс]. – Режим доступа: http://www.rbc.ru.
105. Азербайджан намерен перевести все госуслуги в электронный вид к 2020 г. [Электронный ресурс]/ Али Аббасов (министр связи и высоких технологий Азербайджана), научно-практическая конференции «Проблемы построения электронного правительства». – Режим доступа: http://d-russia.ru/azerbajdzhan-nameren-perevesti-vse-gosuslugi-v-elektronnyj-vid-k-2020-g.html.
106. Азербайджан расширяет перечень услуг электронного правительства [Электронный ресурс]/ Новости PRAVO.BY. – Режим доступа: http://www.pravo.by/main.aspx?guid=35393.
107. Жизнь без границ! Портал для людей с инвалидностью [Электронный ресурс]. – Режим доступа: http://www.bezgraniz.com/blog/2010/page/1428/. – Заголовок с экрана.

Приложение 1. Типовые требования к виду профессиональной деятельности «Системный администратор информационно-коммуникационных систем»

I. Общие сведения

Администрирование информационно-коммуникационных (инфокоммуникационных) систем

(наименование вида профессиональной деятельности)

Основная цель вида профессиональной деятельности:

Обеспечение требуемого качественного бесперебойного режима работы инфокоммуникационной системы

Группа занятий:

(код ОКЗ)	(наименование)	(код ОКЗ)	(наименование)
2131	Разработчики и аналитики компьютерных систем	3122	Техники и операторы по обслуживанию компьютерных устройств
2144	Инженеры-электроники, инженеры по связи и приборостроению	7522	Профессии рабочих по обслуживанию и ремонту линейных сооружений и станционного оборудования связи
3114	Техники-электроники и техники по телекоммуникациям	-	-

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида трудовой деятельности)

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Администрирование структурированной кабельной системы (СКС)	4	Документирование инфраструктуры СКС и ее составляющих	A/01.4	4
			Мониторинг СКС с целью локализации неисправностей	A/02.4	4
B	Администрирование прикладного программного обеспечения инфокоммуникационной системы организации	5	Установка прикладного программного обеспечения	B/01.5	5
			Оценка критичности возникновения инцидентов при работе прикладного программного обеспечения	B/02.5	5
			Оптимизация функционирования прикладного программного обеспечения	B/03.5	5
			Интеграция прикладного программного обеспечения в единую структуру инфокоммуникационной системы	B/04.5	5
			Реализация регламентов обеспечения информационной безопасности прикладного программного обеспечения	B/05.5	5
			Разработка нормативно-технической документации на процедуры управления прикладным программным обеспечением	B/06.5	5
			Разработка требований к аппаратному обеспечению и поддерживающей инфраструктуре для эффективного функционирования прикладного программного обеспечения	B/07.5	5
C	Управление программно-аппаратными средствами информационных служб инфокоммуникационной системы организации	6	Установка персональных компьютеров, учрежденческой автоматической телефонной станции (УАТС), подключение периферийных и абонентских устройств	C/01.6	6
			Управление доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы	C/02.6	6
			Мониторинг событий, возникающих в процессе работы	C/03.6	6

			инфокоммуникационной системы		
			Восстановление работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев	C/04.6	6
			Протоколирование событий, возникающих в процессе работы инфокоммуникационной системы	C/05.6	6
			Ввод в эксплуатацию аппаратных, программно-аппаратных и программных средств инфокоммуникационной инфраструктуры совместно с представителями поставщиков оборудования	C/06.6	6
			Обслуживание периферийного оборудования	C/07.6	6
			Организация инвентаризации технических средств	C/08.6	6
D	Администрирование сетевой подсистемы инфокоммуникационной системы организации	6	Настройка сетевых элементов инфокоммуникационной системы	D/01.6	6
			Контроль за использованием ресурсов сетевых устройств и программного обеспечения	D/02.6	6
			Управление безопасностью сетевых устройств и программного обеспечения	D/03.6	6
			Диагностика отказов и ошибок сетевых устройств и программного обеспечения	D/04.6	6
			Контроль производительности сетевой инфраструктуры инфокоммуникационной системы	D/05.6	6
			Проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	D/06.6	6
E	Администрирование систем управления базами данных инфокоммуникационной системы организации	7	Инсталляция (установка) системы управления базой данных (СУБД)	E/01.7	7
			Мониторинг работы СУБД	E/02.7	7
			Настройка систем резервного копирования и восстановления баз данных	E/03.7	7
F	Администрирование системного программного обеспечения	7	Установка системного программного обеспечения	F/01.7	7
			Оптимизация работы дисковой подсистемы (подсистемы ввода-вывода)	F/02.7	7

	инфокоммуникационной системы организации		Администрирование файловых систем	F/03.7	7
			Оценка критичности возникновения инцидентов для системного программного обеспечения	F/04.7	7
			Реализация регламентов обеспечения информационной безопасности системного программного обеспечения инфокоммуникационной системы организации	F/05.7	7
G	Управление развитием инфокоммуникационной системы организации	7	Анализ системных проблем обработки информации на уровне инфокоммуникационной системы	G/01.7	7
			Подготовка предложений по развитию инфокоммуникационной системы	G/02.7	7
			Разработка нормативной и технической документации на аппаратные средства и программное обеспечение	G/03.7	7
			Контроль обновления версий аппаратных, программно-аппаратных и программных средств	G/04.7	7

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

Наименование	Администрирование структурированной кабельной системы (СКС)	Код	A	Уровень квалификации	4

Возможные наименования должностей	Младший специалист отдела инфокоммуникационных технологий Менеджер отдела инфокоммуникационных технологий Младший системный администратор

Требования к образованию и обучению	Среднее профессиональное образование – программы подготовки квалифицированных рабочих (служащих)
Требования к опыту практической работы	Не менее трех месяцев работы в области технической поддержки, администрирования, программирования устройств инфокоммуникационных систем
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	7522	Профессии рабочих по обслуживанию и ремонту линейных сооружений и станционного оборудования связи

3.1.1. Трудовая функция

Наименование	Документирование инфраструктуры СКС и ее составляющих	Код	A/01.4	Уровень (подуровень) квалификации	4

Трудовые действия	Обозначение всех элементов, составляющих кабельную подсистему инфокоммуникационной системы
	Учет всех элементов, составляющих кабельную подсистему инфокоммуникационной системы
	Обозначение всех элементов трасс прокладки телекоммуникационных кабелей
	Учет всех элементов трасс прокладки телекоммуникационных кабелей
	Обозначение телекоммуникационных и других помещений, в которых монтируются составляющие инфокоммуникационной системы
	Учет телекоммуникационных и других помещений, в которых монтируются составляющие инфокоммуникационной системы
	Документирование изменений в администрируемой кабельной системе
	Взаимодействие с внешней организацией, монтирующей оптические кабели
Необходимые умения	Вести нормативно-техническую документацию по структурированной кабельной системе (СКС)
	Пользоваться нормативно-технической документацией в области

	инфокоммуникационных технологий
	Организовывать инвентаризацию технических средств
	Фиксировать в журнале инвентарный номер устройства и месторасположение установленного устройства
	Маркировать элементы СКС
Необходимые знания	Среды передачи данных
	Типы и технические характеристики кабелей связи
	Составляющие волоконно-оптических линий передачи
	Типы коннекторов телекоммуникационных кабелей
	Подсистемы и элементы СКС
	Стандарты создания телекоммуникаций служебных и производственных зданий
	Планирование кабельных систем зданий
	Методика построения системы телекоммуникаций служебных и производственных зданий
	Стандарты на помещения, в которых устанавливается СКС и телекоммуникационное оборудование
	Стандарты администрирования телекоммуникационной инфраструктуры в служебных и производственных зданиях
	Стандарты на инфраструктуру телекоммуникационной системы заземления и выравнивания потенциалов в служебных и производственных зданиях
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.1.2. Трудовая функция

Наименование	Мониторинг СКС с целью локализации неисправностей	Код	A/02.4	Уровень (подуровень) квалификации	4

Трудовые действия	Установка системы управления СКС
	Контроль правильности работы СКС
	Локализация неисправностей в работе СКС
	Устранение выявленных неисправностей в работе СКС
	Документирование изменений в администрируемой СКС
Необходимые умения	Применять специализированные контрольно-измерительные приборы и оборудование
	Работать со специализированными коммутационными кабелями – патч-кордами
	Вести нормативно-техническую документацию
Необходимые знания	Регламенты профилактических работ на администрируемой СКС
	Специализированное программное обеспечение для работы с аппаратными средствами администрирования СКС
	Стандарты администрирования телекоммуникационной инфраструктуры

	в служебных и производственных зданиях
	Составляющие волоконно-оптических линий передачи
	Типы коннекторов телекоммуникационных кабелей
	Подсистемы и элементы СКС
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.2. Обобщенная трудовая функция

Наименование	Администрирование прикладного программного обеспечения инфокоммуникационной системы организации	Код	B	Уровень квалификации	5

Возможные наименования должностей	Системный техник Младший системный администратор

Требования к образованию и обучению	Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных и телекоммуникационных технологий или
Требования к опыту практической работы	Не менее трех месяцев работы в области технической поддержки, администрирования, программирования устройств инфокоммуникационных систем
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	3114	Техники-электроники и техники по телекоммуникациям
	3122	Техники и операторы по обслуживанию компьютерных устройств

3.2.1. Трудовая функция

Наименование	Установка прикладного программного обеспечения	Код	B/01.5	Уровень (подуровень) квалификации	5

Трудовые действия	Запуск процедуры установки прикладного программного обеспечения на конечных устройствах пользователей и/или серверном оборудовании
	Мониторинг процедуры установки прикладного программного обеспечения

	Контроль процедуры установки прикладного программного обеспечения
	Лицензионная регистрация прикладного программного обеспечения на конечных устройствах пользователей и/или серверном оборудовании
	Настройка установленного прикладного программного обеспечения на конечных устройствах пользователей и/или серверном оборудовании
	Обновление установленного прикладного программного обеспечения на конечных устройствах пользователей и/или серверном оборудовании
Необходимые умения	Соблюдать процедуру установки прикладного программного обеспечения в соответствии с требованиями организации - производителя
	Идентифицировать инциденты, возникающие при установке программного обеспечения и принять решение по изменению процедуры установки
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Лицензионные требования по настройке устанавливаемого программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Основы архитектуры, устройства и функционирования вычислительных систем
	Принципы организации, состав и схемы работы операционных систем
	Стандарты информационного взаимодействия систем
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.2.2. Трудовая функция

Наименование	Оценка критичности возникновения инцидентов при работе прикладного программного обеспечения	Код	B/02.5	Уровень (подуровень) квалификации	5

Трудовые действия	Обнаружение критических инцидентов при работе прикладного программного обеспечения
	Определение причин возникновения критических инцидентов при работе прикладного программного обеспечения
	Выполнение действий по устранению критических инцидентов при работе прикладного программного обеспечения в рамках должностных обязанностей
	Идентификация инцидентов при работе прикладного программного обеспечения
	Регистрация инцидентов при работе прикладного программного обеспечения
Необходимые умения	Идентифицировать инциденты при работе прикладного программного обеспечения
	Оценивать степень критичности инциденты при работе прикладного программного обеспечения

	Устранять возникающие инциденты
Необходимые знания	Лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Принципы организации, состав и схемы работы операционных систем
	Стандарты информационного взаимодействия систем
	Основы делопроизводства
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.2.3. Трудовая функция

Наименование	Оптимизация функционирования прикладного программного обеспечения	Код	B/03.5	Уровень (подуровень) квалификации	5

Трудовые действия	Анализ функционирования прикладного программного обеспечения по значимым параметрам
	Разработка плана работ по оптимизации функционирования прикладного программного обеспечения инфокоммуникационной системы
	Выполнение работ по оптимизации функционирования прикладного программного обеспечения инфокоммуникационной системы и оценка результата
Необходимые умения	Анализировать функционирование инфокоммуникационной системы по выбранным параметрам
	Использовать специализированное программное обеспечение для оптимизации функционирования прикладного программного обеспечения
	Выполнять настройку прикладного программного обеспечения в соответствии с принятыми критериями оптимизации
Необходимые знания	Основные параметры функционирования инфокоммуникационной системы
	Методы измерения параметров функционирования прикладного программного обеспечения инфокоммуникационной системы
	Методы контроля параметров функционирования прикладного программного обеспечения инфокоммуникационной системы
	Методы мониторинга параметров функционирования прикладного программного обеспечения инфокоммуникационной системы
	Принципы оптимизации инфокоммуникационных систем
	Методы оптимизации инфокоммуникационных систем
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с аппаратными, программно-

	аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.2.4. Трудовая функция

Наименование	Интеграция прикладного программного обеспечения в единую структуру инфокоммуникационной системы	Код	B/04.5	Уровень (подуровень) квалификации	5

Трудовые действия	Анализ структуры и параметров функционирования интегрируемого прикладного программного обеспечения
	Выбор принципов и методов интеграции прикладного программного обеспечения инфокоммуникационных систем
	Выполнение работ в соответствии с выбранным методом интеграции
	Тестирование интегрированной системы
	Запуск в эксплуатацию интегрированной инфокоммуникационной системы
Необходимые умения	Анализировать функционирование интегрируемого прикладного программного обеспечения
	Выполнять настройку прикладного программного обеспечения
	Оценивать функционирование прикладного программного обеспечения в рамках единой структуры инфокоммуникационной системы
Необходимые знания	Основные параметры функционирования интегрируемого прикладного программного обеспечения администрируемой инфокоммуникационной системы и/или ее составляющих
	Методы измерения параметров функционирования прикладного программного обеспечения в рамках единой структуры инфокоммуникационной системы
	Методы контроля параметров функционирования прикладного программного обеспечения в рамках единой структуры инфокоммуникационной системы
	Методы мониторинга параметров функционирования прикладного программного обеспечения в рамках единой структуры инфокоммуникационной системы
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.2.5. Трудовая функция

Наименование	Реализация регламентов обеспечения информационной безопасности прикладного программного обеспечения	Код	B/05.5	Уровень (подуровень) квалификации	5

Трудовые действия	Установка аппаратно-программных средств защиты прикладного программного обеспечения
	Настройка аппаратно-программных средств защиты прикладного программного обеспечения
	Проведение регламентов обеспечения защиты информации в соответствии с политикой информационной безопасности
	Проведение регламентов обеспечения защиты информационных систем в соответствии с политикой информационной безопасности (в том числе управление правами доступа)
Необходимые умения	Выполнять настройку прикладного программного обеспечения в соответствии с регламентами обеспечения информационной безопасности
	Производить авторизацию пользователей прикладного программного обеспечения
	Применять программно-аппаратные средства защиты информации
	Применять программные средства защиты информации
Необходимые знания	Основы обеспечения информационной безопасности
	Отраслевые и локальные нормативно-правовые акты в области информационной безопасности, действующие в организации
	Типовые уязвимости, учитываемые при настройке устанавливаемого программного обеспечения
	Типовые уязвимости, учитываемые при эксплуатации устанавливаемого программного обеспечения
	Методы и средства защиты информации
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Регламенты обеспечения информационной безопасности
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.2.6. Трудовая функция

Наименование	Разработка нормативно-технической документации на процедуры управления прикладным программным обеспечением	Код	B/06.5	Уровень (подуровень) квалификации	5

Трудовые действия	Разработка технических заданий на процедуры управления программным обеспечением инфокоммуникационной системы
	Разработка нормативно-технической документации на процедуры настройки и интеграции прикладного программного обеспечения, включая инструкции для пользователей
	Актуализация нормативно-технической документации на процедуры настройки и интеграции прикладного программного обеспечения, включая инструкции для пользователей
	Хранение нормативно-технической документации на процедуры настройки и интеграции прикладного программного обеспечения, включая инструкции для пользователей

	Уничтожение нормативно-технической документации на процедуры настройки и интеграции прикладного программного обеспечения, включая инструкции для пользователей
Необходимые умения	Применять отраслевую нормативную документацию на аппаратное обеспечение инфокоммуникационной системы
	Оформлять техническую документацию на аппаратное обеспечение инфокоммуникационной системы
	Применять отраслевую нормативную документацию на программно-аппаратное обеспечение инфокоммуникационной системы
	Оформлять техническую документацию на программно-аппаратное обеспечение инфокоммуникационной системы
	Применять отраслевую нормативную документацию на программное обеспечение инфокоммуникационной системы
	Оформлять нормативную и техническую документацию на программное обеспечение инфокоммуникационной системы
Необходимые знания	Требования к структуре, содержанию и оформлению нормативной документации
	Требования к структуре, содержанию и оформлению технической документации
	Основы документационного обеспечения деятельности информационно-технологических структурных подразделений организации
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.2.7. Трудовая функция

Наименование	Разработка требований к аппаратному обеспечению и поддерживающей инфраструктуре для эффективного функционирования прикладного программного обеспечения	Код	B/07.5	Уровень (подуровень) квалификации	5

Трудовые действия	Контроль текущего состояния аппаратного обеспечения и поддерживающей инфраструктуры
	Мониторинг текущего состояния аппаратного обеспечения и поддерживающей инфраструктуры
	Анализ текущего состояния аппаратного обеспечения и поддерживающей инфраструктуры
	Формирование требований к аппаратному обеспечению и поддерживающей инфраструктуре инфокоммуникационной системы
Необходимые умения	Оценивать инциденты, возникающие в ходе эксплуатации аппаратного обеспечения и поддерживающей инфраструктуры
	Оценивать технические параметры аппаратного обеспечения и поддерживающей инфраструктуры, необходимые для эффективного

	функционирования прикладного программного обеспечения
	Формировать критерии для выбора аппаратного обеспечения и поддерживающей инфраструктуры
	Идентифицировать класс аппаратного обеспечения и поддерживающей инфраструктуры для эффективного функционирования прикладного программного обеспечения
Необходимые знания	Основные типы аппаратного обеспечения
	Основные типы объектов поддерживающей инфраструктуры
	Основные характеристики аппаратного обеспечения
	Основные характеристики объектов поддерживающей инфраструктуры
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.3. Обобщенная трудовая функция

Наименование	Код	Уровень квалификации
Управление программно-аппаратными средствами информационных служб инфокоммуникационной системы организации	C	6

Возможные наименования должностей	Системный администратор Специалист Инженер

Требования к образованию и обучению	Высшее образование – бакалавриат или Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных и телекоммуникационных технологий
Требования к опыту практической работы	Не менее одного года работы в области технической поддержки, администрирования, программирования устройств инфокоммуникационных систем при среднем профессиональном (техническом) образовании
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и

		приборостроению
	3114	Техники-электроники и техники по телекоммуникациям
	3122	Техники и операторы по обслуживанию компьютерных устройств

3.3.1. Трудовая функция

Наименование	Установка персональных компьютеров, учрежденческой автоматической телефонной станции (УАТС), подключение периферийных и абонентских устройств	Код	C/01.6	Уровень (подуровень) квалификации	6

Трудовые действия	Проверка возможности установки УАТС в помещениях организации
	Проверка возможности подключения УАТС к инфокоммуникационной системе
	Проверка системы электропитания
	Установка УАТС, абонентских и периферийных устройств согласно инструкции
	Проверка функционирования устройств
	Фиксирование в журнале инвентарных номеров устройств и месторасположения каждого установленного устройства
	Маркировка абонентских и периферийных устройств
	Инсталляция программного обеспечения для поддержки работы пользователей
	Настройка программного обеспечения для поддержки работы пользователей
	Документирование параметров настройки программного обеспечения
Необходимые умения	Конфигурировать УАТС
	Конфигурировать периферийные устройства
	Конфигурировать абонентские устройства
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Организовывать инвентаризацию периферийных и абонентских технических средств
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемой УАТС
	Инструкции по эксплуатации администрируемой УАТС
	Инструкции по установке администрируемого периферийного оборудования
	Инструкции по эксплуатации администрируемого периферийного оборудования
	Инструкции по установке администрируемого абонентского

	оборудования
	Инструкции по эксплуатации администрируемого абонентского оборудования
	Принципы установки и настройки программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.3.2. Трудовая функция

Наименование	Управление доступом к программно-аппаратным средствам информационных служб инфокоммуникационной системы	Код	C/02.6	Уровень (подуровень) квалификации	6

Трудовые действия	Назначение прав доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы
	Изменение прав доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы
	Применение специальных процедур по управлению правами доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы
	Контроль соблюдения прав доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы
	Техническая поддержка пользователей в пределах выделенных зон ответственности по вопросам функционирования программного обеспечения на конечных устройствах пользователей
Необходимые умения	Идентифицировать права пользователей по доступу к программно-аппаратным средствам информационных служб инфокоммуникационной системы и/или ее составляющих
	Применять специальные программно-аппаратные средства контроля доступа пользователей к программно-аппаратным средствам информационных служб инфокоммуникационной системы
	Пользоваться нормативно-технической документацией на администрируемые аппаратные, программно-аппаратные и программные средства
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемого телекоммуникационного оборудования
	Инструкции по эксплуатации администрируемого телекоммуникационного оборудования
	Инструкции по установке администрируемого компьютерного

	оборудования
	Инструкции по эксплуатации администрируемого компьютерного оборудования
	Инструкции по установке администрируемого сетевого оборудования
	Инструкции по эксплуатации администрируемого сетевого оборудования
	Инструкции по установке администрируемого периферийного оборудования
	Инструкции по эксплуатации администрируемого периферийного оборудования
	Инструкции по установке администрируемого абонентского оборудования
	Инструкции по эксплуатации администрируемого абонентского оборудования
	Принципы установки и настройки программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты по организации доступа к программно-аппаратным средствам информационных служб, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.3.3. Трудовая функция

Наименование	Мониторинг событий, возникающих в процессе работы инфокоммуникационной системы	Код	C/03.6	Уровень (подуровень) квалификации	6

Трудовые действия	Наблюдение за работой инфокоммуникационной системы и/или ее составляющих
	Обнаружение отклонений от штатного режима работы инфокоммуникационной системы и/или ее составляющих
	Анализ отклонений от штатного режима работы инфокоммуникационной системы и/или ее составляющих
	Устранение возникающих отклонений от штатного режима работы инфокоммуникационной системы и/или ее составляющих
Необходимые умения	Отличать штатный режим работы инфокоммуникационной системы и/или ее составляющих от нештатного режима работы
	Применять специализированные контрольно-измерительные средства
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Типовые ошибки, возникающие при работе инфокоммуникационной системы, признаки их проявления при работе и методы устранения
	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети

	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемого телекоммуникационного оборудования
	Инструкции по эксплуатации администрируемого телекоммуникационного оборудования
	Инструкции по установке администрируемого компьютерного оборудования
	Инструкции по эксплуатации администрируемого компьютерного оборудования
	Инструкции по установке администрируемого сетевого оборудования
	Инструкции по эксплуатации администрируемого сетевого оборудования
	Инструкции по установке администрируемого периферийного оборудования
	Инструкции по эксплуатации администрируемого периферийного оборудования
	Инструкции по установке администрируемого абонентского оборудования
	Инструкции по эксплуатации администрируемого абонентского оборудования
	Принципы установки и настройки программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты по организации доступа к программно-аппаратным средствам информационных служб, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.3.4. Трудовая функция

Наименование	Восстановление работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев	Код	C/04.6	Уровень (подуровень) квалификации	6

Трудовые действия	Анализ сбоев функционирования программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих
	Выявление причин возникновения аварийных ситуаций на программно-аппаратных средствах инфокоммуникационной системы и/или ее составляющих
	Разработка схемы и процедуры послеаварийного восстановления работоспособности инфокоммуникационной системы и/или ее составляющих
	Фиксирование причины и результаты восстановления работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих
Необходимые умения	Устанавливать программно-аппаратные средства

	инфокоммуникационной системы и/или ее составляющих
	Выбирать способы восстановления работоспособности инфокоммуникационной системы и/или ее составляющих
	Документировать причины сбоев и результаты восстановления работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Правила и методы технического обслуживания программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих
	Правила и методы ремонта программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих
	Методы и средства восстановления работоспособности программно-аппаратных средств инфокоммуникационной системы и/или ее составляющих после сбоев
	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемого телекоммуникационного оборудования
	Инструкции по эксплуатации администрируемого телекоммуникационного оборудования
	Инструкции по установке администрируемого компьютерного оборудования
	Инструкции по эксплуатации администрируемого компьютерного оборудования
	Инструкции по установке администрируемого сетевого оборудования
	Инструкции по эксплуатации администрируемого сетевого оборудования
	Инструкции по установке администрируемого периферийного оборудования
	Инструкции по эксплуатации администрируемого периферийного оборудования
	Инструкции по установке администрируемого абонентского оборудования
	Инструкции по эксплуатации администрируемого абонентского оборудования
	Принципы установки и настройки программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты по организации доступа к программно-аппаратным средствам информационных служб, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.3.5. Трудовая функция

Наименование	Протоколирование событий, возникающих в процессе работы инфокоммуникационной системы	Код	C/05.6	Уровень (подуровень) квалификации	6

Трудовые действия	Фиксация отклонений от штатного режима работы инфокоммуникационной системы
	Ведение журнала учета отклонений от штатного режима работы инфокоммуникационной системы
	Информирование сотрудников, отвечающих за устранение отклонений от штатного режима работы инфокоммуникационной системы
Необходимые умения	Описывать работу инфокоммуникационной системы и/или ее составляющих и отклонения от штатного режима работы
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Техническая терминология, отражающая состояние инфокоммуникационной системы и ошибки в ее работе
	Технические инструкции по работе с установленным аппаратным, программно-аппаратным и программным обеспечением и оборудованием
	Основы делопроизводства
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.3.6. Трудовая функция

Наименование	Ввод в эксплуатацию аппаратных, программно-аппаратных и программных средств инфокоммуникационной инфраструктуры совместно с представителями поставщиков оборудования	Код	C/06.6	Уровень (подуровень) квалификации	6

Трудовые действия	Разработка правил приемки, монтажа и испытания вводимых в эксплуатацию новых аппаратных, программно-аппаратных и программных средств инфокоммуникационной инфраструктуры
	Разработка графиков приемки, монтажа и испытаний
	Проверка соответствия выполненных работ требованиям проектной документации
	Оформление актов ввода в эксплуатацию аппаратных, программно-аппаратных и программных средств инфокоммуникационной инфраструктуры совместно с представителями поставщиков оборудования

Необходимые умения	Анализировать требования проектной документации
	Проверять правильность монтажа аппаратных, программно-аппаратных и программных средств инфокоммуникационной инфраструктуры
	Проводить испытания вводимых в эксплуатацию аппаратных, программно-аппаратных и программных средств инфокоммуникационной инфраструктуры
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Правила приемки и сдачи выполненных работ
	Основы проектирования инфокоммуникационных систем
	Основы монтажа инфокоммуникационных систем
	Инструкции по установке программно-технических средств
	Инструкции по эксплуатации программно-технических средств
	Отраслевые и локальные нормативно-правовые акты по организации ввода в эксплуатацию аппаратных, программно-аппаратных и программных средств инфокоммуникационной инфраструктуры, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.3.7. Трудовая функция

Наименование	Обслуживание периферийного оборудования	Код	C/07.6	Уровень (подуровень) квалификации	6

Трудовые действия	Выявление причин неисправности периферийного оборудования
	Подбор комплектующих изделий для выполнения заявки по обслуживанию периферийного оборудования
	Проверка исправности комплектующих изделий периферийного оборудования
	Демонтаж поврежденных элементов периферийного оборудования
	Установка исправных комплектующих изделий в периферийное оборудование инфокоммуникационной системы
Необходимые умения	Заказывать комплектующие изделия для обслуживания периферийного оборудования
	Инсталлировать комплектующие изделия в инфокоммуникационные устройства
	Организовывать транспортировку комплектующих изделий
	Составлять акты списания поврежденных устройств
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования администрируемого периферийного оборудования

	Архитектура администрируемого периферийного оборудования
	Инструкции по установке телекоммуникационного, компьютерного, сетевого, абонентского и периферийного оборудования
	Инструкции по эксплуатации телекоммуникационного, компьютерного, сетевого, абонентского и периферийного оборудования
	Способы и приемы ремонта инфокоммуникационной техники
	Правила демонтажа периферийных устройств инфокоммуникационной техники
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
Другие характеристики	-

3.3.8. Трудовая функция

Наименование	Организация инвентаризации технических средств	Код	C/08.6	Уровень (подуровень) квалификации	6

Трудовые действия	Контроль выполнения графика проведения инвентаризации
	Контроль выполнения процедуры списания технических средств
	Регулярная проверка отчетов по результатам инвентаризации и списанию аппаратных, программно-аппаратных и программных средств
Необходимые умения	Вести техническую документацию по объектам инфокоммуникационной системы
	Контролировать наличие и движение аппаратных, программно-аппаратных и программных средств
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Правила и процедуры проведения инвентаризации
	Правила маркировки устройств и элементов инфокоммуникационной системы
	Основы делопроизводства
	Процедура списания технических средств
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.4. Обобщенная трудовая функция

Наименование	Администрирование сетевой подсистемы инфокоммуникационной системы	Код	D	Уровень квалификации	6

организации		

Возможные наименования должностей	Системный инженер Системный администратор

Требования к образованию и обучению	Высшее образование – бакалавриат или Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных и телекоммуникационных технологий
Требования к опыту практической работы	Не менее одного года работы в области системного администрирования при среднем профессиональном образовании
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
	3114	Техники-электроники и техники по телекоммуникациям
	3122	Техники и операторы по обслуживанию компьютерных устройств

3.4.1. Трудовая функция

Наименование	Настройка сетевых элементов инфокоммуникационной системы	Код	D/01.6	Уровень (подуровень) квалификации	6

Трудовые действия	Установка сетевых элементов инфокоммуникационной системы
	Подключение сетевых элементов инфокоммуникационной системы
	Конфигурирование операционных систем сетевых элементов инфокоммуникационной системы
	Проверка корректности функционирования администрируемых сетевых устройств и программного обеспечения
	Документирование первоначальных и измененных параметров установки
	Протоколирование событий, возникающих в процессе функционирования администрируемых сетевых устройств и программного обеспечения
	Установка систем управления сетью
	Настройка сетевого программного обеспечения
	Конфигурирование базовых параметров и сетевых интерфейсов

	Конфигурирование протоколов сетевого, канального и транспортного уровня
	Проверка функционирования устройства после установки и настройки программного обеспечения
	Конфигурирование протоколов управления
	Установка специального программного обеспечения для учета конфигураций, слежения за производительностью сетевой системы и защиты от несанкционированного доступа
	Настройка специального программного обеспечения для учета конфигураций, слежения за производительностью сетевой системы и защиты от несанкционированного доступа
	Документирование базовой конфигурации сетевых элементов инфокоммуникационной системы
Необходимые умения	Применять различные методы управления сетевыми устройствами
	Применять методы задания базовых параметров и параметров защиты от несанкционированного доступа к операционным системам
	Использовать методы статической и динамической конфигурации параметров операционных систем
	Применять специальные процедуры по управлению сетевыми устройствами
	Параметризировать протоколы канального, сетевого и транспортного уровня модели взаимодействия открытых систем
	Применять средства контроля и оценки конфигураций операционных систем
	Определять механизм изменения и модификации базовой конфигурации
	Внедрять процесс проверки текущей конфигурации на соответствие заданным базовым параметрам (аудит конфигурации)
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Восстановление параметров по умолчанию согласно документации по операционным системам
	Восстановление параметров при помощи серверов архивирования
	Восстановление параметров при помощи средств управления специализированных операционных систем сетевого оборудования
	Использовать типовые процедуры восстановления данных
	Работать с серверами архивирования и средствами управления операционными системами
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Модели информационно-телекоммуникационной сети «Интернет»
	Способы коммуникации процессов операционных систем
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Инструкции по установке администрируемых сетевых устройств

	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.4.2. Трудовая функция

Наименование	Контроль за использованием ресурсов сетевых устройств и программного обеспечения	Код	D/02.6	Уровень (подуровень) квалификации	6

Трудовые действия	Оценка производительности критических приложений, наиболее влияющих на производительность сетевых устройств и программного обеспечения в целом
	Планирование требуемой производительности сетевых устройств и программного обеспечения администрируемой сети
	Оценка требуемой производительности сетевых устройств и программного обеспечения администрируемой сети
	Ведение специального документа «Оценка готовности системы»
	Использование утилит операционных систем
	Установка дополнительных программных продуктов и их параметризация
Необходимые умения	Выяснять приемлемые для пользователей параметры работы сети в условиях нормальной обычной работы (базовые параметры)
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Использовать современные методы контроля производительности инфокоммуникационных систем
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Кабельные и сетевые анализаторы
	Метрики производительности
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель взаимодействия открытых систем (модель OSI/ISO)
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения

	Инструкции по эксплуатации администрируемого программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.4.3. Трудовая функция

Наименование	Управление безопасностью сетевых устройств и программного обеспечения	Код	D/03.6	Уровень (подуровень) квалификации	6

Трудовые действия	Настройка параметров управления безопасностью операционных систем сетевых устройств
	Установка специальных средств управления безопасностью сетевых устройств администрируемой сети
	Установка средств обеспечения безопасности удаленного доступа
	Настройка средств обеспечения безопасности удаленного доступа
Необходимые умения	Определять механизм изменения и модификации базовой конфигурации
	Внедрять процесс проверки текущей конфигурации на соответствие заданным базовым параметрам (аудит конфигурации)
	Конфигурировать операционные системы
	Конфигурировать сетевые устройства
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Классификация операционных систем согласно классам безопасности
	Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Защищенные протоколы управления
	Основные средства криптографии
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Модели информационно-телекоммуникационной сети «Интернет»
	Регламенты проведения профилактических работ на администрируемой

	инфокоммуникационной системе
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	

3.4.4. Трудовая функция

Наименование	Диагностика отказов и ошибок сетевых устройств и программного обеспечения	Код	D/04.6	Уровень (подуровень) квалификации	6

Трудовые действия	Поиск отказов сетевых устройств и программного обеспечения
	Устранение отказов сетевых устройств и программного обеспечения
	Поиск ошибок сетевых устройств и программного обеспечения
	Устранение ошибок сетевых устройств и программного обеспечения
	Документирование отказов и ошибок в работе сетевых устройств и программного обеспечения
Необходимые умения	Использовать современные стандарты при настройке параметров администрируемых устройств и программного обеспечения
	Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств
	Применять программно-аппаратные средства для диагностики отказов и ошибок программного обеспечения
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Модели информационно-телекоммуникационной сети «Интернет»
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Основы делопроизводства
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.4.5. Трудовая функция

Наименование	Контроль производительности сетевой инфраструктуры инфокоммуникационной системы	Код	D/05.6	Уровень (подуровень) квалификации	6

Трудовые действия	Определение базовой производительности сетевой инфраструктуры инфокоммуникационной системы
	Контроль отклонений от номиналов производительности сетевой инфокоммуникационной системы
	Коррекция производительности сетевой инфокоммуникационной системы
	Документирование отклонений производительности сетевой инфраструктуры инфокоммуникационной системы
Необходимые умения	Использовать современные стандарты при администрировании устройств и программного обеспечения
	Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры
	Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Модели информационно-телекоммуникационной сети «Интернет»
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Основы делопроизводства
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.4.6. Трудовая функция

Наименование	Проведение регламентных работ на	Код	D/06.6	Уровень	6

сетевых устройствах и программном обеспечении инфокоммуникационной системы		(подуровень) квалификации		

Трудовые действия	Осуществление профилактических работ по поддержке сетевых устройств
	Осуществление профилактических работ по поддержке программного обеспечения
	Планирование стратегии восстановления сетевой системы и программного обеспечения инфокоммуникационной системы
Необходимые умения	Использовать современные средства администрирования баз данных
	Применять современные контрольно-измерительные средства
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Модели информационно-телекоммуникационной сети «Интернет»
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
	Нормативно-правовые акты, действующие в организации
Другие характеристики	-

3.5. Обобщенная трудовая функция

Наименование	Администрирование систем управления базами данных инфокоммуникационной системы организации	Код	E	Уровень квалификации	7

Возможные наименования должностей	Администратор баз данных Системный администратор

Требования к образованию и обучению	Высшее образование – специалитет, магистратура
Требования к опыту практической работы	-
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
	230101	Вычислительные машины, комплексы, системы и сети

3.5.1. Трудовая функция

Наименование	Инсталляция (установка) системы управления базой данных (СУБД)	Код	E/01.7	Уровень (подуровень) квалификации	7

Трудовые действия	Установка на жесткий диск сервера базы данных программного обеспечения СУБД
	Загрузка отдельных компонент СУБД на различные сервера баз данных
	Задание параметров размещения будущей базы данных и выделение под ее множества (отношения реляционной СУБД) дискового пространства
	Выбор методов доступа к данным
	Задание параметров работы ядра СУБД
	Задание работы отдельных приложений
	Резервное копирование данных
Необходимые умения	Загружать компоненты СУБД
	Работать со специальным инструментарием администратора базы данных (ассистент конфигурирования и центр управления для реализации части операций)
	Копировать данные на различные носители
Необходимые знания	Положения, инструкции по разработке и оформлению документации
	Нормативно-техническая и проектная документация
	Архитектура программных компонентов СУБД
	Особенности операционной системы
	Особенности реализации сетевой технологии в организации
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-

	аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.5.2. Трудовая функция

Наименование	Мониторинг работы СУБД	Код	E/02.7	Уровень (подуровень) квалификации	7

Трудовые действия	Запуск утилит мониторинга для контроля текущей ситуации СУБД
	Задание пороговых значений индикаторов
	Отслеживание наличия средств сбора или предоставления статистики у приложений, работающих с базами данных
	Защита баз данных от несанкционированного доступа
	Задание параметров работы ядра СУБД
	Задание работы отдельных приложений
	Протоколирование событий, возникающих в процессе работы СУБД инфокоммуникационной системы
Необходимые умения	Работать со специальным инструментарием для администратора базы данных (монитор снимков и монитор событий)
	Осуществлять самостоятельный поиск информации, необходимой для выполнения профессиональных задач
	Авторизовать пользователей баз данных
	Производить аутентификацию пользователей баз данных
	Производить аудит пользователей баз данных
Необходимые знания	Положения, инструкции по разработке и оформлению документации
	Нормативно-техническая и проектная документация
	Архитектура программных компонент СУБД
	Особенности операционной системы
	Особенности реализации сетевой технологии в организации
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.5.3. Трудовая функция

Наименование	Настройка систем резервного копирования и восстановления баз данных	Код	E/03.7	Уровень (подуровень) квалификации	7

Трудовые действия	Реорганизация баз данных на месте
	Реорганизация баз данных путем выгрузки и загрузки
	Реорганизация баз данных приращениями
	Реорганизация баз данных параллельно с эксплуатацией
	Аварийное восстановление баз данных

	Восстановление предыдущей версии данных
	Восстановление данных с повторением транзакций
Необходимые умения	Архивировать базы данных
	Определять точки восстановления данных
	Применять современные методы и способы реорганизации и восстановления данных
	Осуществлять самостоятельный поиск информации, необходимой для выполнения профессиональных задач
	Использовать современные программные средства резервирования данных
	Использовать современные программно-аппаратные средства резервирования данных
Необходимые знания	Положения, инструкции по разработке и оформлению документации по ведению баз данных
	Нормативно-техническая и проектная документация по СУБД
	Архитектура программных компонент СУБД
	Особенности администрируемой операционной системы
	Особенности реализации сетевой технологии в организации
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.6. Обобщенная трудовая функция

Наименование	Код	Уровень квалификации
Администрирование системного программного обеспечения инфокоммуникационной системы организации	F	7

Возможные наименования должностей	Ведущий специалист Ведущий системный инженер Старший системный администратор

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных и телекоммуникационных систем и средств
Требования к опыту практической работы	Не менее шести месяцев работы в области системного администрирования
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем

	2144	Инженеры-электроники, инженеры по связи и приборостроению

3.6.1. Трудовая функция

Наименование	Установка системного программного обеспечения	Код	F/01.7	Уровень (подуровень) квалификации	7

Трудовые действия	Подготовка площадки и оборудования для установки операционных систем в соответствии с руководством по эксплуатации операционной системы
	Инсталляция файл-сервера
	Инсталляция программного обеспечения рабочих станций
	Планирование структур каталогов (директорий)
	Планирование пользователей и групп пользователей
	Планирование процедур защиты информации
	Планирование процедур регистрации пользователей
	Настройка параметров операционных систем
	Создание рабочих копий дистрибутива (поставляемой производителем операционной системы копии продукта)
Необходимые умения	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Проверять условия эксплуатации и выполнение требований по электропитанию оборудования
	Использовать специальные средства при работе с оборудованием
	Готовить рабочие таблицы файл-сервера
	Вычислять размер памяти для каждого тома, общую память, память, необходимую для работы самой операционной системы
Необходимые знания	Максимальные ограничения по поддерживаемой операционной системой оперативной и дисковой памяти
	Принципы информационной безопасности инфокоммуникационной системы
	Модели доступа пользователей к инфокоммуникационной системе
	Основы администрирования операционной системы
	Основы безопасности функционирования инфокоммуникационной системы
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.6.2. Трудовая функция

Наименование	Оптимизация работы дисковой подсистемы (подсистемы ввода-вывода)	Код	F/02.7	Уровень (подуровень) квалификации	7

Трудовые действия	Инициализация дисковых адаптеров и контроллеров
	Выставление нужных адресов и прерываний
	Установка переключателей на платах
	Подсоединение шин
	Установка параметров КМОП (CMOS) компьютера
	Форматирование низкого уровня
	Организация разделов (партиций)
	Форматирование высокого уровня
Необходимые умения	Использовать специальные процедуры для повышения производительности и восстановления в случае сбоев дисковой подсистемы
	Использовать специальные программные продукты для повышения производительности и восстановления в случае сбоев дисковой подсистемы
	Конвергировать конкурирующие стандарты SATA и SCSI с помощью стандарта SAS
	Зеркалировать диски
	Пользоваться нормативно-технической документацией производителя дисковых подсистем
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Типы интерфейсов дисковых подсистем
	Устройство дисковых подсистем ввода-вывода
	Особенности работы конкретной устанавливаемой операционной системы
	Особенности дисковых контроллеров
	Типы дисков, для которых не рекомендуется низкоуровневое форматирование
	Температурные режимы, рекомендуемые при высокоуровневом форматировании
	Условия восстановления информации при высокоуровневом форматировании
	Методики применения профессиональных знаний о работе инфокоммуникационной системы
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.6.3. Трудовая функция

Наименование	Администрирование файловых систем	Код	F/03.7	Уровень (подуровень) квалификации	7

Трудовые действия	Выделение томов под каждую файловую систему в случае поддержания операционной системой нескольких файловых систем
	Монтирование томов, на которых будут располагаться файловые системы
Необходимые умения	Проверять тип файловой системы тома и ее целостности
	Считывать системные структуры данных (оглавления тома)
	Инициализировать соответствующие модули операционной системы
	Включать файловые системы в общее пространство имен
	Пользоваться нормативно-технической документацией по файловым системам
	Комбинировать имеющиеся системные средства и избегать их противоречий
Необходимые знания	Методы доступа к файловым системам
	Наборы утилит для работы с администрируемыми файловыми системами
	Методы восстановления данных
	Протоколы передачи файлов
	Рекомендации Международной организации по стандартизации (ISO) по организации директорий в гетерогенных многопользовательских системах
	Рекомендации Международного союза электросвязи (ITU-T) по организации директорий в гетерогенных многопользовательских системах
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.6.4. Трудовая функция

Наименование	Оценка критичности возникновения инцидентов для системного программного обеспечения	Код	F/04.7	Уровень (подуровень) квалификации	7

Трудовые действия	Обнаружение критических инцидентов при работе системного программного обеспечения
	Определение причин возникновения критических инцидентов при работе системного программного обеспечения
	Выполнение действий по устранению критических инцидентов при работе системного программного обеспечения в рамках должностных обязанностей
	Регистрация инцидентов при работе системного программного обеспечения
Необходимые умения	Идентифицировать инциденты при работе системного программного обеспечения
	Применять специализированные программно-аппаратные средства для

	локализации инцидентов при работе системного программного обеспечения
Необходимые знания	Правила настройки и эксплуатации устанавливаемого системного программного обеспечения, включая лицензионные требования
	Основы архитектуры, устройства и функционирования вычислительных систем
	Принципы организации, состав и схемы работы операционных систем
	Стандарты информационного взаимодействия систем
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.6.5. Трудовая функция

Наименование	Реализация регламентов обеспечения информационной безопасности системного программного обеспечения инфокоммуникационной системы организации	Код	F/05.7	Уровень (подуровень) квалификации	7

Трудовые действия	Установка аппаратно-программных средств защиты системного программного обеспечения
	Настройка аппаратно-программных средств защиты системного программного обеспечения
	Проведение регламентов обеспечения защиты информации в соответствии с политикой информационной безопасности
	Проведение регламентов обеспечения защиты информационных систем в соответствии с политикой информационной безопасности (в том числе управление правами доступа)
Необходимые умения	Выполнять настройку системного программного обеспечения в соответствии с регламентами обеспечения информационной безопасности
	Проводить авторизацию пользователей, имеющих доступ к настройке системного программного обеспечения инфокоммуникационной системы организации
	Применять программно-аппаратные средства защиты информации
	Применять программные средства защиты информации
Необходимые знания	Основы обеспечения информационной безопасности
	Нормативно-правовые акты в области информационной безопасности
	Инструкции по настройке устанавливаемого системного программного обеспечения, включая знания о типовых уязвимостях
	Инструкции по эксплуатации устанавливаемого системного программного обеспечения, включая знания о типовых уязвимостях
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Регламенты обеспечения информационной безопасности

	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.7. Обобщенная трудовая функция

Наименование	Управление развитием инфокоммуникационной системы организации	Код	G	Уровень квалификации	7

Возможные наименования должностей	Ведущий системный администратор Главный системный администратор

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных и телекоммуникационных систем и средств
Требования к опыту практической работы	Не менее шести месяцев работы в области системного администрирования
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению

3.7.1. Трудовая функция

Наименование	Анализ системных проблем обработки информации на уровне инфокоммуникационной системы	Код	G/01.7	Уровень (подуровень) квалификации	7

Трудовые действия	Анализ динамики изменения показателей качества работы инфокоммуникационной системы и/или ее составляющих
	Разработка предложений по модернизации аппаратных, программно-аппаратных и программных технических средств
	Анализ качества выполнения работ на соответствие инструкциям по эксплуатации аппаратных, программно-аппаратных и программных технических средств
	Составление анкет для выявления требований и пожеланий по выявлению системных проблем обработки информации

	Анализ выявленных требований и пожеланий по выявлению системных проблем обработки информации
Необходимые умения	Собирать данные для анализа показателей качества функционирования аппаратных, программно-аппаратных и программных технических средств инфокоммуникационной системы
	Рассчитывать показатели использования и функционирования аппаратных, программно-аппаратных и программных технических средств
	Выявлять особенности новой продукции и правильно позиционировать ее на рынке
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Работать с информацией в условиях неопределенности, избыточности и недостаточности исходных данных
Необходимые знания	Принципы организации современных инфокоммуникационных систем
	Принципы функционирования инфокоммуникационных систем
	Продукция мировых и отечественных производителей телекоммуникационного оборудования различных типов
	Состояние и перспективы развития информационных и инфокоммуникационных технологий
	Основные теории и концепции в области инноваций и инновационного менеджмента
	Основные теории и концепции стратегического планирования
Другие характеристики	-

3.7.2. Трудовая функция

Наименование	Подготовка предложений по развитию инфокоммуникационной системы	Код	G/02.7	Уровень (подуровень) квалификации	7

Трудовые действия	Отслеживание отечественных и зарубежных разработок в области информационных и коммуникационных технологий
	Разработка предложений по модернизации аппаратных, программно-аппаратных и программных средств инфокоммуникационной системы
	Подготовка аналитических отчетов по обзору новых аппаратных, программно-аппаратных и программных решений
Необходимые умения	Обосновывать предложения по реализации стратегии в области инфокоммуникационных технологий
	Использовать программные комплексы для обработки статистической информации
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Документировать отчеты и предложения по развитию инфокоммуникационной системы
	Работать с информацией в условиях неопределенности, избыточности и недостаточности информации
	Привлекать экспертов по смежным и профильным областям
Необходимые знания	Принципы организации инфокоммуникационных систем
	Принципы функционирования инфокоммуникационных систем

	Основы технического нормирования
	Основы менеджмента
	Основы маркетинга
	Основы делопроизводства
	Способы, формы и методы коммерциализации продукции
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Структура и планы развития организации
Другие характеристики	-

3.7.3. Трудовая функция

Наименование	Разработка нормативной и технической документации на аппаратные средства и программное обеспечение	Код	G/03.7	Уровень (подуровень) квалификации	7

Трудовые действия	Изучение нормативной и технической документации на аппаратные средства и программное обеспечение, использующие новые инфокоммуникационные технологии
	Освоение аппаратных средств и программного обеспечения, использующих новые инфокоммуникационные технологии
	Внедрение в практику администрирования новых инфокоммуникационных технологий
	Подготовка рекомендаций по эксплуатации аппаратных средств и программного обеспечения, использующих новые инфокоммуникационные технологии
	Подготовка руководства пользователя аппаратных средств и программного обеспечения, использующих новые инфокоммуникационные технологии
Необходимые умения	Применять отраслевую нормативную документацию на аппаратные средства и программное обеспечение
	Применять отраслевую нормативную документацию на программное обеспечение
	Оформлять техническую документацию на аппаратные средства
	Оформлять техническую документацию на программное обеспечение
	Использовать при оформлении руководства пользователя понятные технические термины
	Использовать при оформлении руководства пользователя понятные графические пояснения
Необходимые знания	Состояние и перспективы развития информационных и коммуникационных технологий
	Рынок программно-аппаратных средств
	Стратегия развития организации
	Продукция мировых и отечественных производителей телекоммуникационного и компьютерного оборудования различных типов
	Основные технические характеристики, преимущества и недостатки

	инфокоммуникационных систем и/или их составляющих отечественных и зарубежных производителей
	Перспективы и основные тенденции развития инфокоммуникационной отрасли
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Технические регламенты по эксплуатации администрируемых аппаратных средств
	Технические регламенты по эксплуатации администрируемого программного обеспечения
	Основы делопроизводства
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

3.7.4. Трудовая функция

Наименование	Контроль обновления версий аппаратных, программно-аппаратных и программных средств	Код	G/04.7	Уровень (подуровень) квалификации	7

Трудовые действия	Сравнение обновленной и предыдущей версии программного обеспечения
	Проверка совместимости обновленных версий аппаратных, программно-аппаратных и программных средств
	Обновление программного обеспечения
	Корректировка действий при обнаружении ошибок обновления
Необходимые умения	Пользоваться нормативно-технической документацией на администрируемое программное обеспечение
	Анализировать технические параметры различных версий аппаратных средств
	Анализировать технические параметры различных версий программно-аппаратных средств
	Анализировать технические параметры различных версий программных средств
Необходимые знания	Рынок программных и аппаратных средств
	Состояние и перспективы развития информационных и коммуникационных технологий
	Техническая документация на администрируемые аппаратные, программно-аппаратные и программные средства
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы
Другие характеристики	-

Приложение 2. Типовые требования к виду профессиональной деятельности «Специалист по администрированию сетевых усройств информационно-коммуникационных систем»

I. Общие сведения

Администрирование сетевых устройств информационно-коммуникационной (инфокоммуникационной) системы

(наименование вида профессиональной деятельности)

Основная цель вида профессиональной деятельности:

Обеспечение требуемого режима работы сетевых устройств, входящих в состав инфокоммуникационной системы

Группа занятий:

2131	Разработчики и аналитики компьютерных систем	3132	Техники и операторы аппаратуры для радио-, телевещания и телесвязи
2144	Инженеры-электроники, инженеры по связи и приборостроению	7522	Профессии рабочих по обслуживанию и ремонту линейных сооружений и станционного оборудования связи
3122	Техники и операторы по обслуживанию компьютерных устройств	-	-
(код ОКЗ)	(наименование)	(код ОКЗ)	(наименование)

Отнесение к видам экономической деятельности:

64.20.7	Прочая деятельность в области электросвязи
72.60	Прочая деятельность, связанная с использованием вычислительной техники и информационных технологий
(код ОКВЭД)	(наименование вида экономической деятельности)

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида трудовой деятельности)

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Администрирование процесса установки сетевых устройств инфокоммуникационных систем	4	Установка активных сетевых устройств	A/01.4	4
			Настройка программного обеспечения сетевых устройств	A/02.4	4
			Установка специальных средств управления сетевыми устройствами	A/03.4	4
B	Администрирование процесса конфигурирования сетевых устройств и программного обеспечения	5	Настройка параметров сетевых устройств и программного обеспечения согласно технологической политике организации	B/01.5	5
			Инвентаризация параметров и функциональных схем работы сетевых устройств администрируемой сети	B/02.5	5
			Оценка эффективности конфигурации сетевых устройств с точки зрения производительности сети и защиты от несанкционированного доступа	B/03.5	5
C	Администрирование процесса контроля производительности сетевых устройств и программного обеспечения	6	Оценка производительности сетевых устройств и программного обеспечения	C/01.6	6
			Контроль использования сетевых устройств и программного обеспечения	C/02.6	6
			Управление средствами тарификации сетевых ресурсов	C/03.6	6
			Коррекция производительности сетевой инфокоммуникационной системы	C/04.6	6
D	Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	6	Определение параметров безопасности и защиты программного обеспечения сетевых устройств	D/01.6	6
			Установка специальных средств управления безопасностью администрируемой сети	D/02.6	6
			Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	D/03.6	6

E	Проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	6	Осуществление регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы	E/01.6	6
			Планирование восстановления сетевой инфокоммуникационной системы	E/02.6	6
			Восстановление параметров программного обеспечения сетевых устройств	E/03.6	6
			Планирование модернизации сетевых устройств	E/04.6	6
F	Администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения	7	Устранение сбоев и отказов сетевых устройств и операционных систем	F/01.7	7
			Документирование ошибок в работе сетевых устройств и программного обеспечения	F/02.7	7
			Устранение ошибок сетевых устройств и операционных систем	F/03.7	7

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

Наименование	Администрирование процесса установки сетевых устройств инфокоммуникационных систем	Код	A	Уровень квалификации	4

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Младший сетевой администратор Младший специалист по администрированию сетевых устройств

Требования к образованию и обучению	Среднее профессиональное образование – программы подготовки квалифицированных рабочих (служащих)
Требования к опыту практической работы	Не менее трех месяцев работы в области технической поддержки, администрирования, программирования устройств инфокоммуникационных систем
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	7522	Профессии рабочих по обслуживанию и ремонту линейных сооружений и станционного оборудования связи
ЕКС	-	-
ОКПДТР	19827	Электромонтер линейных сооружений телефонной связи и радиофикации
	19859	Электромонтер по ремонту и монтажу кабельных линий
ОКСО	-	-

3.1.1. Трудовая функция

Наименование	Установка активных сетевых устройств	Код	A/01.4	Уровень (подуровень) квалификации	4

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального

	стандарта
Трудовые действия	Установка сетевых устройств (концентраторов, мостов, маршрутизаторов, шлюзов, модемов, мультиплексоров, конвертеров, коммутаторов)
	Подключение сетевых устройств (концентраторов, мостов, маршрутизаторов, шлюзов, модемов, мультиплексоров, конвертеров, коммутаторов)
	Проверка работоспособности администрируемых сетевых устройств
	Протоколирование событий, возникающих в процессе установки администрируемых сетевых устройств
	Документирование первоначальных и измененных параметров установки администрируемых сетевых устройств
Необходимые умения	Применять различные методы управления сетевыми устройствами
	Применять методы задания базовых параметров и параметров защиты от несанкционированного доступа к операционным системам
	Использовать методы статической и динамической конфигурации параметров операционных систем
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Принципы функционирования сетевых аппаратных средств
	Архитектуры сетевых аппаратных средств
	Принципы работы операционных систем
	Архитектура операционных систем
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Протоколы управления сетевых систем
	Техническая документация по операционной системе конфигурируемого сетевого устройства
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.1.2. Трудовая функция

Наименование	Настройка программного обеспечения сетевых устройств	Код	A/02.4	Уровень (подуровень) квалификации	4

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Подключение средств управления сетевыми устройствами
	Инсталляция сетевого программного обеспечения
	Конфигурирование базовых параметров операционных систем сетевых устройств и сетевых интерфейсов
	Проверка правильности установки базовой конфигурации сетевых устройств и программного обеспечения в соответствии с руководством инженера
	Конфигурирование протоколов сетевого, канального и транспортного уровня
	Проверка функционирования сетевых устройств после установки и настройки программного обеспечения
	Документирование базовой конфигурации сетевых устройств и программного обеспечения для последующего контроля непротиворечивости, целостности, проверяемости и повторяемости конфигурации сетевых устройств и программного обеспечения в ходе эксплуатации
Необходимые умения	Применять специальные процедуры управления сетевыми устройствами
	Параметризировать протоколы канального, сетевого и транспортного уровня модели взаимодействия открытых систем
	Применять средства контроля и оценки конфигураций операционных систем
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Принципы функционирования вычислительной техники
	Принципы работы операционных систем
	Инструкции по установке администрируемых аппаратных сетевых устройств
	Инструкции по эксплуатации администрируемых аппаратных сетевых устройств
	Модель взаимодействия открытых систем (модель OSI/ISO)
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.1.3. Трудовая функция

Наименование	Установка специальных средств управления сетевыми устройствами	Код	A/03.4	Уровень (подуровень) квалификации	4

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Инсталляция специального программного обеспечения для учета конфигураций, слежения за производительностью сетевых устройств и защиты их от несанкционированного доступа
	Настройка базовых параметров специального программного обеспечения для учета конфигураций, слежения за производительностью сетевых устройств и защиты их от несанкционированного доступа
	Документирование базовых параметров специального программного обеспечения для учета конфигураций, слежения за производительностью сетевых устройств и защиты их от несанкционированного доступа
	Обновление специального программного обеспечения для учета конфигураций, слежения за производительностью сетевых устройств и защиты их от несанкционированного доступа
Необходимые умения	Применять специальные процедуры установки средств управления сетью
	Настраивать специальные средства управления сетевыми устройствами
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Принципы функционирования аппаратных средств
	Архитектуры аппаратных средств
	Принципы работы операционных систем
	Протоколы управления и типы протоколов маршрутизации
	Модель взаимодействия открытых систем (модель OSI/ISO)
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Инструкции по установке операционных систем
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации операционных систем
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемого программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.2. Обобщенная трудовая функция

Наименование	Администрирование процесса конфигурирования сетевых устройств и программного обеспечения	Код	B	Уровень квалификации	5

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Специалист по сетевому администрированию Специалист по администрированию сетевых устройств

Требования к образованию и обучению	Среднее профессиональное образование – программы подготовки специалистов среднего звена, программы подготовки квалифицированных рабочих (служащих) Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее шести месяцев работы по администрированию процесса установки сетевых элементов
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	3122	Техники и операторы по обслуживанию компьютерных устройств
	3132	Техники и операторы аппаратуры для радио-, телевещания и телесвязи
ЕКС	-	-
ОКПДТР	27099	Техник-программист
ОКСО	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.2.1. Трудовая функция

Наименование	Код	Уровень (подуровень) квалификации
Настройка параметров сетевых устройств и программного обеспечения согласно технологической политике организации	B/01.5	5

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Создание стандарта задания параметров для каждого вида администрируемых коммуникационных устройств сети
	Создание стандарта задания параметров для каждого вида

	администрируемых серверов
	Создание стандарта задания параметров для каждого вида администрируемых операционных систем, применяемых на администрируемой сети
	Согласование технологических стандартов организации, которой принадлежит конфигурируемая сеть
	Загрузка (вручную или автоматически) в базу данных управляющей системы соответствующих параметров (стандартизированных и соответствующих технологической политике организации)
	Выгрузка (вручную или автоматически) из базы данных управляющей системы соответствующих параметров (стандартизированных и соответствующих технологической политике организации)
	Конфигурирование параметров администрируемых сетевых устройств и программного обеспечения согласно утвержденных технологических стандартов организации
	Документирование параметров администрируемых сетевых устройств и программного обеспечения согласно утвержденных технологических стандартов организации
Необходимые умения	Использовать отраслевые стандарты при настройке параметров администрируемых сетевых устройств и программного обеспечения
	Учитывать и отражать в конфигурации сетевых устройств технологические стандарты организации
	Учитывать и отражать в конфигурации сетевых устройств стандарты безопасности
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Способы коммуникации процессов операционных систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Основы делопроизводства
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.2.2. Трудовая функция

Наименование	Инвентаризация параметров и функциональных схем работы сетевых устройств администрируемой сети	Код	B/02.5	Уровень (подуровень) квалификации	5

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Проверка всех версий установленных компонентов администрируемой сети
	Подготовка графического представления о взаимодействии всех аппаратных и программных компонентов администрируемой сети
	Проведение аудита работы всех сетевых протоколов
	Фиксирование в журнале инвентарных номеров технических средств администрируемой сети
	Фиксирование в журнале месторасположения технических средств администрируемой сети
	Маркировка технических средств администрируемой сети
	Подготовка расписания проведения регламентных работ на администрируемой сети
Необходимые умения	Применять системы управления сетью
	Выполнять настройку протоколов управления операционных систем сетевых устройств
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Программные средства инвентаризации
	Правила техники безопасности при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.2.3. Трудовая функция

Наименование	Оценка эффективности конфигурации сетевых устройств с точки зрения производительности сети и защиты от несанкционированного доступа	Код	B/03.5	Уровень (подуровень) квалификации	5

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Применение метрики «минимальное время восстановления» при создании стратегии архивирования параметров и конфигурации администрируемой сети
	Анализ производительности администрируемой сети с применением специализированного оборудования и программного обеспечения
	Создание профайла (списков) параметров организации, влияющих на защиту от несанкционированного доступа
	Проверка правильности используемой политики безопасности
	Подготовка отчетов для анализа слабых мест в конфигурации системы безопасности
	Централизованное сохранение всех идентификаторов и паролей пользователей, сведений о разрешенных сотрудникам правах доступа к различным компонентам администрируемой сети
Необходимые умения	Применять специальные процедуры по управлению правами доступа пользователей
	Работать с официальными сайтами организаций – разработчиков компонентов администрируемой сети
	Работать с официальными рассылками изменений к компонентам администрируемой сети
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой

	инфокоммуникационной системе
	Федеральные и отраслевые требования по защите сети от несанкционированного доступа
	Технологические требования организации, которой принадлежит администрируемая сеть, по защите сети от несанкционированного доступа
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.3. Обобщенная трудовая функция

Наименование	Администрирование процесса контроля производительности сетевых устройств и программного обеспечения	Код	C	Уровень квалификации	6

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Сетевой администратор Специалист по сетевому администрированию Специалист по администрированию сетевых устройств

Требования к образованию и обучению	Высшее образование – бакалавриат или Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее шести месяцев работы по администрированию сетевых элементов при среднем профессиональном образовании
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
	3122	Техники и операторы по обслуживанию компьютерных устройств
	3132	Техники и операторы аппаратуры для радио-, телевещания и телесвязи
ЕКС	-	-

ОКПДТР	27099	Техник-программист
	22824	Инженер-программист
	22870	Инженер электросвязи
ОКСО	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.3.1. Трудовая функция

Наименование	Оценка производительности сетевых устройств и программного обеспечения	Код	C/01.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Оценка производительности критических приложений, наиболее влияющих на производительность сетевых устройств и программного обеспечения в целом
	Планирование требуемой производительности администрируемой сети
	Ведение специального документа «Оценка готовности системы»
Необходимые умения	Выяснять приемлемые для пользователей параметры работы сети в условиях нормальной обычной работы (базовые параметры)
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Использовать современные методы контроля производительности инфокоммуникационных систем
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Кабельные и сетевые анализаторы
	Средства глубокого анализа сети
	Метрики производительности администрируемой сети
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель взаимодействия открытых систем (модель OSI/ISO)
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.3.2. Трудовая функция

Наименование	Контроль использования сетевых устройств и программного обеспечения	Код	C/02.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Установка кабельных и сетевых анализаторов для контроля изменения номиналов сетевых устройств и программного обеспечения администрируемой сети в целом и отдельных подсистем инфокоммуникационной системы
	Применение утилит операционных систем для контроля изменения номиналов сетевых устройств и программного обеспечения администрируемой сети в целом и отдельных подсистем инфокоммуникационной системы
	Контроль изменения номиналов устройств и программного обеспечения администрируемой сети в целом и отдельных подсистем инфокоммуникационной системы
	Анализ параметров производительности администрируемой сети за установленный период (сутки, неделя, месяц, квартал, год)
	Сравнение параметров производительности администрируемой сети за установленный период (сутки, неделя, месяц, квартал, год)
	Создание отчетов о производительности администрируемой сети
Необходимые умения	Работать с контрольно-измерительными аппаратными и программными средствами
	Использовать современные измерительные приборы и программное обеспечение
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Анализировать корреляции различных параметров при изменениях производительности
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике

	(IEEE)
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.3.3. Трудовая функция

Наименование	Управление средствами тарификации сетевых ресурсов	Код	C/03.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Использование утилит операционных систем для тарификации сетевых ресурсов
	Установка дополнительных программных продуктов для тарификации сетевых ресурсов
	Параметризация дополнительных программных продуктов для тарификации сетевых ресурсов
Необходимые умения	Конфигурировать операционные системы сетевых устройств администрируемой сети
	Работать с контрольно-измерительными аппаратными и программными средствами
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Отчеты управляющей системы
	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.3.4. Трудовая функция

Наименование	Коррекция производительности сетевой инфокоммуникационной системы	Код	C/04.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Возврат базовых параметров производительности сетевых устройств инфокоммуникационной системы к номинальным значениям
	Добавление новых интерфейсов сетевых устройств
	Добавление каналов ввода-вывода серверов (в зависимости от возможностей операционной системы)
	Изменение конфигурации сетевых устройств
	Изменение путей прохождения трафика с обходом узких мест сетевой инфокоммуникационной системы
	Изменение параметров загрузки операционной системы и системы управления базой данных
	Изменение методов доступа к данным
	Полная модификация части администрируемой сети с изменением ее архитектуры
Необходимые умения	Использовать современные средства контроля производительности администрируемой сети
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Работать с контрольно-измерительными аппаратными и программными средствами
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой

	инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.4. Обобщенная трудовая функция

Наименование	Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	Код	D	Уровень квалификации	6

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Сетевой инженер Сетевой администратор Специалист по администрированию сетевых устройств

Требования к образованию и обучению	Высшее образование – бакалавриат или Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее шести месяцев по администрированию сетевых элементов при среднем профессиональном образовании
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
	3122	Техники и операторы по обслуживанию компьютерных устройств
	3132	Техники и операторы аппаратуры для радио-, телевещания и телесвязи
ЕКС	-	-
ОКПДТР	27099	Техник-программист
	27032	Техник по защите информации
	22567	Инженер по защите информации
	22824	Инженер-программист
	22870	Инженер электросвязи

	26579	Специалист по защите информации
ОКСО	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.4.1. Трудовая функция

Наименование	Определение параметров безопасности и защиты программного обеспечения сетевых устройств	Код	D/01.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Планирование защиты приложений от несанкционированного доступа
	Оценка безопасности и защиты приложений от несанкционированного доступа
	Планирование защиты операционных систем от несанкционированного доступа
	Оценка защиты операционных систем от несанкционированного доступа
Необходимые умения	Выяснять приемлемые для пользователей параметры работы сети в условиях нормальной обычной работы (базовые параметры)
	Применять аппаратные средства защиты сетевых устройств от несанкционированного доступа
	Применять программные средства защиты сетевых устройств от несанкционированного доступа
	Применять программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Классификация операционных систем согласно классам безопасности
	Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком

	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Защищенные протоколы управления
	Основные средства криптографии
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.4.2. Трудовая функция

Наименование	Установка специальных средств управления безопасностью администрируемой сети	Код	D/02.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Параметризация операционных систем дополнительных средств защиты администрируемой сети от несанкционированного доступа
	Установка специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа
	Установка межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети
Необходимые умения	Настраивать параметры современных программно-аппаратных межсетевых экранов
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Сегментировать элементы администрируемой сети
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой

	инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.4.3. Трудовая функция

Наименование	Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	Код	D/03.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Параметризация операционных систем средств удаленного доступа
	Установка дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация
	Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов)
	Документирование настроек средств обеспечения безопасности удаленного
Необходимые умения	Подключать и настраивать современные межсетевые экраны
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Работать с контрольно-измерительными аппаратными и программными средствами
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Защищенные протоколы управления
	Основные средства криптографии
	Регламенты проведения профилактических работ на администрируемой

	инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.5. Обобщенная трудовая функция

Наименование	Проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы	Код	E	Уровень квалификации	6

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Сетевой инженер Сетевой администратор Специалист по администрированию сетевых устройств

Требования к образованию и обучению	Высшее образование – бакалавриат или Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее шести месяцев работы по администрированию сетевых элементов при среднем профессиональном образовании
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
	3122	Техники и операторы по обслуживанию компьютерных устройств
	3132	Техники и операторы аппаратуры для радио-, телевещания и телесвязи
ЕКС	-	-
ОКПДТР	27099	Техник-программист
	22824	Инженер-программист
	22870	Инженер электросвязи

ОКСО	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.5.1. Трудовая функция

Наименование	Осуществление регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы	Код	E/01.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Инвентаризация оборудования и параметров операционных систем сетевых устройств
	Проведение регламентных работ по защите от статического электричества
	Планирование расписания архивирования и архивирование параметров операционных систем сетевых устройств
	Перезагрузка операционных систем сетевых устройств
	Проведение регламентного обслуживания оборудования в соответствии с рекомендациями производителя
Необходимые умения	Инсталлировать операционные системы сетевых устройств
	Осуществлять мониторинг администрируемых сетевых устройств
	Составлять расписание резервного копирования операционных систем сетевых устройств
	Разбирать и собирать администрируемые сетевые устройства
	Использовать современные средства контроля производительности администрируемой сети
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)

	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.5.2. Трудовая функция

Наименование	Планирование восстановления сетевой инфокоммуникационной системы	Код	E/02.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Установка серверов архивирования программного обеспечения сетевой инфокоммуникационной системы
	Параметризация серверов архивирования программного обеспечения сетевой инфокоммуникационной системы
	Формирование комплекта запасных частей и приборов сетевого оборудования
	Планирование расписаний копирования программного обеспечения сетевой инфокоммуникационной системы
Необходимые умения	Использовать современные стандарты параметризации программного обеспечения сетевой инфокоммуникационной системы
	Комплектовать составные элементы сетевого оборудования
	Составлять регламенты резервного копирования программного обеспечения сетевой инфокоммуникационной системы
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе

	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.5.3. Трудовая функция

Наименование	Восстановление параметров программного обеспечения сетевых устройств	Код	E/03.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Восстановление параметров по умолчанию согласно документации операционных систем
	Восстановление параметров при помощи серверов архивирования
	Восстановление параметров при помощи средств управления специализированных операционных систем сетевого оборудования
Необходимые умения	Использовать типовые процедуры восстановления данных
	Определять точки восстановления данных
	Работать с серверами архивирования и средствами управления операционных систем
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.5.4. Трудовая функция

Наименование	Планирование модернизации сетевых устройств	Код	E/04.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Сбор потребностей пользователей сетевой системы
	Анализ потребностей пользователей сетевой системы
	Прогнозирование сроков модернизации сетевых устройств
	Разработка краткосрочных и долгосрочных планов модернизации сети
	Планирование работ по развертыванию, конфигурированию и эксплуатации сетевых устройств
Необходимые умения	Составлять график модернизации программно-аппаратных средств
	Работать с информацией организаций – производителей администрируемых сетевых устройств и программного обеспечения
	Применять новые инфокоммуникационные технологии
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
	Следить за новыми инфокоммуникационными технологиями
	Обосновывать предложения по реализации стратегии в области инфокоммуникационных технологий
	Получать информацию о новых сетевых стандартах
	Обновлять информацию о новых сетевых стандартах
Необходимые знания	Принципы функционирования сетевых аппаратных средств
	Архитектуры сетевых аппаратных средств
	Стратегия развития организации
	Состояние и перспективы развития информационных и коммуникационных технологий
	Рекомендации производителей и экспертов
	Технологии в сетевом администрировании
	Принципы работы сетевых элементов
	Модель взаимодействия открытых систем (модель OSI/ISO)
	Протоколы всех уровней модели взаимодействия открытых систем
	Модели управления сетью
	Модель открытых сетевых вычислений
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети

Другие характеристики	-

3.6. Обобщенная трудовая функция

Наименование	Администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения	Код	F	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Сетевой администратор Сетевой аналитик Специалист по сетевому администрированию Специалист по администрированию сетевых устройств

Требования к образованию и обучению	Высшее образование – специалитет, магистратура
Требования к опыту практической работы	-
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
ЕКС	-	-
ОКПДТР	27099	Техник-программист
	22824	Инженер-программист
	22870	Инженер электросвязи
ОКСО	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.6.1. Трудовая функция

Наименование	Устранение сбоев и отказов сетевых устройств и операционных систем	Код	F/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Выявление сбоев и отказов сетевых устройств и операционных систем
	Определение сбоев и отказов сетевых устройств и операционных систем
	Устранение последствий сбоев и отказов сетевых устройств и операционных систем
	Сопоставление аварийной информации от различных устройств сети
	Локализация отказов в сетевых устройствах и операционных системах
	Инициирование корректирующих действий
	Регистрация сообщений об ошибках в сетевых устройствах и операционных системах
	Фильтрация сообщений об ошибках в сетевых устройствах и операционных системах
	Маршрутизация сообщений об ошибках в сетевых устройствах и операционных системах
	Контроль ежедневных отчетов от систем мониторинга
Необходимые умения	Анализировать сообщения об ошибках в сетевых устройствах и операционных системах
	Локализовать отказ и инициировать корректирующие действия
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.6.2. Трудовая функция

Наименование	Документирование ошибок в работе сетевых устройств и программного обеспечения	Код	F/02.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код	Регистрационный

			оригинала	номер профессионального стандарта

Трудовые действия	Проверка целостности программного обеспечения
	Установка средств защиты сетевых устройств и программного обеспечения
	Проведение испытаний установленных сетевых устройств и программного обеспечения
	Проверка на совместимость существующего и устанавливаемого программного обеспечения
	Фиксация в журнале изменений в конфигурации сетевых устройств и программного обеспечения
Необходимые умения	Документировать изменения в конфигурации администрируемого программного обеспечения
	Устанавливать и инициализировать новое программное обеспечение
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Основы делопроизводства
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

3.6.3. Трудовая функция

Наименование	Устранение ошибок сетевых устройств и операционных систем	Код	F/03.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Контроль системы сбора и передачи учетной информации
	Проведение работ по исправлению ошибок конфигурации сетевых устройств и операционных систем
	Проведение работ по замене сетевых устройств или их компонентов для устранения ошибок работы
	Составление отчетов об использовании сетевых ресурсов и операционных системах
Необходимые умения	Производить мониторинг администрируемой сети
	Конфигурировать операционные системы сетевых устройств
	Пользоваться контрольно-измерительными приборами и аппаратурой
	Документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику
	Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
Необходимые знания	Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
	Архитектуры аппаратных, программных и программно-аппаратных средств администрируемой сети
	Инструкции по установке администрируемых сетевых устройств
	Инструкции по эксплуатации администрируемых сетевых устройств
	Инструкции по установке администрируемого программного обеспечения
	Инструкции по эксплуатации администрируемого программного обеспечения
	Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
	Модель Международной организации по стандартизации (ISO) для управления сетевым трафиком
	Модели Института инженеров по электротехнике и радиоэлектронике (IEEE)
	Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
	Требования охраны труда при работе с сетевой аппаратурой администрируемой сети
Другие характеристики	-

Приложение 3. Типовые требования к виду профессиональной деятельности «Системный программист»

I. Общие сведения

Создание системного программного обеспечения
(наименование вида профессиональной деятельности)

Основная цель вида профессиональной деятельности:

Разработка, отладка, модификация и поддержка системного программного обеспечения

Группа занятий:

2131	Разработчики и аналитики компьютерных систем	2132	Программисты
(код ОКЗ)	(наименование)	(код ОКЗ)	(наименование)

Отнесение к видам экономической деятельности:

72.21	Разработка программного обеспечения
72.22	Прочая деятельность по разработке программного обеспечения и консультированию в этой области
72.30	Обработка данных
(код ОКВЭД)	(наименование вида экономической деятельности)

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида трудовой деятельности)

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Разработка компонентов системных программных продуктов	6	Разработка драйверов устройств	A/01.6	6
			Разработка компиляторов, загрузчиков, сборщиков	A/02.6	6
			Разработка системных утилит	A/03.6	6
			Создание инструментальных средств программирования	A/04.6	6
B	Разработка систем управления базами данных	7	Разработка компонентов системы управления базами данных	B/01.7	7
			Отладка разрабатываемой системы управления базами данных	B/02.7	7
			Документирование разработанной системы управления базами данных в целом и ее компонентов	B/03.7	7
			Сопровождение созданной системы управления базами данных	B/04.7	7
C	Разработка операционных систем	7	Формирование требований к операционной системе	C/01.7	7
			Разработка архитектуры операционной системы	C/02.7	7
			Написание компонентов операционной системы	C/03.7	7
			Контроль соблюдения архитектуры в процессе написания операционной системы	C/04.7	7
			Отладка разрабатываемых компонентов операционной системы	C/05.7	7
			Документирование разрабатываемой операционной системы	C/06.7	7
			Сопровождение созданной операционной	C/07.7	7

			системы		
D	Организация разработки системного программного обеспечения	7	Планирование разработки системного программного обеспечения	D/01.7	7
			Формирование группы программистов для разработки системного программного обеспечения	D/02.7	7
			Организация работы программистов в группе по разработке системного программного обеспечения	D/03.7	7
			Контроль деятельности рабочей группы программистов по разработке системного программного обеспечения	D/04.7	7
			Предоставление заказчику результатов разработки системного программного обеспечения	D /05.7	7
E	Интеграция разработанного системного программного обеспечения	7	Планирование интеграции разработанного системного программного обеспечения	E/01.7	7
			Внедрение разработанного системного программного обеспечения	E/02.7	7

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

Наименование	Разработка компонентов системных программных продуктов	Код	A	Уровень квалификации	6

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Разработчик системного программного обеспечения Системный программист

Требования к образованию и обучению	Высшее образование – бакалавриат Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных технологий и программного обеспечения
Требования к опыту практической работы	Не менее одного года работы в области программирования
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2132	Программисты
ЕКС	-	-
ОКПДТР	22824	Инженер-программист
	25857	Программист
ОКСО	230105	Программное обеспечение вычислительной техники и автоматизированных систем
	230201	Информационные системы и технологии

3.1.1. Трудовая функция

Наименование	Разработка драйверов устройств	Код	A/01.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального

стандарта

Трудовые действия	Получение технической документации устройства, для которого разрабатывается драйвер
	Изучение технической документации устройства, для которого разрабатывается драйвер
	Разработка блок-схемы драйвера устройства
	Написание исходного кода драйвера устройства
	Отладка разработанного драйвера устройства
	Разработка эксплуатационной документации на разработанный драйвер
	Сопровождение разработанного драйвера устройства
	Реинжиниринг разработанного драйвера устройства
Необходимые умения	Применять языки программирования, определенные в техническом задании на разработку драйвера, для написания программного кода
	Создавать блок-схемы алгоритмов функционирования разрабатываемых программных продуктов
	Оценивать вычислительную сложность алгоритмов функционирования разрабатываемых программных продуктов
	Работать со стандартными контроллерами устройств (графическим адаптером, клавиатурой, мышью, сетевым адаптером)
	Работать с документацией, прилагаемой разработчиком устройства
	Осуществлять отладку драйверов устройств для операционной системы
Необходимые знания	Архитектура аппаратной платформы, для которой разрабатывается драйвер
	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Стандарты реализации интерфейсов подключаемых устройств
	Технологии разработки драйверов
	Системы прерываний и адресации памяти операционной системы
	Технологии разработки и отладки системных продуктов
	Комплекты средств разработки целевой операционной системы
	Система команд микропроцессора целевой аппаратной платформы
	Принципы кроссплатформенного программирования
	Конструкции распределенного и параллельного программирования
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Методы организации файловых систем
	Принципы построения сетевого взаимодействия
	Архитектура и принципы функционирования коммуникационного оборудования
	Стандарты информационного взаимодействия систем
	Методики тестирования разрабатываемого программного обеспечения
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Государственные стандарты Единой системы программной документации (ЕСПД)
Другие характеристики	-

3.1.2. Трудовая функция

Наименование	Разработка компиляторов, загрузчиков, сборщиков	Код	A/02.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Получение технической документации по языку программирования, системе команд процессора устройства, адресации памяти и регистров процессора устройства
	Изучение технической документации по языку программирования, системе команд процессора устройства, адресации памяти и регистров процессора устройства
	Разработка блок-схемы компиляторов, загрузчиков, сборщиков
	Написание исходного кода компиляторов, загрузчиков, сборщиков
	Отладка компиляторов, загрузчиков, сборщиков
	Разработка эксплуатационной документации для разработанных компиляторов, загрузчиков, сборщиков
	Сопровождение разработанных компиляторов, загрузчиков, сборщиков
	Реинжиниринг разработанных компиляторов, загрузчиков, сборщиков
Необходимые умения	Применять языки целевой аппаратной платформы, определенной в техническом задании на разработку, для написания программного кода
	Применять технологию разработки компиляторов
	Создавать блок-схемы алгоритмов функционирования разрабатываемых программных продуктов
	Оценивать вычислительную сложность алгоритма функционирования разрабатываемых программных продуктов
	Осуществлять отладку программных продуктов для целевой операционной системы
Необходимые знания	Архитектура целевой аппаратной платформы, для которой разрабатывается программное обеспечение
	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Системы команд процессора целевой аппаратуры
	Способы адресации памяти целевой аппаратной платформы
	Технологии разработки компиляторов
	Конструкции распределенного и параллельного программирования
	Методы и основные этапы трансляции
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Стандарты информационного взаимодействия систем
	Методики тестирования разрабатываемого программного обеспечения
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД

Другие характеристики	-

3.1.3. Трудовая функция

Наименование	Разработка системных утилит	Код	A/03.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Получение технической документации по целевой операционной системе
	Изучение технической документации по целевой операционной системе
	Получение технической документации по целевому аппаратному средству
	Изучение технической документации по целевому аппаратному средству
	Разработка блок-схемы утилиты
	Написание исходного кода утилиты
	Отладка разработанной утилиты
	Разработка эксплуатационной документации
	Сопровождение разработанной утилиты
	Реинжиниринг кода утилиты
Необходимые умения	Применять языки программирования, определенные в техническом задании на разработку системных утилит, для написания программного кода
	Создавать блок-схемы алгоритмов функционирования разрабатываемых программных продуктов
	Оценивать вычислительную сложность алгоритма функционирования разрабатываемых программных продуктов
	Осуществлять отладку утилит операционной системы
Необходимые знания	Архитектура целевой аппаратной платформы
	Система команд микропроцессора на целевой аппаратной платформе
	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Технологии программирования и разработки блок-схем
	Основы теории алгоритмов и ее применения
	Конструкции распределенного и параллельного программирования
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Принципы построения сетевого взаимодействия
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Стандарты информационного взаимодействия систем
	Отраслевые и локальные нормативно-правовые акты, действующие в организации

	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.1.4. Трудовая функция

Наименование	Создание инструментальных средств программирования	Код	A/04.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Определение перечня необходимой для создания инструментальных средств программирования технической документации
	Освоение необходимой для создания инструментальных средств программирования технической документации
	Разработка исходного кода и создание бинарных файлов программного обеспечения создаваемых инструментальных средств программирования
	Тестирование программного обеспечения создаваемых инструментальных средств программирования
	Разработка эксплуатационной документации создаваемых инструментальных средств программирования
	Сопровождение программного обеспечения создаваемых инструментальных средств программирования
Необходимые умения	Применять языки программирования низкого уровня, определенные в техническом задании на разработку инструментальных средств программирования, для написания программного кода
	Осуществлять отладку программ, написанных на языке программирования низкого уровня
	Применять языки программирования высокого уровня, определенные в техническом задании на разработку инструментальных средств программирования, для написания программного кода
	Осуществлять отладку программ, написанных на языках высокого уровня
	Использовать коммерческие операционные системы
	Оформлять техническую документацию
Необходимые знания	Средства программирования и их классификация
	Архитектура сред программирования
	Классификация языков программирования
	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Основные структуры данных
	Основные модели данных и их организация
	Принципы объектно-ориентированного программирования
	Языки функционального и логического программирования
	Конкурентное программирование

	Методы и алгоритмы грамматического разбора текста программы
	Компиляторы языков программирования, их виды, принципы работы
	Методы и алгоритмы генерации исполняемого кода
	Система команд микропроцессора целевой аппаратной платформы
	Структура объектных и исполняемых файлов в целевой операционной системе
	Компоновщики, методы сборки исполняемых файлов из объектных файлов
	Методы и алгоритмы оптимизации исполняемого кода
	Интерпретаторы языков программирования, их виды, принципы работы
	Методы управления памятью
	Принципы работы программного отладчика
	Основы делопроизводства
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.2. Обобщенная трудовая функция

Наименование	Разработка систем управления базами данных	Код	B	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Ведущий инженер-программист Ведущий системный программист

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных технологий и программного обеспечения
Требования к опыту практической работы	Не менее одного года работы в области системного программирования
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем

	2132	Программисты
ЕКС	-	-
ОКПДТР	22824	Инженер-программист
	25857	Программист
ОКСО	230105	Программное обеспечение вычислительной техники и автоматизированных систем
	230201	Информационные системы и технологии

3.2.1. Трудовая функция

Наименование	Разработка компонентов системы управления базами данных	Код	B/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Получение технической документации на разработку системы управления базами данных
	Изучение технической документации на разработку системы управления базами данных
	Разработка структуры системы управления базами данных в целом и ее отдельных компонентов
	Создание блок-схемы системы управления базами данных
	Разработка системы многозадачного и многопользовательского режимов
	Разработка системы администрирования данных
	Разработка системы поддержки транзакционных механизмов
	Разработка системы масштабируемости системы управления базами данных
	Разработка системы контроля целостности данных
	Разработка системы безопасности системы управления базами данных
	Разработка системы резервного копирования
	Написание исходного кода системы управления базами данных на языке программирования системы управления базами данных
	Передача исходного кода системы управления базами данных на тестирование
Необходимые умения	Идентифицировать класс разрабатываемой системы управления базами данных в зависимости от выполняемых ею задач, определенных в техническом задании на разработку системы управления базами данных
	Идентифицировать класс разрабатываемой системы управления базами данных в зависимости от аппаратных средств, определенных в техническом задании на разработку системы управления базами данных
	Создавать блок-схемы алгоритмов функционирования разрабатываемых компонентов системы управления базами данных
	Оценивать вычислительную сложность алгоритмов функционирования разрабатываемых компонентов системы управления базами данных
	Применять языки программирования, определенные в техническом задании на разработку системы управления базами данных, для написания программного кода

	Осуществлять подготовку и сохранение резервных копий данных
	Применять нормативно-техническую документацию при использовании систем управления базами данных
Необходимые знания	Теория баз данных
	Основные структуры данных
	Основные модели данных и их организация
	Принципы построения языков запросов и манипулирования данными
	Методы обработки данных
	Основы современных систем управления базами данных
	Методы поддержки, контроля и оптимизации баз данных
	Системы хранения и анализа баз данных
	Методы повышения надежности работы системы управления базами данных
	Методы построения баз знаний и принципы построения экспертных систем
	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Конструкции распределенного и параллельного программирования
	Способы и механизмы управления данными
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Методы организации файловых систем
	Принципы построения сетевого взаимодействия
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Рынок современных систем управления базами данных и баз данных
	Принципы организации инфокоммуникационных систем
	Основы информационной безопасности
	Подходы к автоматизации и стандарты автоматизации организации
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
Другие характеристики	-

3.2.2. Трудовая функция

Наименование	Отладка разрабатываемой системы управления базами данных	Код	B/02.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала		
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Приемка исходного кода системы управления базами данных после тестирования
	Анализ результатов тестирования разрабатываемой системы управления базами данных
	Отладка исходного кода системы управления базами данных на языке программирования разрабатываемой системы управления базами данных в целом и кодов ее компонентов
	Отладка системы многозадачного и многопользовательского режимов
	Отладка системы поддержки транзакционных механизмов
	Коррекция системы администрирования данных по результатам тестирования
	Отладка системы масштабируемости разрабатываемой системы управления базами данных в целом и ее компонентов
	Отладка системы контроля целостности данных
	Отладка системы безопасности разрабатываемой системы управления базами данных в целом и ее компонентов
	Настройка системы резервного копирования
	Уточнение блок-схемы функционирования разрабатываемой системы управления базами данных в целом и ее компонентов после тестирования
Необходимые умения	Применять языки программирования, определенные в техническом задании на разработку системы управления базами данных, для написания программного кода
	Выявлять ошибки в программном коде
	Применять методы и приемы отладки программного кода
	Проверять соответствие выполненных работ требованиям проектной документации на разрабатываемую систему управления базами данных
	Применять нормативно-техническую документацию при использовании систем управления базами данных
	Осуществлять подготовку и сохранение резервных копий данных
Необходимые знания	Теория баз данных
	Современные методики тестирования разрабатываемого программного обеспечения
	Методы поддержки, контроля и оптимизации баз данных
	Методы обработки данных
	Методы повышения надежности работы системы управления базами данных
	Основные модели данных и их организация
	Системы хранения и анализа баз данных
	Принципы построения языков запросов и манипулирования данными
	Основы современных систем управления базами данных
	Методы построения баз знаний и принципы построения экспертных систем
	Системное программное обеспечение и программное обеспечение баз данных
	Основы теории алгоритмов и ее применения
	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Конструкции распределенного и параллельного программирования
	Способы и механизмы управления данными

	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Методы организации файловых систем
	Принципы построения сетевого взаимодействия
	Основы архитектуры, устройства и функционирования вычислительных систем
	Устройство и принципы функционирования информационных систем
	Языки бизнес-приложений
	Стандарты информационного взаимодействия систем
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
Другие характеристики	-

3.2.3. Трудовая функция

Наименование	Документирование разработанной системы управления базами данных в целом и ее компонентов	Код	B/03.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала		
				Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Протоколирование структуры разработанной системы управления базами данных в целом и ее компонентов
	Протоколирование системы безопасности разработанной системы управления базами данных в целом и ее компонентов
	Протоколирование системы резервного копирования
	Протоколирование системы администрирования данных
	Протоколирование исходного кода разработанной системы управления базами данных в целом и ее компонентов
	Подготовка отчетов о функционировании систем управления базами данных
	Подготовка эксплуатационной документации по работе с системой управления базами данных
	Подготовка технологической документации по работе с системой управления базами данных
	Разработка методических инструкций по работе с системой управления базами данных
Необходимые умения	Вести эксплуатационную документацию
	Вести технологическую документацию
	Применять нормативно-техническую документацию при использовании систем управления базами данных
Необходимые знания	Методы документирования системы управления базами данных в целом и ее компонентов
	Программные продукты, используемые для документирования системы управления базами данных в целом и ее компонентов

	Специальная терминология в области систем управления баз данных
	Основные структуры данных
	Основные модели данных и их организация
	Принципы построения языков запросов и манипулирования данными
	Основы современных систем управления базами данных
	Методы построения баз знаний и принципы построения экспертных систем
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основы архитектуры, устройства и функционирования вычислительных систем
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Принципы организации инфокоммуникационных систем
	Основы информационной безопасности
	Подходы к автоматизации и стандарты автоматизации организации
	Основы делопроизводства
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.2.4. Трудовая функция

Наименование	Сопровождение созданной системы управления базами данных	Код	B/04.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Анализ ошибок в компонентах системы управления базами данных по данным эксплуатации
	Устранение ошибок в компонентах системы управления базами данных по данным эксплуатации
	Оформление результатов работ по модификации системы управления базами данных в целом и ее компонентов
	Сопровождение документации по системе управления базами данных в целом и ее компонентам
	Консультирование по использованию системы управления базами данных в целом и ее компонентов, ее установке, параметризации, по диагностике сбоев операционной системы
Необходимые умения	Применять языки программирования, определенные в техническом задании на разработку системы управления базами данных, для написания программного кода
	Обнаруживать ошибки в работе системы управления базами данных

	Работать в используемой системе регистрации ошибок
	Готовить документацию по разработанной системе управления базами данных в соответствие с действующими федеральными, отраслевыми и локальными нормативно-правовыми актами
	Осуществлять консультации пользователей по созданной системе управления базами данных
Необходимые знания	Синтаксис языка программирования, использованного в системе управления базами данных, особенности программирования на этом языке, стандартные библиотеки языка программирования
	Методы поиска ошибок в операционных системах
	Методы документирования работы созданной системы управления базами данных в целом и ее компонентов
	Программные продукты, используемые для документирования работы созданной системы управления базами данных в целом и ее компонентов
	Порядок управления версиями разрабатываемой базы данных
	Механизмы мониторинга системы управления базами данных
	Основы систем управления базами данных
	Способы и механизмы управления данными
	Основные модели данных и их организация
	Специальная терминология в области систем управления баз данных
	Теория баз данных
	Системы хранения и анализа баз данных
	Принципы построения языков запросов и манипулирования данными
	Методы построения баз знаний и принципы построения экспертных систем
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Устройство и принципы функционирования информационных систем
	Программные средства и платформы инфраструктуры информационных технологий организаций
	Аппаратные средства и платформы инфраструктуры информационных технологий организаций
	Принципы организации инфокоммуникационных систем
	Основы информационной безопасности
	Подходы к автоматизации и стандарты автоматизации организации
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.3. Обобщенная трудовая функция

Наименование	Разработка операционных систем	Код	C	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Ведущий инженер-программист Ведущий системный программист

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных технологий и программного обеспечения
Требования к опыту практической работы	Не менее одного года работы в области системного программирования
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2132	Программисты
ЕКС	-	-
ОКПДТР	22824	Инженер-программист
	25857	Программист
ОКСО	230105	Программное обеспечение вычислительной техники и автоматизированных систем
	230201	Информационные системы и технологии

3.3.1. Трудовая функция

Наименование	Формирование требований к операционной системе	Код	C/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Взаимодействие с заказчиком и другими заинтересованными лицами с целью формирования требований к разрабатываемой операционной системе
	Составление спецификаций требований к разрабатываемой операционной системе
	Согласование спецификаций требований к разрабатываемой операционной системе со всеми заинтересованными лицами

	Ведение базы данных требований к разрабатываемой операционной системе
Необходимые умения	Идентифицировать класс разрабатываемой операционной системы в зависимости от выполняемых ею задач, определенных в техническом задании на разработку операционной системы
	Идентифицировать класс разрабатываемой операционной системы в зависимости от аппаратных средств, определенных в техническом задании на разработку операционной системы
	Переформулировать ожидания от программных средств в требования к ним
	Выявлять требования к программным средствам на основе опроса заинтересованных лиц
	Выявлять требования к программным средствам на основе спецификаций оборудования
	Анализировать требования, проверять их полноту и осуществимость
	Писать текст спецификации требований к программным средствам
	Работать в используемой системе управления требованиями
Необходимые знания	Состав и классификация требований к операционным системам
	Основные характеристики качества требований к операционным системам
	Методы выявления и анализа требований к операционным системам
	Способы изложения требований в спецификации на программные средства
	Стандарты по работе с требованиями к программным средствам
	Дисциплина управления требованиями
	Теория операционных систем и теории языков программирования
	Сетевые технологии и протоколы
	Специальная терминология в области операционных систем
	Основы теории алгоритмов и ее применения
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Программные средства и платформы инфраструктуры информационных технологий организаций
	Аппаратные средства и платформы инфраструктуры информационных технологий организаций
	Основы информационной безопасности
	Теория системного анализа
	Правила ведения деловой переписки
	Правила ведения деловых переговоров
	Основы делового этикета
	Английский язык на уровне чтения технической документации и разговорный технический в области информационных и компьютерных технологий

	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Государственные стандарты ЕСПД
Другие характеристики	-

3.3.2. Трудовая функция

Наименование	Разработка архитектуры операционной системы	Код	C/02.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Изучение технической документации на устройства, в среде которых разрабатывается операционная система
	Разработка архитектуры операционной системы и ее слоев
	Обсуждение и согласование программной архитектуры с заказчиком
	Фиксирование программной архитектуры операционной системы в технической документации
	Разработка блок-схемы операционной системы
	Разработка интерфейсов модулей операционной системы и согласования параметров
	Выбор алгоритмов реализации расписаний, видов расписаний процессора
	Выбор алгоритмов реализации расписаний, видов расписаний доступа к подсистемам ввода/ вывода
	Выбор алгоритмов реализации расписаний, видов расписаний обращения к дисковым подсистемам
	Выбор алгоритмов обращения к оперативной памяти и реализации расписаний, видов расписаний
	Выбор реализации мультипрограммной работы, системы прерываний, реализации «часов»
	Выбор способов реализации коммуникации и синхронизации процессов
	Выбор алгоритмов приоритизации процессов и расписаний их загрузки
	Выбор алгоритмов реализации многопоточного режима работы (цепочек) процессов
	Определение состава ядра операционной системы и состава утилит
	Определение требований к компиляторам для работы процессов под управлением ядра
	Выбор версии языка программирования, определенного в техническом задании
Необходимые умения	Применять языки программирования, определенные в техническом задании на разработку операционной системы, для написания программного кода
	Идентифицировать класс разрабатываемой операционной системы в зависимости от выполняемых ею задач, определенных в техническом

	задании на разработку операционной системы
	Идентифицировать класс разрабатываемой операционной системы в зависимости от аппаратных средств, определенных в техническом задании на разработку операционной системы
	Планировать архитектуру операционной системы
	Разрабатывать блок-схемы системных программных продуктов
	Пользоваться вычислительными методами для разработки расписаний, сортировок, методов доступа к памяти и файловым системам
	Разрабатывать алгоритмы и составлять их текстовые и графические описания
	Разрабатывать структуры классов и составлять их текстовые и графические описания
	Идентифицировать технические риски, находить способы защиты от них
	Излагать архитектурные решения по разрабатываемой операционной системе, объяснять их сильные и слабые стороны
	Пользоваться документацией по аппаратным средствам
Необходимые знания	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Теория операционных систем и теории языков программирования
	Сетевые технологии и протоколы
	Система команд конкретной вычислительной техники
	Специальная терминология в области операционных систем
	Основы теории алгоритмов и ее применения
	Основные структуры данных
	Конструкции распределенного и параллельного программирования
	Методы построения расписаний
	Методы коммуникации процессов
	Методы организации памяти вычислительных устройств
	Методы синхронизации процессов
	Методы организации подсистем ввода/вывода
	Методы и основные этапы трансляции
	Способы и механизмы управления данными
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Методы организации файловых систем
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Основные модели данных и принципы их организации
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Теория системного анализа
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий

	Государственные стандарты ЕСПД
Другие характеристики	-

3.3.3. Трудовая функция

Наименование	Написание компонентов операционной системы	Код	C/03.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Поиск технической документации по используемым средствам и технологиям (языкам программирования, программным интерфейсам, протоколам передачи данных)
	Освоение технической документации по используемым средствам и технологиям (языкам программирования, программным интерфейсам, протоколам передачи данных)
	Выбор языка программирования для описания алгоритмов и структур данных разрабатываемой операционной системы
	Разработка блок-схемы разрабатываемых компонентов операционной системы
	Написание исходного кода разрабатываемого компонента операционной системы в соответствии с заданной спецификацией
Необходимые умения	Разрабатывать блок-схемы системных программных продуктов
	Оценивать вычислительную сложность алгоритма функционирования разрабатываемых компонентов операционной системы
	Применять языки программирования, определенные в техническом задании на разработку операционной системы, для написания программного кода
Необходимые знания	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Методы построения расписаний
	Методы коммуникации процессов
	Методы организации памяти вычислительных устройств
	Методы синхронизации процессов
	Методы организации подсистем ввода/вывода
	Архитектура конкретного вычислительного устройства, используемого при разработке операционной системы
	Теория и методы структурного программирования
	Специальная терминология в области системного программирования
	Основные структуры данных
	Конструкции распределенного и параллельного программирования
	Методы и основные этапы трансляции
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Методы организации файловых систем

	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Принципы построения языков запросов и манипулирования данными
	Основы архитектуры, устройства и функционирования вычислительных систем
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.3.4. Трудовая функция

Наименование	Контроль соблюдения архитектуры в процессе написания операционной системы	Код	C/04.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Инспектирование кода разрабатываемой операционной системы
	Проверка реализации архитектурных решений
	Обсуждение архитектурных решений в ходе рабочих совещаний о состоянии разработки операционной системы
	Модификация архитектурных решений разрабатываемой операционной системы в процессе реализации
Необходимые умения	Применять языки программирования, определенные в техническом задании на разработку операционной системы, для написания программного кода
	Отслеживать исходный код разрабатываемой операционной системы
	Модифицировать исходный код разрабатываемой операционной системы
	Подготавливать отчеты о ревизии исходного кода с пояснениями к ошибкам, связанным с несоблюдением архитектуры
Необходимые знания	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Теоретические основы системного программирования
	Типичные ошибки и проблемы в реализации системных программных средств
	Теория операционных систем и теории языков программирования
	Сетевые технологии и протоколы
	Система команд конкретной вычислительной техники
	Специальная терминология в области системного программирования
	Основные структуры данных
	Конструкции распределенного и параллельного программирования

	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Методы организации файловых систем
	Принципы построения сетевого взаимодействия
	Основные модели данных и их организация
	Принципы построения языков запросов и манипулирования данными
	Основы архитектуры, устройства и функционирования вычислительных систем
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Основы информационной безопасности
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Государственные стандарты ЕСПД
Другие характеристики	-

3.3.5. Трудовая функция

Наименование	Отладка разрабатываемых компонентов операционной системы	Код	C/05.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Уточнение структуры компонентов операционных систем и системы в целом
	Уточнение блок-схемы разрабатываемых компонентов операционных систем и системы в целом
	Отладка системы многозадачного и многопользовательского режимов
	Отладка системы безопасности разрабатываемых компонентов операционных систем и системы в целом
	Настройка системы резервного копирования
	Отладка системы поддержки транзакционных механизмов
	Коррекция системы администрирования
	Отладка системы масштабируемости разрабатываемых компонентов операционных систем и системы в целом
	Отладка системы контроля целостности разрабатываемых компонентов операционных систем и системы в целом
	Отладка исходного кода разрабатываемых компонентов операционных систем и системы в целом на языке программирования, определенном в техническом задании
Необходимые умения	Применять языки программирования, определенные в техническом задании на разработку операционной системы, для написания программного кода
	Выявлять ошибки в программном коде
	Применять методы и приемы отладки программного кода

	Оценивать вычислительную сложность алгоритма функционирования разрабатываемых компонентов операционной системы
	Проверять соответствие выполненных работ требованиям проектной документации
	Применять нормативно-техническую документацию при использовании операционной системы
	Осуществлять подготовку и сохранение резервных копий операционной системы
Необходимые знания	Синтаксис, особенности программирования и стандартные библиотеки выбранного языка программирования
	Методики тестирования разрабатываемых операционных систем
	Методы обработки данных
	Методы повышения надежности работы операционных систем
	Основные структуры данных
	Конструкции распределенного и параллельного программирования
	Способы и механизмы управления данными
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Методы организации файловых систем
	Принципы построения сетевого взаимодействия
	Основы архитектуры, устройства и функционирования вычислительных систем
	Устройство и принципы функционирования информационных систем
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Современные стандарты информационного взаимодействия систем
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
Другие характеристики	-

3.3.6. Трудовая функция

Наименование	Документирование разрабатываемой операционной системы	Код	C/06.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Оформление исходного кода в соответствии с технологией системного программирования
	Написание комментариев к исходным программным компонентам операционной системы
	Написание технической документации в соответствии с правилами проекта по разработке операционной системы
	Оформление программной документации в соответствии с требованиями ЕСПД
	Запись всех значимых результатов работ в систему контроля версий

Необходимые умения	Работать в системе контроля версий, используемой в проекте по разработке операционной системы
	Оформлять документацию при помощи программных средств
	Вести эксплуатационную документацию по разработке операционной системы
	Вести технологическую документацию по разработке операционной системы
	Готовить заявки на получение свидетельства о государственной регистрации программы для электронных вычислительных машин в Федеральный институт промышленной собственности (Роспатент)
Необходимые знания	Правила оформления и комментирования кода в соответствии с технологией системного программирования
	Принципы управления версиями программного обеспечения
	Порядок управления версиями в текущем проекте по разработке операционной системы
	Специальная терминология в области разработки операционных систем
	Основные структуры данных
	Конструкции распределенного и параллельного программирования
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основные модели данных и их организация
	Основы программирования
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Принципы организации инфраструктуры информационных технологий
	Английский язык на уровне чтения технической документации по информационным и компьютерным технологиям
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Государственные стандарты ЕСПД
Другие характеристики	-

3.3.7. Трудовая функция

Наименование	Сопровождение созданной операционной системы	Код	C/07.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Устранение ошибок в компонентах операционной системы по данным

	эксплуатации
	Внесение изменений в компонент операционной системы при обнаружении ошибки операционной системы
	Оформление результатов работ по модификации операционной системы
	Сопровождение документации операционной системы
	Консультирование по использованию операционной системы, ее установке, параметризации, по диагностике сбоев операционной системы
Необходимые умения	Применять языки программирования, определенные в техническом задании на разработку операционной системы, для написания программного кода
	Осуществлять консультации пользователей операционной системы
	Обнаруживать ошибки операционной системы
	Работать в используемой системе регистрации ошибок
Необходимые знания	Синтаксис языка программирования сопровождаемой операционной системы, особенности программирования на этом языке, стандартные библиотеки языка программирования
	Методы поиска ошибок в операционных системах
	Методы документирования работы операционной системы
	Программные продукты, используемые для документирования работы операционной системы
	Порядок управления версиями в проекте по созданию операционной системы
	Механизмы мониторинга операционной системы
	Специальная терминология в области системного программирования
	Конструкции распределенного и параллельного программирования
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Принципы построения сетевого взаимодействия
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Основы информационной безопасности
	Английский язык на уровне чтения технической документации в области информационных и компьютерных технологий
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Государственные стандарты ЕСПД
Другие характеристики	-

3.4. Обобщенная трудовая функция

Наименование	Организация разработки системного программного обеспечения	Код	D	Уровень квалификации	7

Происхождение обобщенной трудовой	Оригинал	X	Заимствовано из оригинала		

функции				
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Ведущий системный программист Ведущий инженер-программист Главный инженер-программист Руководитель рабочей группы системных программистов Главный системный программист

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных технологий и программного обеспечения
Требования к опыту практической работы	Не менее двух лет работы в области системного программирования
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2132	Программисты
ЕКС	-	-
ОКПДТР	22824	Инженер-программист
	25857	Программист
	26153	Руководитель группы (функциональной в прочих областях деятельности)
ОКСО	230105	Программное обеспечение вычислительной техники и автоматизированных систем
	230201	Информационные системы и технологии

3.4.1. Трудовая функция

Наименование	Планирование разработки системного программного обеспечения	Код	D/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Проведение переговоров с заказчиком о целях, задачах, рамках и других свойствах проекта по разработке системного программного обеспечения
	Обсуждение с техническими специалистами выполнимости проекта по разработке системного программного обеспечения

	Оценка сроков, ресурсоемкости, себестоимости проекта по разработке системного программного обеспечения
	Составление бюджета проекта по разработке системного программного обеспечения
	Заказ необходимых для выполнения проекта по разработке системного программного обеспечения ресурсов
	Подготовка документации по разработке системного программного обеспечения
	Составление плана-графика выполнения проекта по разработке системного программного обеспечения
Необходимые умения	Описывать цели проекта и критерии успешности их достижения
	Описывать задачи проекта исходя из его целей и методов их достижения
	Оценивать трудоемкость разработки программных средств
	Составлять графики выполнения работ
	Составлять бюджет проекта по разработке программных средств
	Идентифицировать организационные и технические риски проектов
Необходимые знания	Дисциплина управления проектами
	Особенности управления проектами по разработке программных средств
	Стандарты системной и программной инженерии
	Технологическая область, в которой идет разработка системного программного обеспечения
	Технологии, применяемые в конкретном проекте по разработке системного программного обеспечения
	Методы и средства оценки трудоемкости разработки программных средств
	Методы и средства составления сетевых графиков выполнения работ
	Порядок взаиморасчетов юридических и физических лиц по действующему законодательству
	Законодательство Российской Федерации в сфере защиты авторских и смежных прав
	Трудовое законодательство Российской Федерации
	Правила ведения деловой переписки
	Правила ведения деловых переговоров
	Основы делового этикета
	Типичные риски в процессе разработки программ, методы их идентификации и работы с ними
	Методы верификации и валидации программных средств
	Критерии качества программных средств
	Методы контроля качества программных средств
	Специальная терминология в области разработки системного программного обеспечения
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Методики тестирования разрабатываемых информационных систем

	Стандарты информационного взаимодействия систем
	Основы информационной безопасности
	Теория системного анализа
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации и разговорный технический в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.4.2. Трудовая функция

Наименование	Формирование группы программистов для разработки системного программного обеспечения	Код	D/02.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Оценка необходимого состава и количества специалистов в проекте по разработке системного программного обеспечения
	Описание имеющихся в проекте по разработке системного программного обеспечения вакансий для специалистов
	Проведение интервью со специалистами, претендующими на участие в проекте по разработке системного программного обеспечения
	Контролирование подготовки, согласование и подписание договоров со специалистами
	Выделение в проекте по разработке системного программного обеспечения задач, перекладываемых на субподрядчиков
	Выбор субподрядчиков и проведение с ними коммерческих переговоров
	Контроль подготовки, согласования и подписания договоров с субподрядчиками
Необходимые умения	Составлять описание вакансий
	Проводить интервью с разработчиками
	Оценивать возможности кандидата на реализацию поставленной задачи
	Проводить коммерческие переговоры с субподрядчиками
Необходимые знания	Текущее состояние рынка труда в сфере программирования
	Трудовое законодательство Российской Федерации
	Текущее положение на рынке аутсорсинга разработки
	Гражданское законодательство Российской Федерации
	Законодательство Российской Федерации в сфере защиты авторских и смежных прав
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения

	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Программные средства и платформы инфраструктуры информационных технологий организаций
	Аппаратные средства и платформы инфраструктуры информационных технологий организаций
	Основы информационной безопасности
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации и разговорный технический в области информационных и компьютерных технологий
Другие характеристики	-

3.4.3. Трудовая функция

Наименование	Организация работы программистов в группе по разработке системного программного обеспечения	Код	D/03.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Проработка постановки задачи с руководителем проекта и архитектором по разработке системного программного обеспечения
	Деление поставленной задачи на подзадачи и распределение их между программистами
	Определение способа интеграции разработанных компонентов системного программного обеспечения в единое целое
	Составление плана-графика решения задачи силами рабочей группы
	Настройка системы контроля версий для решения поставленной задачи
	Настройка системы регистрации ошибок для решения поставленной задачи
	Составление задания для группы стандартов кодирования (в том числе комментирования кода)
	Определение порядка проведения рабочих совещаний группы
	Определение формы и регулярности текущей отчетности членов группы
Необходимые умения	Объективно оценивать сильные и слабые стороны членов группы
	Идентифицировать технические и организационные риски разработки
	Оценивать возможный ущерб от реализации рисков, вырабатывать контрмеры
	Оценивать трудоемкость работы с учетом возможностей группы и рисков
	Составлять сетевые графики проекта

	Доводить до членов группы принимаемые управленческие решения
	Доводить до членов группы принимаемые технические решения
	Работать в используемой системе управления требованиями
	Работать в используемой системе управления версиями
Необходимые знания	Основные стандарты системной и программной инженерии
	Методологии разработки программных средств
	Основы управления проектами
	Дисциплина управления требованиями
	Системы управления версиями
	Дисциплина управления конфигурациями
	Механизмы мониторинга системы управления базами данных
	Основы систем управления базами данных
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем
	Программные средства и платформы инфраструктуры информационных технологий
	Аппаратные средства и платформы инфраструктуры информационных технологий
	Основы информационной безопасности
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации и разговорный технический в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.4.4. Трудовая функция

Наименование	Контроль деятельности рабочей группы программистов по разработке системного программного обеспечения	Код	D/04.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал	X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Проведение регулярных рабочих совещаний группы по разработке системного программного обеспечения
	Получение и изучение текущих отчетов членов группы по разработке системного программного обеспечения
	Контроль соблюдения членами группы сроков решения задач

	Перераспределение задач между членами группы
	Контроль соблюдения членами группы дисциплины управления версиями разрабатываемого системного программного обеспечения
	Контроль соблюдение членами группы заданных стандартов кодирования
	Контроль разработки программной документации в соответствии с ЕСПД
	Оценка соответствия получаемых результатов спецификации требований
	Оценка соответствия получаемых результатов фактическим нуждам заказчика
	Оценка качества разрабатываемых программных средств
	Контроль соблюдения плана-графика разработки компонент системного программного обеспечения
	Управление требованиями, влияющими на разработку системного программного обеспечения
	Контроль за обеспечением проекта по разработке системного программного обеспечения необходимыми ресурсами
	Управление рисками в проекте по разработке системного программного обеспечения
Необходимые умения	Идентифицировать возникающие риски по устным и письменным отчетам
	Оценивать влияние рисков на сроки решения задачи и вырабатывать контрмеры
	Оценивать влияние рисков на качество результата и вырабатывать контрмеры
	Работать в используемой системе управления проектом
	Работать в используемой системе управления версиями
	Работать с сетевыми графиками проекта
Необходимые знания	Типичные риски в процессе разработки программ, методы их идентификации и работы с ними
	Методы верификации и валидации программных средств
	Критерии качества программных средств
	Методы контроля качества программных средств
	Специальная терминология в области разработки системного программного обеспечения
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Устройство и принципы функционирования информационных систем
	Методики тестирования разрабатываемых информационных систем
	Стандарты информационного взаимодействия систем
	Основы информационной безопасности
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации и разговорный технический в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.4.5. Трудовая функция

Наименование	Предоставление заказчику результатов разработки системного программного обеспечения	Код	D/05.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Проведение после согласования с заказчиком испытаний и приемки разработанного системного программного обеспечения
	Передача заказчику исходного кода разработанного системного программного обеспечения
	Передача заказчику исполняемых файлов разработанного системного программного обеспечения
	Предоставление заказчику текущей отчетности о состоянии проекта по разработке системного программного обеспечения
	Согласование и передача заказчику технологической документации на разработанное системное программное обеспечение
	Согласование и передача заказчику эксплуатационной документации на разработанное системное программное обеспечение
	Разработка инструкции по работе с разработанным системным программным обеспечением
Необходимые умения	Проверять техническую документацию
	Рецензировать техническую документацию
	Организовывать в проекте процесс документирования программных средств
	Организовывать в проекте процесс поставки программных средств заказчику
Необходимые знания	Отраслевые и локальные стандарты, описывающие испытания и приемку программных средств
	Правила испытаний и приемки программных средств у заказчика
	Стандарты на документацию разработки программных средств
	Стандарты на эксплуатационную документацию программных средств
	Взаимосвязь процесса документирования с основными процессами жизненного цикла программных средств
	Методы верификации и валидации программных средств
	Критерии качества программных средств
	Методы контроля качества программных средств
	Основы систем управления базами данных
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Устройство и принципы функционирования информационных систем
	Стандарты информационного взаимодействия систем

	Основы информационной безопасности
	Современные подходы к автоматизации и стандарты автоматизации организации
	Правила ведения деловой переписки
	Правила ведения деловых переговоров
	Основы делового этикета
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации и разговорный технический в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.5. Обобщенная трудовая функция

Наименование	Код	Уровень квалификации
Интеграция разработанного системного программного обеспечения	E	7

Происхождение обобщенной трудовой функции				
Оригинал	X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Ведущий системный программист Ведущий инженер-программист Главный инженер-программист Руководитель рабочей группы системных программистов Главный системный программист

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных технологий и программного обеспечения
Требования к опыту практической работы	Не менее двух лет работы в области системного программирования
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
ЕКС	-	-
ОКПДТР	22824	Инженер-программист
	25857	Программист
	26153	Руководитель группы (функциональной в прочих областях деятельности)

ОКСО	230105	Программное обеспечение вычислительной техники и автоматизированных систем
	230201	Информационные системы и технологии

3.5.1. Трудовая функция

Наименование	Планирование интеграции разработанного системного программного обеспечения	Код	E/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Планирование архитектуры инфокоммуникационной системы
	Планирование использования аппаратных и программных средств
	Выбор стратегии интеграции и практикуемых способов сборки разработанного системного программного обеспечения
	Определение порядка управления версиями сборок разработанного системного программного обеспечения
	Подготовка интеграционного сервера и настройка автоматической сборки разработанного системного программного обеспечения
Необходимые умения	Устанавливать и настраивать серверы интеграции, налаживать автоматическую сборку разработанного системного программного обеспечения
	Определять порядок сборки разработанного системного программного обеспечения с учетом зависимостей в компонентах
	Писать скрипты автоматизации сборки на скриптовых языках
	Писать задания для сред управления заданиями
	Работать в используемой системе управления требованиями
	Работать в используемой системе управления версиями
Необходимые знания	Подходы к интеграции системного программного обеспечения
	Представление о зависимостях и способах работы с зависимостями
	Типичный процесс интеграции, его обязательные и необязательные стадии
	Основные серверы интеграции, их основные возможности и особенности
	Скриптовые языки, средства управления заданиями
	Механизмы мониторинга системы управления базами данных
	Основы систем управления базами данных
	Принципы организации, состав и схемы работы операционных систем
	Принципы построения сетевого взаимодействия
	Основные методы разработки программного обеспечения
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Устройство и принципы функционирования информационных систем
	Методики тестирования разрабатываемых информационных систем
	Стандарты информационного взаимодействия систем

	Программные средства и платформы инфраструктуры информационных технологий
	Аппаратные средства и платформы инфраструктуры информационных технологий
	Основы информационной безопасности
	Теория системного анализа
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации и разговорный технический в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

3.5.2. Трудовая функция

Наименование	Внедрение разработанного системного программного обеспечения	Код	E/02.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Внедрение аппаратных средств
	Внедрение системного и прикладного программного обеспечения
	Инсталляция системного программного обеспечения
	Параметризация операционных систем при установке
	Администрирование интеграционного сервера
	Регулярный анализ отчетов о результатах сборки и прогонки юнит-тестов
	Контроль подготовки эксплуатационной документации
	Подготовка стабилизированной сборки разработанного системного программного обеспечения для передачи в серийное производство
Необходимые умения	Устанавливать и настраивать серверы интеграции, налаживать автоматическую сборку разработанного системного программного обеспечения
	Определять порядок сборки разработанного системного программного обеспечения с учетом зависимостей в компонентах
	Писать скрипты автоматизации сборки разработанного системного программного обеспечения на скриптовых языках
	Писать задания для сред управления заданиями
	Работать в используемой системе управления требованиями
	Работать в используемой системе управления версиями
Необходимые знания	Подходы к внедрению системного программного обеспечения
	Представление о зависимостях и способах работы с зависимостями
	Типичный процесс внедрения программного обеспечения, его обязательные и необязательные стадии
	Основные серверы интеграции, их основные возможности и особенности

	Скриптовые языки, средства управления заданиями
	Принципы организации, состав и схемы работы операционных систем
	Принципы управления ресурсами
	Принципы построения сетевого взаимодействия
	Основные модели данных и их организация
	Принципы построения языков запросов и манипулирования данными
	Основы архитектуры, устройства и функционирования вычислительных систем
	Архитектура и принципы функционирования коммуникационного оборудования
	Основы систем управления базами данных
	Устройство и принципы функционирования информационных систем
	Методики тестирования разрабатываемых информационных систем
	Стандарты информационного взаимодействия систем
	Основы информационной безопасности
	Теория системного анализа
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
	Английский язык на уровне чтения технической документации и разговорный технический в области информационных и компьютерных технологий
	Государственные стандарты ЕСПД
Другие характеристики	-

Приложение 4. Типовые требования к виду профессиональной деятельности «Специалист по технической поддержке информационно-коммуникационных систем»

I. Общие сведения

Техническая поддержка клиентов при установке и эксплуатации информационно-коммуникационных (инфокоммуникационных) систем и/или их составляющих
(наименование вида профессиональной деятельности)

Основная цель вида профессиональной деятельности:

Постпродажная помощь клиенту для поддержания в работоспособном состоянии с заданным качеством инфокоммуникационных систем и/или их составляющих

Группа занятий:

2131	Разработчики и аналитики компьютерных систем	4222	Служащие, занятые приемом и информированием посетителей
2144	Инженеры-электроники, инженеры по связи и приборостроению	-	-
(код ОКЗ)	(наименование)	(код ОКЗ)	(наименование)

Отнесение к видам экономической деятельности:

64.20.7	Прочая деятельность в области электросвязи
72.60	Прочая деятельность, связанная с использованием вычислительной техники и информационных технологий
(код ОКВЭД)	(наименование вида экономической деятельности)

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида трудовой деятельности)

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Работа с первичными обращениями клиентов по вопросам технической эксплуатации инфокоммуникационных систем и/или их составляющих	3	Обработка обращений клиентов по вопросам эксплуатации инфокоммуникационных систем и/или их составляющих	A/01.3	3
			Инструктирование клиентов в решении типовых проблем, возникших у клиента при технической эксплуатации инфокоммуникационных систем и/или их составляющих	A/02.3	3
B	Руководство группой специалистов по приему заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих	6	Инструктирование клиентов в решении нетиповых проблем, возникших у клиента в процессе технической эксплуатации инфокоммуникационных систем и/или их составляющих	B/01.6	6
			Контроль выполнения заявок клиентов специалистами по технической поддержке инфокоммуникационных систем и/или их составляющих	B/02.6	6
			Обработка информации о работе специалистов с обращениями клиентов по вопросам технической поддержки инфокоммуникационных систем и/или их составляющих	B/03.6	6
C	Устранение, по обращениям клиентов, возникших у клиента проблем при установке и эксплуатации аппаратного, программного и	6	Консультирование клиентов по согласованным с соответствующими структурными подразделениями организации-поставщика срокам проведения работ по монтажу, пуску и наладке аппаратного, программного, и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих	C/01.6	6

	программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих		Устранение проблемных ситуаций, возникших у клиента при первичном конфигурировании аппаратного, программного и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих, в рамках компетенций, делегированных клиенту (дистанционно и/или на месте)	C/02.6	6
			Устранение возникшей у клиента в ходе эксплуатации проблемы на аппаратном, программном, и программно-аппаратном обеспечении инфокоммуникационных системах и/или их составляющих	C/03.6	6
D	Руководство группой специалистов по выполнению заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих	7	Организация работы группы специалистов структурного подразделения технической поддержки по выполнению заявки клиентов на техническую поддержку инфокоммуникационных систем и/или их составляющих	D/01.7	7
			Контроль качества выполненных работ группой специалистов по реализации заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих	D/02.7	7

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

Наименование	Работа с первичными обращениями клиентов по вопросам технической эксплуатации инфокоммуникационных систем и/или их составляющих	Код	A	Уровень квалификации	3

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Специалист первой линии технической поддержки Оператор технической поддержки Специалист диспетчерской службы Специалист службы поддержки

Требования к образованию и обучению	Основные программы профессионального обучения – программы профессиональной подготовки по профессиям рабочих, должностям служащих, программы переподготовки рабочих, служащих, программы повышения квалификации рабочих, служащих (до одного года)
Требования к опыту практической работы	-
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	4222	Служащие, занятые приемом и информированием посетителей
ЕКС	-	-
ОКПДТР	27099	Техник-программист
ОКСО	-	-

3.1.1. Трудовая функция

Наименование	Обработка обращений клиентов по вопросам эксплуатации инфокоммуникационных систем и/или их составляющих	Код	A/01.3	Уровень (подуровень) квалификации	3

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Прием обращений клиентов по заранее подготовленному опросному листу, согласованному с инженерами соответствующих структурных подразделений
	Регистрация обращений клиентов по заранее подготовленному опросному листу, согласованному с инженерами соответствующих структурных подразделений
	Анализ обращений клиентов с целью выявления аварийных ситуаций и/или возможных путей решения возникшей проблемы
	Формирование журнала событий по обращениям клиентов с подробным описанием выполненных действий и принятых решений
	Занесение решений в единую базу решений по поддерживаемым инфокоммуникационным системам и/или их составляющим
Необходимые умения	Выяснять из беседы с клиентом и понимать причины возникших аварийных ситуаций на поддерживаемых инфокоммуникационных системах и/или их составляющих
	Поддерживать в клиенте уверенность в успешном разрешении его технических затруднений
	Применять установленные правила делового общения при консультировании клиентов
	Отвечать на запросы клиентов в установленные регламентами сроки
	Координировать решение проблем клиентов со специалистами соответствующих технических подразделений организации (специалистами второго уровня технической поддержки)
	Работать с автоматизированными системами взаимодействия с клиентами
	Работать с программами приема, обработки и регистрации обращений клиентов
Необходимые знания	Регламенты обработки обращений в структурное подразделение технической поддержки
	Виды, назначение и правила работы с программным обеспечением для регистрации и обработки заявок на техническую поддержку
	Основные технические характеристики и архитектура поддерживаемых инфокоммуникационных систем и/или их составляющих
	Типовые решения и ответы на наиболее часто задаваемые вопросы по поддерживаемым инфокоммуникационным системам и/или их составляющим
	Основы инфокоммуникационных технологий в части поддерживаемых инфокоммуникационных систем и/или их составляющих
Другие характеристики	-

3.1.2. Трудовая функция

Наименование	Инструктирование клиентов в решении типовых проблем, возникших у клиента при технической эксплуатации инфокоммуникационных систем и/или их составляющих	Код	A/02.3	Уровень (подуровень) квалификации	3

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер

	профессионального стандарта

Трудовые действия	Ответы на наиболее часто задаваемые вопросы по поддерживаемым инфокоммуникационным системам и/или их составляющим
	Консультирование по типовым решениям по поддерживаемым инфокоммуникационным системам и/или их составляющим
	Перенаправление заявки клиента к соответствующим специалистам технических подразделений или к руководителю первой линии группы технической поддержки для разрешения возникшей проблемы
Необходимые умения	Анализировать и решать типовые запросы клиентов
	Объяснить клиентам пути решения возникшей проблемы
	Координировать решение типовых проблем, с которыми обратился клиент, со специалистами соответствующих технических подразделений организации (специалистами второго уровня технической поддержки)
	Обрабатывать информацию с использованием современных технических средств
	Работать с информационными системами и базами данных клиентов и поддерживаемого оборудования и программного обеспечения
Необходимые знания	Регламенты обработки обращений в структурное подразделение технической поддержки
	Основные технические характеристики и архитектура поддерживаемых инфокоммуникационных и/или их составляющих
	Типовые решения и ответы на наиболее часто задаваемые вопросы по поддерживаемым инфокоммуникационным системам и/или их составляющим
	Руководства пользователя, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Организационная структура организации
	Основы психологии
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
Другие характеристики	-

3.2. Обобщенная трудовая функция

Наименование	Руководство группой специалистов по приему заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих	Код	B	Уровень квалификации	6

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования	Старший специалист технической поддержки Руководитель службы приема заявок

должностей	

Требования к образованию и обучению	Высшее образование – бакалавриат
Требования к опыту практической работы	-
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
ЕКС	-	-
ОКПДТР	22824	Инженер-программист
	22870	Инженер электросвязи
	26151	Руководитель группы (специализированной в прочих отраслях)
ОКСО	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.2.1. Трудовая функция

Наименование	Код	Уровень (подуровень) квалификации
Инструктирование клиентов в решении нетиповых проблем, возникших у клиента в процессе технической эксплуатации инфокоммуникационных систем и/или их составляющих	B/01.6	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Анализ нетиповой заявки, поступившей от сотрудников первой линии технической поддержки
	Уточнение деталей проблемы, возникшей у клиента в процессе технической эксплуатации инфокоммуникационных систем и/или их составляющих
	Инструктирование клиента по устранению проблемы, возникшей у клиента в процессе технической эксплуатации инфокоммуникационных систем и/или их составляющих (дистанционно)
	Перенаправление заявки к соответствующим специалистам технических подразделений (специалистам второго уровня технической поддержки)
Необходимые умения	Анализировать и решать нетиповые запросы клиентов

	Инструктировать клиента по действиям, необходимым для устранения проблемы, возникшей у клиента в процессе технической эксплуатации инфокоммуникационных систем и/или их составляющих
	Объяснять клиенту последовательность и сроки выполнения его заявки
	Координировать решение нетиповых обращений клиентов со специалистами соответствующих технических подразделений организации (специалистами второго уровня технической поддержки)
	Использовать при инструктировании клиента понятные ему технические термины и выражения
Необходимые знания	Регламенты обработки обращений в структурное подразделение технической поддержки
	Основные технические характеристики и архитектура поддерживаемых инфокоммуникационных систем и/или их составляющих
	Типовые решения и ответы на наиболее часто задаваемые вопросы по поддерживаемым инфокоммуникационным системам и/или их составляющим
	Руководства пользователя, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Организационная структура организации
	Руководства инженера, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Основы психологии
	Основы менеджмента
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
Другие характеристики	-

3.2.2. Трудовая функция

Наименование	Код	Уровень (подуровень) квалификации
Контроль выполнения заявок клиентов специалистами по технической поддержке инфокоммуникационных систем и/или их составляющих	B/02.6	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Отслеживание выполнения заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих
	Документирование выполнения заявок на техническую поддержку поддерживаемых инфокоммуникационных систем и/или их составляющих
	Информирование клиента о выполнении поступившей заявки на техническую поддержку инфокоммуникационных систем и/или их составляющих
Необходимые умения	Обрабатывать информацию о ходе выполнения заявок клиентов

	специалистами по технической поддержке с использованием автоматизированных технических средств
	Координировать ход выполнения заявки клиента со специалистами соответствующих технических подразделений организации (специалистами второго уровня технической поддержки)
	Применять автоматизированные системы управления взаимоотношениями с клиентами для контроля выполнения заявок клиентов специалистами по технической поддержке инфокоммуникационных систем и/или их составляющих
	Использовать все доступные способы информирования клиентов (телефон, факс, СМС, электронную почту)
Необходимые знания	Регламенты обработки обращений в структурное подразделение технической поддержки
	Программное обеспечение для регистрации и обработки заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих
	Регламенты взаимодействия сотрудников структурного подразделения технической поддержки с другими структурными подразделениями организации
	Методы объективного и субъективного контроля
	Основы инфокоммуникационных технологий
	Основы менеджмента
	Основы делопроизводства
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
Другие характеристики	-

3.2.3. Трудовая функция

Наименование	Обработка информации о работе специалистов с обращениями клиентов по вопросам технической поддержки инфокоммуникационных систем и/или их составляющих	Код	B/03.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Сбор информации о работе с обращениями клиентов по вопросам технической поддержки инфокоммуникационных систем и/или их составляющих
	Документирование обращений клиентов по вопросам технической поддержки инфокоммуникационных систем и/или их составляющих
	Обобщение поступивших обращений клиентов на техническую поддержку инфокоммуникационных систем и/или их составляющих и последовательности их выполнения сотрудниками структурного подразделения технической поддержки
	Передача обобщенных сведений о поступающих от клиентов обращениях на техническую поддержку инфокоммуникационных систем

	и/или их составляющих соответствующим структурным подразделениям организации
	Подготовка рекомендаций по координации работ по выполнению поступающих от клиентов обращений на техническую поддержку инфокоммуникационных систем и/или их составляющих
Необходимые умения	Координировать решение обращений клиентов со специалистами соответствующих технических подразделений организации (специалистами второго уровня технической поддержки)
	Обрабатывать информацию о работе специалистов с обращениями клиентов по вопросам технической поддержки инфокоммуникационных систем и/или их составляющих с использованием автоматизированных технических средств
	Применять автоматизированные системы управления взаимоотношениями с клиентами для обработки информации о работе специалистов с обращениями клиентов по вопросам технической поддержки инфокоммуникационных систем и/или их составляющих
	Готовить материалы для выработки рекомендаций по координации работ на выполнение заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих соответствующими подразделениями организации
Необходимые знания	Регламенты обработки обращений в структурное подразделение технической поддержки
	Регламенты взаимодействия сотрудников структурного подразделения технической поддержки с другими структурными подразделениями организации
	Организационная структура организации
	Основы делопроизводства
	Правила ведения базы данных клиентов
	Правила ведения базы данных заявок клиентов на оказание технической поддержки
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
Другие характеристики	-

3.3. Обобщенная трудовая функция

Наименование	Код	Уровень квалификации
Устранение, по обращениям клиентов, возникших у клиента проблем при установке и эксплуатации аппаратного, программного и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих	C	6

Происхождение обобщенной трудовой функции				
Оригинал	X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования	Специалист второй линии технической поддержки Ведущий специалист по технической поддержке

должностей	Эксперт по поставляемому оборудованию

Требования к образованию и обучению	Высшее образование – бакалавриат или Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области маркетинга, менеджмента, экономики, новых инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее шести месяцев работы в области технической поддержки инфокоммуникационных систем при среднем профессиональном образовании
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
	3122	Техники и операторы по обслуживанию компьютерных устройств
	3132	Техники и операторы аппаратуры для радио-телевещания и телесвязи
ЕКС	-	-
ОКПДТР	27099	Техник-программист
	22824	Инженер-программист
	22870	Инженер электросвязи
ОКСО	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.3.1. Трудовая функция

Наименование	Консультирование клиентов по согласованным с соответствующими структурными подразделениями организации-поставщика срокам проведения работ по монтажу, пуску и наладке аппаратного, программного, и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих	Код	C/01.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Проведение консультаций по обращениям клиентов о сроках выполнения работ со структурными подразделениями, выполняющими монтажные и пусконаладочные работы аппаратного, программного, и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих
	Согласование работ по обращениям клиентов со структурными подразделениями, выполняющими монтажные и пусконаладочные работы аппаратного, программного, и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих
	Информирование клиента о согласованных сроках выполнения монтажных и пусконаладочных работ и/или их изменении
Необходимые умения	Анализировать поступающие от клиентов обращения по уточнению сроков выполнения монтажных и пусконаладочных работ
	Объяснять возникшую проблему сотрудникам структурных подразделений, выполняющих монтажные и пусконаладочные работы
	Обрабатывать информацию о ходе согласования и уточнения сроков выполнения монтажных и пусконаладочных работ с использованием автоматизированных средств управления взаимодействиями с клиентами
	Использовать все доступные способы информирования клиентов (телефон, факс, СМС, электронную почту)
Необходимые знания	Технические характеристики поддерживаемых инфокоммуникационных систем и/или их составляющих на уровне эксперта
	Архитектура поддерживаемых инфокоммуникационных систем и/или их составляющих на уровне эксперта
	Организационная структура организации
	Регламенты взаимодействия сотрудников структурного подразделения технической поддержки с другими структурными подразделениями организации
	Правила ведения деловой переписки
	Правила ведения деловых переговоров
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
Другие характеристики	-

3.3.2. Трудовая функция

Наименование	Устранение проблемных ситуаций, возникших у клиента при первичном конфигурировании аппаратного, программного и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих, в рамках компетенций, делегированных клиенту (дистанционно и/или на месте)	Код	C/02.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Оказание помощи клиенту по устранению проблемных ситуаций при первичном конфигурировании аппаратных средств, поддерживаемых инфокоммуникационных систем и/или их составляющих
	Оказание помощи клиенту по устранению проблемных ситуаций при первичном конфигурировании аппаратно-программных средств, поддерживаемых инфокоммуникационных систем и/или их составляющих
	Оказание помощи клиенту по устранению проблемных ситуаций при первичном конфигурировании программных средств, поддерживаемых инфокоммуникационных систем и/или их составляющих
	Обучение клиентов первичному конфигурированию поддерживаемых инфокоммуникационных систем и/или их составляющих в рамках делегируемых клиенту полномочий
Необходимые умения	Настраивать универсальные операционные системы, используемые в поддерживаемом оборудовании
	Настраивать специализированные операционные системы, используемые в поддерживаемом оборудовании
	Настраивать прикладное программное обеспечение, используемое в поддерживаемом оборудовании
	Настраивать поддерживаемые абонентские оконечные устройства клиентов
	Обрабатывать информацию о ходе устранения проблемных ситуаций, возникших у клиента при первичном конфигурировании инфокоммуникационной системы/или ее составляющих, с использованием автоматизированных средств управления взаимодействиями с клиентами
Необходимые знания	Инструкции по установке поддерживаемых инфокоммуникационных систем и/или их составляющих
	Инструкции по конфигурированию поддерживаемых инфокоммуникационных систем и/или их составляющих
	Руководства инженера, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Руководства пользователя, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Технические характеристики и архитектура поддерживаемых инфокоммуникационных систем и/или их составляющих
	Операционные системы, используемые в поддерживаемых инфокоммуникационных систем и/или их составляющих
	Языки программирования, используемые в поддерживаемых инфокоммуникационных систем и/или их составляющих
	Регламенты взаимодействия сотрудников структурного подразделения технической поддержки с другими структурными подразделениями организации
	Требования охраны труда при работе с поддерживаемыми инфокоммуникационными системами и/или их составляющими
Другие характеристики	-

3.3.3. Трудовая функция

Наименование	Устранение возникшей у клиента в ходе эксплуатации проблемы на аппаратном, программном и программно-аппаратном обеспечении инфокоммуникационных системах и/или их составляющих	Код	C/03.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Анализ переданной специалистом первой линии технической поддержки заявки, поступившей от клиента на устранение проблемной ситуации, возникшей в ходе эксплуатации аппаратного, программного и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих
	Детальное обсуждение с ответственным представителем клиента возникшей проблемы
	Проверка состояния аппаратного, программного и программно-аппаратного обеспечения инфокоммуникационных систем и/или их составляющих (дистанционно или с выездом на место установки инфокоммуникационной системы)
	Поиск возникшей проблемы по данным, полученным от клиента
	Устранение возникшей в ходе эксплуатации проблемы на аппаратном, программном, и программно-аппаратном обеспечении инфокоммуникационных системы и/или их составляющих
	Документирование результатов выполнения заявки совместно с ответственным представителем клиента
	Сбор данных о количестве отказов оборудования и их причинах
	Документирование данных о количестве отказов оборудования и их причинах
Необходимые умения	Настраивать общесистемные операционные системы, используемые в поддерживаемом оборудовании
	Настраивать специализированные операционные системы, используемые в поддерживаемом оборудовании
	Настраивать прикладное программное обеспечение, используемое в поддерживаемом оборудовании
	Настраивать абонентские оконечные устройства клиентов
	Объяснять клиенту правила эксплуатации поддерживаемых инфокоммуникационных систем и/или их составляющих
	Обрабатывать информацию о ходе устранения возникшей у клиента проблемы с использованием автоматизированных средств управления взаимодействиями с клиентами
Необходимые знания	Инструкции по установке поддерживаемых инфокоммуникационных систем и/или их составляющих
	Инструкции по конфигурированию поддерживаемых инфокоммуникационных систем и/или их составляющих
	Руководства инженера, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих

	Руководства пользователя, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Технические характеристики и архитектура поддерживаемых инфокоммуникационных систем и/или их составляющих
	Операционные системы, используемые в поддерживаемых инфокоммуникационных системах и/или их составляющих
	Языки программирования, используемые в поддерживаемых инфокоммуникационных системах и/или их составляющих
	Правила технической эксплуатации поддерживаемых инфокоммуникационных систем и/или их составляющих
	Регламенты взаимодействия сотрудников технической поддержки с другими структурными подразделениями организации
	Основы делопроизводства
	Требования охраны труда при работе с поддерживаемыми инфокоммуникационными системами и/или их составляющими
Другие характеристики	-

3.4. Обобщенная трудовая функция

Наименование	Руководство группой специалистов по выполнению заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих	Код	D	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Ведущий специалист по технической поддержке Руководитель группы технической поддержки

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области компьютерных и телекоммуникационных технологий
Требования к опыту практической работы	Не менее одного года работы в структурном подразделении технической поддержки
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем

	2144	Инженеры-электроники, инженеры по связи и приборостроению
ЕКС	-	-
ОКПДТР	22824	Инженер-программист
	22870	Инженер электросвязи
	26151	Руководитель группы (специализированной в прочих отраслях)
ОКСО	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.4.1. Трудовая функция

Наименование	Организация работы группы специалистов структурного подразделения технической поддержки по выполнению заявки клиентов на техническую поддержку инфокоммуникационных систем и/или их составляющих	Код	D/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Назначение ответственных за выполнение работ по выполнению заявки клиента на оказание технической поддержки инфокоммуникационных систем и/или их составляющих
	Назначение сроков выполнения работ каждому ответственному исполнителю
	Утверждение плана работ по выполнению заявки клиента на оказание технической поддержки инфокоммуникационных систем и/или их составляющих
	Консультирование специалистов при решении особо сложных проблем, возникших при эксплуатации инфокоммуникационных систем
	Оказание практической помощи специалистам при решении особо сложных проблем, возникших при эксплуатации инфокоммуникационных систем
	Координация работ по выполнению наиболее сложных заявок на техническую поддержку с представителями организаций – производителей (разработчиков) инфокоммуникационных систем и/или их составляющих
Необходимые умения	Руководить проектами по внедрению новых методов и моделей организации процессов технической поддержки
	Организовывать и координировать деятельность подчиненных сотрудников при выполнении заявок клиентов на техническую поддержку инфокоммуникационных систем и/или их составляющих
	Вести деловые переговоры с представителями клиентов и представителями организаций – производителей (разработчиков) поддерживаемых инфокоммуникационных систем и/или их составляющих

	Вести деловую переписку с представителями клиентов и представителями организаций – производителей (разработчиков) поддерживаемых инфокоммуникационных систем и/или их составляющих
	Обрабатывать информацию о ходе выполнения заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих группой специалистов с использованием технических средств автоматизации управления бизнес-процессами
Необходимые знания	Инструкции по установке поддерживаемых инфокоммуникационных систем и/или их составляющих
	Инструкции по конфигурированию поддерживаемых инфокоммуникационных систем и/или их составляющих
	Руководства инженера, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Руководства пользователя, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Технические характеристики и архитектура поддерживаемых инфокоммуникационных систем и/или их составляющих
	Правила технической эксплуатации поддерживаемых инфокоммуникационных систем и/или их составляющих
	Организационная структура организации
	Регламенты взаимодействия сотрудников технической поддержки с другими структурными подразделениями организации
	Регламенты взаимодействия сотрудников технической поддержки с представителями организаций – производителей (разработчиков) поддерживаемых инфокоммуникационных систем и/или их составляющих
	Основы менеджмента
	Основы психологии
	Правила ведения деловых переговоров
	Правила ведения деловой переписки
	Требования охраны труда при работе с поддерживаемыми инфокоммуникационными системами и/или их составляющими
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
Другие характеристики	-

3.4.2. Трудовая функция

Наименование	Контроль качества выполненных работ группой специалистов по реализации заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих	Код	D/02.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Отслеживание выполнения работ по заявкам на техническую поддержку инфокоммуникационных систем и/или их составляющих
	Документирование работ по выполнению заявок клиентов сотрудниками структурного подразделения технической поддержки
	Подготовка аналитических отчетов по выполнению заявок клиентов сотрудниками структурного подразделения технической поддержки
	Передача обобщенных данных по выполнению заявок клиентов на оказание технической поддержки в соответствующие административные и технические структурные подразделения
	Подготовка предложений по оптимизации работы структурного подразделения технической поддержки
Необходимые умения	Оценивать качество выполнения группой специалистов и каждым специалистом в отдельности работ по реализации заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих
	Готовить материалы к аналитическим отчетам в соответствии с действующими в организации регламентами
	Работать с базами данных по заявкам клиентов на выполнение сложных работ группой специалистов структурного подразделения технической поддержки
	Вести деловые переговоры с клиентами о ходе и качестве выполнения группой специалистов работ по реализации заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих
	Вести деловую переписку с клиентами о ходе и качестве выполнения группой специалистов работ по реализации заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих
	Обрабатывать информацию о качестве выполнения группой специалистов заявок на техническую поддержку инфокоммуникационных систем и/или их составляющих с использованием технических средств автоматизации бизнес-процессов
Необходимые знания	Инструкции по установке поддерживаемых инфокоммуникационных систем и/или их составляющих
	Инструкции по конфигурированию поддерживаемых инфокоммуникационных систем и/или их составляющих
	Руководства инженера, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Руководства пользователя, предоставленные разработчиками поддерживаемых инфокоммуникационных систем и/или их составляющих
	Технические характеристики и архитектура поддерживаемых инфокоммуникационных систем и/или их составляющих
	Правила технической эксплуатации поддерживаемых инфокоммуникационных систем и/или их составляющих
	Методы объективного и субъективного контроля
	Организационная структура организации
	Регламенты взаимодействия сотрудников структурного подразделения технической поддержки с другими структурными подразделениями организации
	Основы делового этикета
	Основы менеджмента

	Основы делопроизводства
	Требования охраны труда при работе с поддерживаемыми инфокоммуникационными системами и/или их составляющими
	Отраслевые и локальные нормативно-правовые акты, действующие в организации
Другие характеристики	-

Приложение 5. Типовые требования к виду профессиональной деятельности «Специалист по информационной безопасности информационно-коммуникационных систем»

I. Общие сведения

Защита информационно-коммуникационных (инфокоммуникационных) систем организации и оконечных устройств сотрудников

(наименование вида профессиональной деятельности)

Основная цель вида профессиональной деятельности:

Обеспечение безопасности обрабатываемой информации, оборудования и среды передачи информации между объектами в инфокоммуникационных системах[1]

Группа занятий:

2131	Разработчики и аналитики компьютерных систем	3122	Техники и операторы по обслуживанию компьютерных устройств
2144	Инженеры-электроники, инженеры по связи и приборостроению	3132	Техники и операторы аппаратуры для радио-, телевещания и телесвязи
(код ОКЗ)	(наименование)	(код ОКЗ)	(наименование)

Отнесение к видам экономической деятельности:

64.20.7	Прочая деятельность в области электросвязи
72.60	Прочая деятельность, связанная с использованием вычислительной техники и информационных технологий
(код ОКВЭД)	(наименование вида экономической деятельности)

II. Описание трудовых функций, входящих в профессиональный стандарт (функциональная карта вида трудовой деятельности)

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Эксплуатация инфокоммуникационных систем с применением методов и средств обеспечения их безопасности	6	Обеспечение информационной безопасности в инфокоммуникационных системах с применением программно-аппаратных средств	A/01.6	6
			Обеспечение информационной безопасности в инфокоммуникационных системах с применением инженерно-технических средств	A/02.6	6
			Обеспечение информационной безопасности в инфокоммуникационных системах с комплексным применением программно-аппаратных и инженерно-технических средств	A/03.6	6
B	Администрирование программно-аппаратных средств защиты информации в инфокоммуникационных системах	6	Настройка программно-аппаратных средств защиты инфокоммуникационных систем	B/01.6	6
			Выполнение регламентов технического обслуживания и текущего ремонта аппаратно-программных средств защиты информации	B/02.6	6
			Анализ нарушений, допускаемых пользователями в инфокоммуникационных системах	B/03.6	6
C	Проведение работ по	7	Проведение контрольных проверок	C/01.7	7

	оценке безопасности инфокоммуникационных систем		работоспособности и эффективности применяемых программно-аппаратных средств защиты информации		
			Применение методов и методик оценки безопасности инфокоммуникационных систем при контрольном анализе системы защиты	C/02.7	7
			Проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности инфокоммуникационной системы	C/03.7	7
			Инструментальный мониторинг защищенности инфокоммуникационных систем	C/04.7	7
			Проведение экспертизы при расследовании инфокоммуникационных преступлений, правонарушений и инцидентов	C/05.7	7
D	Создание распределенных защищенных инфокоммуникационных систем	7	Разработка требований к распределенным защищенным инфокоммуникационным системам и средствам защиты для них с учетом действующих нормативных и методических документов	D/01.7	7
			Проектирование распределенных защищенных инфокоммуникационных систем	D/02.7	7
			Ввод в эксплуатацию и сопровождение распределенных инфокоммуникационных систем с использованием комплексов средств защиты информации и организационно-	D/03.7	7

			технических мероприятий по информационной безопасности		

III. Характеристика обобщенных трудовых функций

3.1. Обобщенная трудовая функция

Наименование	Эксплуатация инфокоммуникационных систем с применением методов и средств обеспечения их безопасности	Код	A	Уровень квалификации	6

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Техник по защите инфокоммуникационных систем Старший техник по защите инфокоммуникационных систем Инженер по информационной безопасности инфокоммуникационных систем

Требования к образованию и обучению	Высшее образование – бакалавриат или Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее шести месяцев работы в области технической поддержки, администрирования, программирования устройств инфокоммуникационных систем при среднем профессиональном (техническом) образовании
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
	3122	Техники и операторы по обслуживанию компьютерных устройств
	3132	Техники и операторы аппаратуры для радио-, телевещания и телесвязи
ЕКС	-	-
ОКПДТР	22567	Инженер по защите информации
	27032	Техник по защите информации
ОКСО	220600	Организация и технология защиты

		информации
	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.1.1. Трудовая функция

Наименование	Обеспечение информационной безопасности в инфокоммуникационных системах с применением программно-аппаратных средств	Код	A/01.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Установка программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах
	Настройка программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах
	Техническая поддержка программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах
Необходимые умения	Применять программно-аппаратные средства обеспечения информационной безопасности в системах
	Осуществлять техническое обслуживание программно-аппаратных средств обеспечения информационной безопасности
	Осуществлять текущий ремонт программно-аппаратных средств обеспечения информационной безопасности
	Проводить мониторинг эффективности программно-аппаратных средств обеспечения информационной безопасности
	Обеспечивать учет, хранение и передачу носителей с конфиденциальной информацией, не составляющей государственную тайну, и средств защиты
Необходимые знания	Понятие информационной безопасности
	Основные характеристики составляющих информационной безопасности
	Источники угроз информационной безопасности
	Меры по предотвращению угроз информационной безопасности
	Методы и средства хранения информации
	Программно-аппаратные средства обеспечения информационной безопасности
	Способы обеспечения информационной безопасности

	Основы организации учета носителей информации с грифами конфиденциальной информации, не составляющей государственную тайну
Другие характеристики	-

3.1.2. Трудовая функция

Наименование	Обеспечение информационной безопасности в инфокоммуникационных системах с применением инженерно-технических средств	Код	A/02.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Установка инженерно-технических средств обеспечения информационной безопасности инфокоммуникационных систем
	Настройка инженерно-технических средств обеспечения информационной безопасности инфокоммуникационных систем
	Техническая поддержка инженерно-технических средств обеспечения информационной безопасности инфокоммуникационных систем
Необходимые умения	Эксплуатировать инженерно-технические средства обеспечения информационной безопасности
	Проводить мониторинг эффективности инженерно-технических средств обеспечения информационной безопасности в инфокоммуникационных системах
	Осуществлять текущий ремонт инженерно-технических средств обеспечения информационной безопасности
Необходимые знания	Понятие информационной безопасности
	Основные характеристики составляющих информационной безопасности
	Источники угроз информационной безопасности
	Меры по предотвращению угроз информационной безопасности
	Инженерно-технические средства обеспечения информационной безопасности в инфокоммуникационных системах
	Способы обеспечения информационной безопасности в инфокоммуникационных системах
Другие характеристики	-

3.1.3. Трудовая функция

Наименование	Обеспечение информационной безопасности в инфокоммуникационных системах с комплексным применением программно-аппаратных и инженерно-технических средств	Код	A/03.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Контроль технического состояния комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах
	Настройка комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах
	Проведение технического обслуживания комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах
	Устранение отказов и восстановление работоспособности комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах
	Документирование отказов в работе комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах
Необходимые умения	Выполнять работы по администрированию подсистем безопасности инфокоммуникационных систем
	Производить установку и адаптацию компонентов подсистем безопасности инфокоммуникационных систем
	Выявлять отказы, возникающие при работе комплексных систем обеспечения информационной безопасности в инфокоммуникационных системах
	Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в инфокоммуникационных системах
Необходимые знания	Архитектуры защищенных инфокоммуникационных систем, операционных систем и сред
	Принципы работы защищенных инфокоммуникационных систем, операционных систем и сред
	Особенности применения программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности в операционных системах, базах данных, инфокоммуникационных сетях
	Источники угроз информационной безопасности
	Меры по предотвращению угроз информационной безопасности
	Основы делопроизводства

Другие характеристики	-

3.2. Обобщенная трудовая функция

Наименование	Администрирование программно-аппаратных средств защиты информации в инфокоммуникационных системах	Код	B	Уровень квалификации	6

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Инженер по информационной безопасности инфокоммуникационных систем Администратор по информационной безопасности инфокоммуникационных систем

Требования к образованию и обучению	Высшее образование – бакалавриат или Среднее профессиональное образование – программы подготовки специалистов среднего звена Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее шести месяцев работы в области технической поддержки, администрирования, программирования устройств инфокоммуникационных систем при среднем профессиональном (техническом) образовании
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
	3122	Техники и операторы по обслуживанию компьютерных устройств
	3132	Техники и операторы аппаратуры для радио-, телевещания и телесвязи
ЕКС	-	-
ОКПДТР	22567	Инженер по защите информации

ОКСО	220600	Организация и технология защиты информации
	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.2.1. Трудовая функция

Наименование	Настройка программно-аппаратных средств защиты инфокоммуникационных систем	Код	B/01.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Определение состава подсистем информационной безопасности
	Настройка подсистем информационной безопасности
	Контроль соответствия параметров подсистем информационной безопасности установленным требованиям
	Установка программного обеспечения, необходимого для администрирования
	Настройка программного обеспечения, необходимого для администрирования
	Формирование политики информационной безопасности организации и контроль выполнения ее требований
	Оценка полноты и качества выполнения сотрудниками организации требований политики безопасности
	Подготовка к аттестации объектов инфокоммуникационных систем на предмет соответствия требованиям по защите инфокоммуникационных систем
Необходимые умения	Анализировать и оценивать угрозы информационной безопасности системы
	Применять защищенные протоколы, межсетевые экраны, средства обнаружения атак и другие средства защиты информации в сетях
	Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
	Формулировать и настраивать политику безопасности основных операционных систем, а также локальных инфокоммуникационных сетей, построенных на их основе
	Анализировать показатели качества сетей и систем связи
	Применять требования по аттестации объектов
Необходимые знания	Требования к составу и характеристикам подсистем защиты информации для различных классов защищенных систем
	Методы практической реализации требований к составу и характеристикам подсистем защиты информации для

	различных классов защищенных систем
	Основные виды методов управления доступом и информационными потоками в инфокоммуникационных системах
	Принципы построения современных операционных систем и особенности их применения для решения задач защиты информации
	Механизмы реализации вредоносных программно-технических и информационных воздействий в инфокоммуникационных системах
	Защитные механизмы и средства обеспечения сетевой безопасности
	Средства и методы предотвращения и обнаружения вторжений
Другие характеристики	-

3.2.2. Трудовая функция

Наименование	Выполнение регламентов технического обслуживания и текущего ремонта аппаратно-программных средств защиты информации	Код	B/02.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Установка аппаратно-программных средств защиты информации
	Настройка аппаратно-программных средств защиты информации
	Эксплуатация аппаратно-программных средств защиты информации
	Обслуживание аппаратно-программных средств защиты информации
	Профилактическая проверка технического состояния и остаточного ресурса оборудования защиты информации, организация профилактических проверок и текущего ремонта
	Составление инструкций по выполнению регламентов технического обслуживания и текущего ремонта аппаратно-программных средств защиты информации
	Определение потребности в технических средствах защиты и контроля
	Ведение эксплуатационной документации аппаратно-программных средств защиты информации
	Ведение технической документации аппаратно-программных средств защиты информации

	Ведение отчетной документации по итогам проведения регламентов технического обслуживания и текущего ремонта аппаратно-программных средств защиты информации
Необходимые умения	Устанавливать аппаратно-программные средства защиты информации
	Настраивать аппаратно-программные средства защиты информации
	Эксплуатировать и обслуживать аппаратно-программные средства защиты информации
	Оценивать остаточный ресурс оборудования защиты информации
	Применять техническую документацию по ремонту средств защиты информации
Необходимые знания	Принципы работы технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты информации
	Правила эксплуатации технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты информации
	Регламенты организации ремонта и технического обслуживания
	Методы измерений, контроля и технических расчетов в области информационной безопасности
	Порядок оформления технической документации по защите информации
	Инструкции по соблюдению режима проведения работ, связанных с обеспечением информационной безопасности
Другие характеристики	-

3.2.3. Трудовая функция

Наименование	Анализ нарушений, допускаемых пользователями в инфокоммуникационных системах	Код	B/03.6	Уровень (подуровень) квалификации	6

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Анализ журналов по доступу к оборудованию, программному обеспечению, средствам защиты
	Выявление случаев нарушений требований безопасности.
	Участие в служебных расследованиях
	Подготовка рекомендаций по устранению нарушений
Необходимые умения	Проверять и оценивать соответствие реальных характеристик программно-аппаратных средств защиты информации характеристикам, заявленным в технической документации на эти средства

	Оценивать выявленные нарушения с точки зрения их актуальности для безопасности
	Готовить и формулировать материалы и выводы служебных расследований
	Использовать техническую документацию и справочники при изучении и освоении программно-аппаратных средств защиты информации
Необходимые знания	Принципы работы программно-аппаратных средств защиты информации
	Правила эксплуатации приобретаемых программно-аппаратных средств защиты информации
	Методы измерений и контроля характеристик программно-аппаратных средств защиты информации
	Систематизация нарушений
Другие характеристики	-

3.3. Обобщенная трудовая функция

Наименование	Проведение работ по оценке безопасности инфокоммуникационных систем	Код	C	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Специалист по безопасности инфокоммуникационных систем Эксперт в области информационной безопасности

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее шести месяцев работы в области защиты информации
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных

		систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
ЕКС	-	-
ОКПДТР	22567	Инженер по защите информации
ОКСО	220600	Организация и технология защиты информации
	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.3.1. Трудовая функция

Наименование	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	Код	C/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Тестирование работоспособности и эффективности применяемых программно-аппаратных средств защиты информации
	Мониторинг эффективности применяемых программно-аппаратных средств защиты информации
	Документирование результатов контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации
Необходимые умения	Оценивать работоспособность и эффективность применяемых программно-аппаратных средств защиты информации
	Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия
	Вести техническую документацию, связанную с проведением контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации
Необходимые знания	Действующие нормативно-правовые акты в части информационной безопасности
	Принципы работы технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты информации
	Правила эксплуатации технических средств получения, обработки, передачи, отображения и хранения информации, аппаратуры контроля, защиты информации

Другие характеристики	-

3.3.2. Трудовая функция

Наименование	Применение методов и методик оценки безопасности инфокоммуникационных систем при контрольном анализе системы защиты	Код	C/02.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Применение типовых методов и методик оценки безопасности инфокоммуникационных систем при контрольном анализе системы защиты
	Разработка обоснований по применению нетиповых методов и методик оценки безопасности инфокоммуникационных систем при контрольном анализе системы защиты
	Применение нетиповых методов и методик оценки безопасности инфокоммуникационных систем при контрольном анализе системы защиты
Необходимые умения	Анализировать инфокоммуникационную систему с целью определения уровня защищенности и доверия
	Разрабатывать профили защиты и формулировать задания по безопасности, формировать политики безопасности инфокоммуникационных систем
	Готовить аналитический отчет по результатам анализа и формулировать предложения по устранению выявленных уязвимостей
	Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа
Необходимые знания	Действующие нормативно-правовые акты в части информационной безопасности
	Модели безопасности инфокоммуникационных систем
	Основные виды политик безопасности инфокоммуникационных систем
	Основные принципы построения защищенных инфокоммуникационных систем
	Основные принципы построения систем обнаружения инфокоммуникационных атак
	Способы обнаружения и нейтрализации последствий вторжений в инфокоммуникационную систему
	Методы проведения расследования инфокоммуникационных инцидентов

	Методы и методики оценки безопасности инфокоммуникационных систем
Другие характеристики	-

3.3.3. Трудовая функция

Наименование	Проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности инфокоммуникационной системы	Код	C/03.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Разработка программ аттестационных испытаний, определяющих порядок, методы, условия и объем проведения аттестационных испытаний объектов на соответствие требованиям по безопасности информации
	Разработка методик аттестационных испытаний, определяющих порядок, методы, условия и объем проведения аттестационных испытаний объектов на соответствие требованиям по безопасности информации
	Применение измерительной техники и аппаратно-программных средств для проведения экспериментально-исследовательских работ
	Подготовка протоколов, отчета и заключения по результатам испытаний
Необходимые умения	Анализировать объекты информатизации и телекоммуникации с целью определения уровня защищенности
	Применять нормативные и правовые акты по аттестации объектов с учетом требований к обеспечению защищенности инфокоммуникационной системы
	Применять измерительную технику и аппаратно-программные средства для проведения экспериментально-исследовательских работ
	Оформлять протоколы, отчеты и заключения по результатам испытаний
Необходимые знания	Основные способы обеспечения защищенности объектов инфокоммуникационных систем
	Основные принципы построения защищенных объектов инфокоммуникационных систем
	Методы и методики оценки безопасности инфокоммуникационных систем

	Порядок применения измерительной техники и аппаратно-программных средств для проведения экспериментально-
	Порядок оформления протоколов, отчетов и заключений по результатам испытаний
Другие характеристики	-

3.3.4. Трудовая функция

Наименование	Инструментальный мониторинг защищенности инфокоммуникационных систем	Код	C/04.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Установка аппаратных средств инструментального мониторинга защищенности инфокоммуникационных систем
	Установка аппаратно-программных средств инструментального мониторинга защищенности инфокоммуникационных систем
	Установка программных средств инструментального мониторинга защищенности инфокоммуникационных систем
	Мониторинг защищенности инфокоммуникационных систем
	Документирование результатов инструментального мониторинга защищенности инфокоммуникационных систем
Необходимые умения	Устанавливать аппаратные средств инструментального мониторинга защищенности администрируемой инфокоммуникационной системы в соответствии с инструкцией по установке
	Устанавливать программные средств инструментального мониторинга защищенности администрируемой инфокоммуникационной системы в соответствии с инструкцией по установке
	Формализовать задачи управления безопасностью инфокоммуникационных систем
	Применять современные инструментальные средства проведения мониторинга защищенности инфокоммуникационных систем
Необходимые знания	Основные принципы построения защищенных распределенных и локальных инфокоммуникационных систем
	Основные принципы построения систем обнаружения инфокоммуникационных атак
	Способы обнаружения последствий вторжений в инфокоммуникационные системы
	Способы нейтрализации последствий вторжений в инфокоммуникационные системы

	Инструкции по установке аппаратных и программных средств инструментального мониторинга защищенности администрируемой инфокоммуникационной системы
Другие характеристики	-

3.3.5. Трудовая функция

Наименование	Проведение экспертизы при расследовании инфокоммуникационных преступлений, правонарушений и инцидентов	Код	C/05.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Криминалистический анализ при расследовании инфокоммуникационных преступлений, правонарушений и инцидентов
	Документирование результатов экспертизы при расследовании инфокоммуникационных преступлений, правонарушений и инцидентов
	Выработка предложений по устранению инфокоммуникационных преступлений, правонарушений, инцидентов, выявленных уязвимостей
Необходимые умения	Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа
	Производить криминалистический анализ
	Прогнозировать возможные пути развития новых видов инфокоммуникационных преступлений, правонарушений и инцидентов
Необходимые знания	Основные уязвимости защищенных инфокоммуникационных систем
	Способы обнаружения последствий вторжений в инфокоммуникационные системы
	Способы нейтрализации последствий вторжений в инфокоммуникационные системы
	Методы и методики проведения расследования инфокоммуникационных преступлений, правонарушений и инцидентов
	Действующие нормативно-правовые акты в области предупреждения и расследования инфокоммуникационных преступлений, правонарушений и инцидентов
Другие характеристики	-

3.4. Обобщенная трудовая функция

Наименование	Создание распределенных защищенных инфокоммуникационных систем	Код	D	Уровень квалификации	7

Происхождение обобщенной трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Возможные наименования должностей	Ведущий специалист по защите информации Главный специалист по защите информации Руководитель проекта по информационной безопасности инфокоммуникационных систем

Требования к образованию и обучению	Высшее образование – специалитет, магистратура Дополнительное профессиональное образование – программы повышения квалификации, программы профессиональной переподготовки в области информационной безопасности инфокоммуникационных систем и/или их составляющих
Требования к опыту практической работы	Не менее одного года работы в области защиты информации
Особые условия допуска к работе	-

Дополнительные характеристики

Наименование документа	Код	Наименование базовой группы, должности (профессии) или специальности
ОКЗ	2131	Разработчики и аналитики компьютерных систем
	2144	Инженеры-электроники, инженеры по связи и приборостроению
ЕКС	-	-
ОКПДТР	20911	Главный специалист по защите информации
	22567	Инженер по защите информации
ОКСО	220600	Организация и технология защиты информации
	210400	Телекоммуникации
	230101	Вычислительные машины, комплексы, системы и сети

3.4.1. Трудовая функция

Наименование	Разработка требований к распределенным защищенным инфокоммуникационным системам и средствам защиты для них с учетом действующих нормативных и методических документов	Код	D/01.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала	Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Определение угроз безопасности, возможных источников и каналов утечки информации
	Выработка решений и мер по обеспечению защиты информации
	Принятие решений и мер по обеспечению защиты информации
	Оценка технико-экономического уровня и эффективности предлагаемых и реализуемых технических решений
Необходимые умения	Подбирать, изучать и обобщать научно-техническую литературу, нормативные и методические материалы по средствам и способам защиты информации
	Разрабатывать модели угроз и модели нарушителя безопасности инфокоммуникационных систем
	Оптимизировать подходы к обеспечению защиты информации инфокоммуникационной системы
	Разрабатывать частные политики безопасности инфокоммуникационных систем, в том числе политики управления доступом и информационными потоками
	Применять отечественные и зарубежные стандарты в области информационной безопасности для оценки защищенности инфокоммуникационной системы
	Применять нормативно-правовые акты в области обеспечения информационной безопасности
Необходимые знания	Нормативно-правовые акты по вопросам, связанным с обеспечением информационной безопасности
	Методы и средства получения, обработки и передачи информации в современных операционных системах, системах управления базами данных и инфокоммуникационных сетях, методы и средства их защиты
	Основные виды атак и механизмы их реализации в инфокоммуникационных системах
	Методы выявления каналов утечки информации и организации технической разведки
	Принципы построения защищенных систем и средств защиты информации инфокоммуникационных систем
	Основные формальные модели управления доступом
	Типовые криптографические протоколы и стандарты
	Порядок сертификации средств защиты информации
	Порядок лицензирования организаций, разрабатывающих средства защиты информации
Другие характеристики	-

3.4.2. Трудовая функция

Наименование	Проектирование распределенных защищенных инфокоммуникационных систем	Код	D/02.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Анализ существующих методов и средств, применяемых для контроля и защиты информации
	Разработка технических заданий на проектирование распределенных защищенных инфокоммуникационных систем
	Разработка планов и графиков проведения работ по проектированию распределенных защищенных инфокоммуникационных систем
	Разработка эскизных проектов распределенных защищенных инфокоммуникационных систем
	Разработка технических проектов распределенных защищенных инфокоммуникационных систем
	Разработка рабочих проектов распределенных защищенных инфокоммуникационных систем
	Разработка программ и методик испытаний распределенных защищенных инфокоммуникационных систем
	Оценка технико-экономического уровня и эффективности предлагаемых и реализуемых технических решений
	Направление на экспертизу и рассмотрение результатов проектирования распределенных защищенных инфокоммуникационных систем
Необходимые умения	Производить исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации
	Применять отечественные и зарубежные стандарты в области информационной безопасности для проектирования средств защиты информации инфокоммуникационной системы
	Создавать и сопровождать архитектуру средств защиты информации
	Подбирать, изучать и обобщать научно-техническую литературу, нормативные и методические материалы по техническим средствам и способам защиты информации
Необходимые знания	Нормативно-правовые акты по вопросам, связанным с обеспечением информационной безопасности
	Основные виды атак и механизмы их реализации в инфокоммуникационных системах
	Методы и средства получения, обработки и передачи информации в современных операционных системах, системах управления базами данных и инфокоммуникационных сетях, методы и средства их защиты

	Принципы построения систем защиты информации инфокоммуникационных систем
	Основные формальные модели управления доступом
	Принципы и методы проектирования программно-аппаратного обеспечения, технологии разработки программного обеспечения
Другие характеристики	-

3.4.3. Трудовая функция

Наименование	Ввод в эксплуатацию и сопровождение распределенных инфокоммуникационных систем с использованием комплексов средств защиты информации и организационно-технических мероприятий по информационной безопасности	Код	D/03.7	Уровень (подуровень) квалификации	7

Происхождение трудовой функции	Оригинал X	Заимствовано из оригинала		
			Код оригинала	Регистрационный номер профессионального стандарта

Трудовые действия	Контроль соответствия параметров подсистем информационной безопасности установленным требованиям
	Установка программного обеспечения, необходимого для администрирования
	Настройка программного обеспечения, необходимого для администрирования распределенных инфокоммуникационных систем
	Применение программно-аппаратных средств обеспечения информационной безопасности в инфокоммуникационных системах
	Применение инженерно-технических средств обеспечения информационной безопасности защищенных инфокоммуникационных систем
	Проведение аттестации на предмет соответствия требованиям по защите инфокоммуникационных систем
	Проверка технического состояния и остаточного ресурса оборудования защиты информации
	Организация профилактических проверок состояния и остаточного ресурса оборудования защиты информации
	Организация текущего ремонта оборудования защиты информации
	Определение потребности в технических средствах защиты и контроля
	Инструментальный мониторинг защищенности инфокоммуникационных систем

	Подготовка аналитических отчетов по результатам анализа инфокоммуникационных преступлений, правонарушений, инцидентов, выявленных уязвимостей
	Выработка предложений по устранению инфокоммуникационных преступлений, правонарушений, инцидентов, выявленных уязвимостей
	Определение угроз безопасности, возможных источников и каналов утечки информации
	Выработка решений и мер по обеспечению защиты информации
	Принятие решений и мер по обеспечению защиты информации
Необходимые умения	Руководить техническим обслуживанием и текущим ремонтом программно-аппаратных средств обеспечения информационной безопасности
	Контролировать работы по администрированию подсистем безопасности инфокоммуникационных систем
	Контролировать установку и адаптацию компонентов подсистем безопасности инфокоммуникационных систем
	Анализировать и оценивать угрозы информационной безопасности системы
	Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
	Оценивать полноту и качество выполнения сотрудниками организации требований политики безопасности
	Устанавливать, настраивать, эксплуатировать и обслуживать аппаратно-программные средства защиты информации
	Использовать техническую документацию, техническую литературу и справочники при сопровождении распределенных инфокоммуникационных систем с применением комплексов средств защиты информации и организационно-технических мероприятий по информационной безопасности
	Использовать профили защиты и заданий по безопасности
	Прогнозировать возможные пути развития новых видов инфокоммуникационных преступлений, правонарушений и инцидентов
Необходимые знания	Источники угроз информационной безопасности и меры по их предотвращению
	Современные программно-аппаратные средства и способы обеспечения информационной безопасности
	Современные инженерно-технические средства и способы обеспечения информационной безопасности в инфокоммуникационных системах
	Состав и принципы работы защищенных инфокоммуникационных систем, операционных систем и сред
	Требования к составу и характеристикам подсистем защиты информации для различных классов защищенных систем, методы их практической реализации
	Механизмы реализации вредоносных программно-

	технических и информационных воздействий в инфокоммуникационных системах
	Защитные механизмы и средства обеспечения сетевой безопасности
	Средства и методы предотвращения и обнаружения вторжений
	Содержание и порядок аттестации инфокоммуникационных систем на их соответствие требованиям по защите информации
	Способы организации ремонта и технического обслуживания
	Принципы работы и правила эксплуатации приобретаемых программно-аппаратных средств защиты информации
	Основные принципы построения систем обнаружения инфокоммуникационных атак
	Способы обнаружения и нейтрализации последствий вторжений в инфокоммуникационную систему
	Методы проведения расследования инфокоммуникационных инцидентов
	Основные принципы построения защищенных инфокоммуникационных систем
	Основные принципы построения защищенных объектов, распределенных и локальных инфокоммуникационных систем, их основные уязвимости
	Методы проведения расследования инфокоммуникационных преступлений, правонарушений и инцидентов
	Методы выявления каналов утечки информации и организации технической разведки
	Порядок сертификации средств защиты информации
	Порядок лицензирования организаций, разрабатывающих средства защиты информации
Другие характеристики	-

Приложение 6. Учебно-методическое пособие «Основы построения защищенных информационно-коммуникационных систем на базе системы обнаружения компьютерных атак ФОРПОСТ»

Учебно-методическое пособие «Основы построения защищенных информационно-коммуникационных систем на базе системы обнаружения компьютерных атак ФОРПОСТ» подготовлен Бюро развития электросвязи МСЭ в рамках реализации региональной инициативы Администрации связи Российской Федерации «Укрепление доверия и безопасности при использовании ИКТ», утвержденной Всемирной конференцией по развитию электросвязи 2014 года (г. Дубай, ОАЭ, 30 марта-10 апреля 2014 года) при поддержке ФГБОУ ВО ордена Трудового Красного Знамени «Московский технический университет связи и информатики» (Российская Федерация).
Учебно-методическое пособие рассчитано на студентов высших учебных заведений стран СНГ изучающих вопросы информационной безопасности и защиты информации в современных информационно-коммуникационных системах.

Составители:
Докучаев В.А., Кондратьев М.Г., Крупнов И.А., Маклачкова В.В., Мытенков С.С., Шведов А.В./ Под ред. д.т.н., профессора В.А.Докучаева

Рецензенты:
Новиков А.А. – с.н.с., к.т.н., генеральный директор ЗАО «РНТ»,
Малочинский В.О. – главный специалист по информационной безопасности ФГБОУ ВО МТУСИ.

Назначение СОА «Форпост»

Система обнаружения компьютерных атак (СОА) «Форпост» версии 2.0 (ЗАО «РНТ») предназначена для автоматического выявления воздействий на контролируемую данным средством автоматизированную информационную систему (АИС), которые могут быть классифицированы как компьютерные атаки.
СОА «Форпост» обеспечивает:

- обнаружение компьютерных атак, направленных на сервера телематических служб (WEB, FTP, электронная почта, СУБД и пр.) и рабочие станции, размещенные в контролируемых сегментах АИС;
- предотвращение развития сетевых компьютерных атак путем блокирования источников атак посредством отправки сетевому оборудованию (межсетевому экрану, коммутатору, маршрутизатору), по протоколам RS-232, telnet, соответствующей последовательности команд на основе шаблонов;
- оповещение администратора безопасности об обнаруженных атаках путем вывода соответствующего сообщения на консоль администратора СОА, записи сообщения в специальный журнал, путем отправки сообщений по электронной почте;
- контроль целостности собственных ресурсов СОА и ресурсов защищаемой АИС, а так же, за счет этого механизма, возможность отслеживания действий нарушителей по отношению к контролируемым ресурсам в скомпрометированной системе;

- ведение журнала системных сообщений, содержащего служебную информацию, формируемую компонентами СОА, журнала сообщений от сетевого оборудования, поступающих по протоколам SNMP и syslog;
- удаленное управление сетевым оборудованием по защищенному с использованием отечественных средств криптографической защиты информации (СКЗИ) каналу;
- интеграцию с внешними системами путем передачи сообщений о зафиксированных компьютерных атаках из журнала СОА по протоколу syslog;
- генерацию отчетов на основе содержимого журналов СОА.
- отслеживание появления новых сообщений системных журналов.

Продукт обладает подсистемой собственной безопасности, которая позволяет шифровать передаваемую между компонентами информацию с использованием отечественных СКЗИ, осуществлять контроль целостности собственных ресурсов и ресурсов защищаемой АИС.

Характеристики СОА «Форпост»

В основу функционирования сетевого датчика СОА «Форпост» положен сигнатурный метод выявления компьютерных атак. Он обеспечивает обнаружение атак или эксплуатируемой уязвимости на основе специальных шаблонов (сигнатур), каждый из которых соответствует конкретной атаке. При получении исходных данных о сетевом трафике информационной системы, СОА «Форпост» производит их анализ на соответствие указанным шаблонам атак, имеющимся в базе данных.

В случае обнаружения сигнатуры в исходных данных, система регистрирует факт обнаружения атаки, оповещает администратора безопасности о данном событии и предоставляет возможность администратору произвести блокирование источника атаки с помощью соответствующего коммуникационного оборудования.

За счет использования датчиков контроля целостности СОА позволяет отслеживать действия нарушителя по отношению к контролируемым ресурсам в скомпрометированной системе.

Дополнительно поддерживается получение данных о функционировании отдельных объектов контролируемой АИС по протоколам syslog и SNMP.

СОА «Форпост» реализует следующие методы реагирования на факт выявления компьютерной атаки:

- идентификация компьютерной атаки с использованием описаний уязвимостей, на которые они направлены, или описаний реализаций компьютерных атак;
- оповещение администратора безопасности об обнаруженных атаках путем вывода соответствующего сообщения на консоль администратора СОА, отправки сообщений по электронной почте;
- регистрация атаки в журнале модулей-датчиков СОА;
- блокировка источника угрозы информационной безопасности путем блокирования источников атак посредством отправки сетевому оборудованию (межсетевому экрану, коммутатору, маршрутизатору), по протоколам RS-232, telnet, последовательности команд на основе шаблонов.

Управление сетевым оборудованием производится компонентом СОА через локальный интерфейс RS-232 или через выделенный сетевой интерфейс с использованием протокола telnet. Связь между удаленной консолью администратора и компонентом СОА,

выполняющим управление сетевым оборудованием осуществляется по защищенному с использованием отечественных СКЗИ каналу.

СОА «Форпост» обеспечивает возможность выборочного контроля ресурсов защищаемой АИС, контроль целостности собственных ресурсов (исполняемых и конфигурационных файлов, веток реестра) СОА и ресурсов защищаемой АИС.

СОА «Форпост» выявляет компьютерные атаки на основе анализа сетевого трафика контролируемой АИС на сетевом, транспортном и прикладном уровнях стека протоколов TCP/IP.

СОА «Форпост» имеет консоль администратора, которая реализует механизм удаленного управления данным средством.

Дополнительно система имеет механизм локального управления, позволяющий: производить настройку своих компонентов, их запуск, остановку и перезапуск; формировать, редактировать и подписывать электронной цифровой подписью администратора СОА список контролируемых на целостность ресурсов.

С целью маскирования СОА «Форпост» в составе контролируемой АИС предполагается выделение СОА в отдельный сегмент, если на защищаемых объектах не установлены датчики контроля целостности, или отделение компонентов СОА от возможных нарушителей с помощью межсетевых экранов, исключая точки съема информации сетевыми датчиками.

В качестве дополнительной меры по затруднению демаскирования компонентов СОА предусмотрена возможность наложения ограничений на сетевые адреса, между которыми осуществляется взаимодействие компонентов.

СОА «Форпост» реализует следующие механизмы собственной защиты:

- обеспечивается идентификация и аутентификация администратора СОА при запуске консоли администратора по имени пользователя и паролю; ведется контроль длины создаваемых паролей (не менее 6 символов) и состав паролей (буквенно-цифровые);
- в процессе работы осуществляется контроль целостности компонентов и конфигураций СОА;
- СОА имеет функцию сигнализации администратору СОА о неверных попытках аутентификации при доступе к консоли администратора, в частности, сигнализации о трех подряд неверных попытках аутентификации путем записи соответствующего события в системный журнал и отсылки сообщения электронной почты;
- управляющая информация, служебная информация компонентов и данные о выявленных компьютерных атаках могут передаваться между компонентами в зашифрованном виде с использованием СКЗИ КриптоПро 3.6 по протоколу TLS;
- предусмотрена возможность наложения ограничений на адреса, с которых осуществляется удаленное администрирование СОА.

СОА «Форпост» имеет автоматизированный механизм обновления базы решающих правил, позволяющий загружать сигнатуры компьютерных атак на датчики, с использованием консоли администратора.

Дополнительно имеются штатные средства задания новых сигнатур компьютерных атак с использованием языка описания сигнатур.

СОА «Форпост» регистрирует в своих журналах:

- сведения о выявленных компьютерных атаках и случаях нарушения целостности контролируемых ресурсов;

- служебную информацию, формируемую компонентами СОА, такую как подключение или отключение компонентов СОА, вход и выход администратора СОА в консоль администратора, информацию о блокировке или разблокировке источника атаки и пр.;
- сообщения от сетевого оборудования, поступающие по протоколам SNMP и syslog;
- информацию о появлении новых сообщений системных журналов.

СОА «Форпост» имеет функцию периодического создания резервных копий базы данных СОА в отдельный файл с последующим выводом соответствующего сообщения на консоль администратора СОА.

Дополнительные характеристики СОА «Форпост»:

- может применяться в АИС с производительностью до 6 ГБит/с;
- имеет механизм фильтрации событий, отображаемых в журналах СОА;
- обладает интуитивно-понятным русскоязычным графическим интерфейсом администрирования;
- работает под управлением операционных систем Windows XP/7/8, Windows Server 2003/2008/2012;
- поддерживает интеграцию с внешними системами (например, с различными системами корреляции: Cisco Mars, ArcSight и др.) путем отсылки сообщений о компьютерных атаках из журнала СОА по протоколу syslog;
- имеет возможность генерации табличных и текстовых отчетов на основе содержимого журналов СОА;
- имеет распределенную модульную архитектуру, обеспечивающую масштабируемость системы, позволяющую адаптироваться под требования конкретной АИС по производительности и отказоустойчивости: в зависимости от используемых аппаратных мощностей и настроек СОА может использоваться для мониторинга каналов со скоростью до 6 Гбит/с; существует возможность резервирования ключевых компонентов.

Системные требования

СОА «Форпост» предъявляет следующие минимальные системные требования к аппаратно-программным средствам:

- операционная система для информационного фонда, координационного центра и сетевого датчика – Windows Server 2003/2008/2012, для остальных компонентов – Windows XP/7/8, Windows Server 2003/2008/2012;
- процессор с частотой не менее 1,6 ГГц;
- оперативной памяти не менее 2048 МБ;
- объем свободного дискового пространства не менее 20 ГБ;
- сетевой интерфейс со скоростью не менее 100 Мбит/с;
- на сервере с сетевым датчиком – дополнительно не менее 1 сетевого интерфейса для захвата трафика со скоростью не менее 100 Мбит/с предпочтительно в серверном исполнении.

Поскольку система распределенная, компоненты СОА могут быть установлены как на один сервер, так и распределены на несколько физических серверов.

При повышенных требованиях по производительности рекомендуется:

- на серверах с информационным фондом, координационными центрами, сетевыми датчиками увеличить тактовую частоту процессора и использовать многоядерные, либо многопроцессорные конфигурации; использовать серверные версии операционной системы Windows;
- на серверах с сетевыми датчиками увеличить объем оперативной памяти до 4 ГБ;
- привести объем дискового пространства в соответствие с потребностями информационного фонда по объему единовременно хранимой в системе информации о событиях;
- на серверах с сетевыми датчиками для захвата трафика использовать сетевые интерфейсы со скоростью 1 Гбит/с в серверном исполнении.

Для того, что бы сетевой датчик мог обрабатывать поток трафика со скоростью 1 Гбит/с, число процессорных ядер должно быть не менее 8 шт. Для обработки трафика со скоростью 500 Мбит/с, число процессорных ядер должно быть не менее 4 шт. При использовании нескольких сетевых датчиков на одном физическом сервере технология Hyper-Threading должна быть отключена.

Особенности применения

СОА «Форпост» имеет следующие особенности применения:

- необходимо своевременно проводить техническое обслуживание системы в соответствии с регламентом, описанном в руководстве администратора, РМАГ.00026-22 90 01;
- уведомление администратора о возникновении ситуации, требующей его внимания, возможно через консоль администратора, всплывающее окно, по электронной почте;
- хранение всей накопленной системой информации о процессах в АИС на протяжении достаточно длительных периодов может приводить к уменьшению производительности, что связано с большими объемами данных, обрабатываемых системой, поэтому в ходе эксплуатации СОА «Форпост» необходимо производить периодическое резервное копирование и удаление несущественной информации (одновременно консоль администратора в журнале модулей-датчиков может выводить на экран не более 100 000 записей);
- размер буфера у агентов, в котором они накапливают информацию, полученную от датчиков и подлежащую отправке в координационный центр, фиксированный и информация в нем обновляется циклически (старые события, подлежащие отправке в координационный центр по достижению максимального размера буфера затираются более новыми), что в случае недостаточной пропускной способности канала связи (или каких-либо других факторов) может приводить к потере части данных;
- приложением поддерживается работа с протоколом IPv4 и IPv6.

СОА «Форпост» предъявляет высокие требования к квалификации и компетентности эксплуатирующего персонала, связанные со спецификой предметной области.

Состав и назначение модулей СОА «Форпост»

СОА «Форпост» имеет распределенную многомодульную архитектуру (типовая структура СОА «Форпост» представлена на рисунке 1). Модули могут быть установлены как

на один сервер, так и распределены на несколько в зависимости от требуемых показателей производительности и отказоустойчивости.

Рассмотрим каждый компонент более подробно.

Информационный фонд представляет собой базу данных, работающую под управлением СУБД MS SQL 2005/2008/2012, специальный компонент «Агент БД», и обеспечивает:

- централизованное хранение событий системы;
- централизованное хранение шаблонов датчиков и базы сигнатур СОА.

Компонент «Агент БД» в связке с **CryptoODBC-драйвером** из состава СОА «Форпост» обеспечивает криптографически защищенный с использованием отечественных СКЗИ информационный обмен между информационным фондом и компонентами СОА, которые к нему подключаются (координационный центр, модуль почтовых уведомлений).

Координационный центр является связующим звеном между модулями системы: обеспечивает передачу информации между ними, выполняет функции контроля работоспособности компонентов.

Консоль администратора обеспечивает пользовательский интерфейс и позволяет:

- просматривать текущее состояние компонентов системы;
- производить удаленную установку, настройку и удаление компонентов системы, для которых предусмотрена такая возможность;

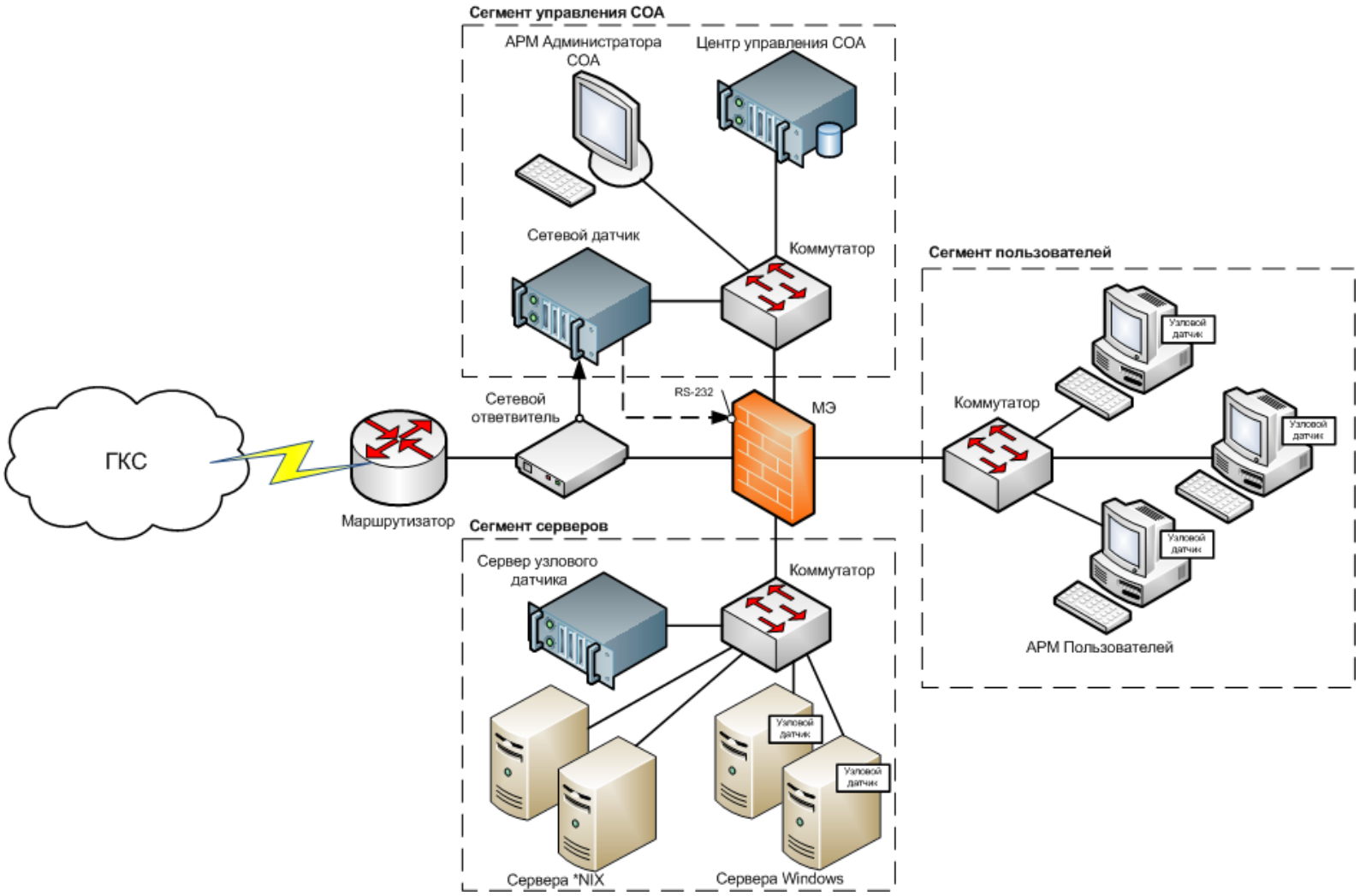


Рис. 1 - Типовая архитектура СОА «Форпост»

- просматривать информацию об обнаруженных атаках и нарушении целостности файлов в журнале модулей-датчиков;
- просматривать системные сообщения, генерируемые компонентами СОА в журнале системных сообщений;
- просматривать в журнале сетевого оборудования сообщения от подключенного к СОА сетевого оборудования;
- просматривать системный журнал, содержащий служебную информацию, формируемую компонентами СОА и информацию об управлении подключенным сетевым оборудованием;
- производить настройку модулей системы;
- производить блокировку источника атаки с помощью сетевого оборудования;
- управлять подключенным к СОА сетевым оборудованием (межсетевые экраны, коммутаторы, маршрутизаторы и т. д.);
- производить выборку ранее произошедших событий с использованием гибкой системы фильтрации;
- генерировать отчёты на основе содержимого журналов СОА.

Модуль интеграции с сетевым оборудованием состоит из следующих функциональных модулей.

Модуль управления сетевым оборудованием – предоставляет возможность посылать команды сетевому оборудованию (коммутаторам, межсетевым экранам и др.) напрямую, либо, на основе шаблонов по протоколам RS-232, telnet, например, с целью блокирования компьютерной атаки в стадии ее развития.

Модуль приема сообщений от сетевых устройств – предоставляет возможность приема SNMP и syslog-сообщений от различных узлов сети (коммутаторы, межсетевые экраны и др.) с последующей их обработкой и выводом в журнал СОА в понятном для пользователя виде.

Модуль интеграции с внешними системами – предоставляет возможность экспорта сообщений, поступающих в журнал датчиков СОА, в различные внешние системы корреляции и мониторинга (такие как Cisco Mars, ArcSight и др.).

Модуль интеграции с сетевым оборудованием предназначен для:

- установления и поддержания подключения к сетевому оборудованию (межсетевые экраны, коммутаторы, маршрутизаторы) по протоколам RS-232, telnet;
- управления сетевым оборудованием (блокировка источников угроз на основе ранее написанных шаблонов, ручное управление);
- получения системных сообщений от сетевого оборудования (по протоколам SNMP и syslog);
- интеграции с внешними системами (например, с различными системами корреляции: Cisco Mars, ArcSight и др.) путем отсылки сообщений о компьютерных атаках из журнала СОА по протоколу syslog.

Модуль почтовых уведомлений позволяет автоматически по электронной почте отправлять заранее заданным адресатам информацию об обнаруженных атаках и событиях, происходящих в системе.

Агент выполняет функции управления датчиками, а также функции обеспечения передачи информации между датчиками и координационным центром. К одному агенту может быть подключен один датчик контроля целостности и несколько сетевых датчиков.

Сетевой датчик осуществляет анализ поступающего трафика на наличие в нем компьютерных атак используя сигнатурный метод; подключается к зеркалирующему (SPAN) порту коммутатора, межсетевого экрана, специализированного ответвителя трафика (TAP) и пр.

Датчик контроля целостности производит контроль целостности собственных ресурсов (исполняемых и конфигурационных файлов, веток реестра) СОА и ресурсов защищаемой АИС. Также датчик контроля целостности отслеживает появление новых сообщений системных журналов.

Взаимодействие компонентов СОА «Форпост» друг с другом происходит по следующей схеме. Главным связующим звеном между компонентами системы является координационный центр, осуществляющий передачу следующей информации между информационным фондом и остальными компонентами:

- данные о зафиксированных событиях (включая результаты работы) и состоянии компонентов;
- шаблоны датчиков и база сигнатур СОА.

Существует возможность резервирования координационного центра (и модуля почтовых уведомлений, который ставится на один сервер с ним).

По умолчанию предполагается, что связь координационных центров с СУБД информационного фонда будет осуществляться с использованием ODBC-драйвера из состава СОА «Форпост» (CryptoODBC-драйвер).

ODBC-драйвер из комплекта поставки операционной системы или СУБД подключается непосредственно к СУБД. ODBC-драйвер из состава СОА «Форпост» (CryptoODBC-драйвер) подключается к СУБД через компонент «Агент БД». Компонент «Агент БД» подключается к СУБД через ODBC-драйвер из комплекта поставки операционной системы или СУБД.

Использование ODBC-драйвера из состава СОА «Форпост» вместо драйвера из комплекта поставки операционной системы или СУБД является обязательным, если предполагается шифрование информационного обмена между координационным центрами и информационным фондом с использованием отечественных криптоалгоритмов.

Допускается использование ODBC-драйвера из комплекта поставки операционной системы или СУБД в случае, если информационный фонд и координационный центр предполагается устанавливать на одном сервере, а так же в случае, если шифрование информационного обмена между координационным центрами и информационным фондом с использованием отечественных криптоалгоритмов не требуется.

Управление датчиками СОА и передача информации между датчиками и координационными центрами осуществляется агентами. Агенты устанавливаются на каждый сетевой узел, на котором установлены любые датчики СОА «Форпост» (сетевой датчик, датчик контроля целостности).

Для обеспечения контроля целостности компонентов СОА «Форпост», датчик контроля целостности устанавливается на каждый сетевой узел, на котором установлены компоненты СОА «Форпост». Дополнительно датчик контроля целостности устанавливается на узлы защищаемой АИС с целью контроля целостности ресурсов защищаемой АИС, возможности отслеживание действий нарушителей по отношению к контролируемым ресурсам в скомпрометированной системе, а также для отслеживания появления новых сообщений системных журналов.

Входными данными сетевого датчика является трафик, снимаемый с зеркалирующего порта коммутатора (межсетевого экрана, специализированного ответвителя трафика (TAP) и др.)

Консоль администратора подключается непосредственно к координационному центру, от которого она получает данные о состоянии компонентов и результаты их работы. С консоли администратора может производиться удаленная установка, удаление, конфигурирование компонентов СОА, управление ими.

Модуль почтовых уведомлений служит для автоматической отправки отчетов по электронной почте и должен подключаться к внешнему почтовому серверу. Данный модуль получает данные непосредственно из информационного фонда, но рассылает только ту информацию, которая была передана от датчиков тем координационным центром, за который установлен данный модуль почтовых уведомлений. Подобный алгоритм работы позволяет исключить дублирование информации, передаваемой по электронной почте от нескольких модулей почтовых уведомлений, установленных на различных координационных центрах.

Функциональность модуля интеграции с сетевым оборудованием интегрирована в агент и координационный центр. Таким образом, существует возможность управлять сетевым оборудованием, подключенным локально к узлам, на которые установлены указанные выше модули СОА.

Логическая структура СОА «Форпост» представлена на рис. 2.

Требования к окружению СОА «Форпост»

Для работы информационного фонда СОА «Форпост» на серверах, предназначенных для его установки, должна быть развернута система управления базами данных (СУБД) MS SQL 2005/2008/2012.

Для использования в подсистеме собственной безопасности СОА «Форпост» отечественных криптоалгоритмов, на все узлы, на которые установлены компоненты СОА, требуется установка внешнего крипропровайдера. В настоящее время поддерживается работа со средством криптографической защиты информации (СКЗИ) КриптоПро CSP 3.6.

Для обеспечения криптографически защищенного (шифрованного) информационного обмена между компонентами СОА «Форпост», а так же для обеспечения работы функции контроля целостности ресурсов, требуется доступ к услугам удостоверяющего центра.

Типовая схема включения СОА в АИС

Типовая схема включения СОА «Форпост» в автоматизированную информационную систему представлена на рисунке 3.

Предполагается, что защищаемая сеть имеет несколько сегментов, разделенных межсетевыми экранами и подключение во внешнюю сеть. Узлы, на которые устанавливаются компоненты СОА «Форпост» (за исключением датчиков контроля целостности) выделяются в отдельный сегмент. Таким образом, в типовой сети имеется три сегмента:

- сегмент серверов;
- сегмент пользователей;
- сегмент СОА «Форпост».

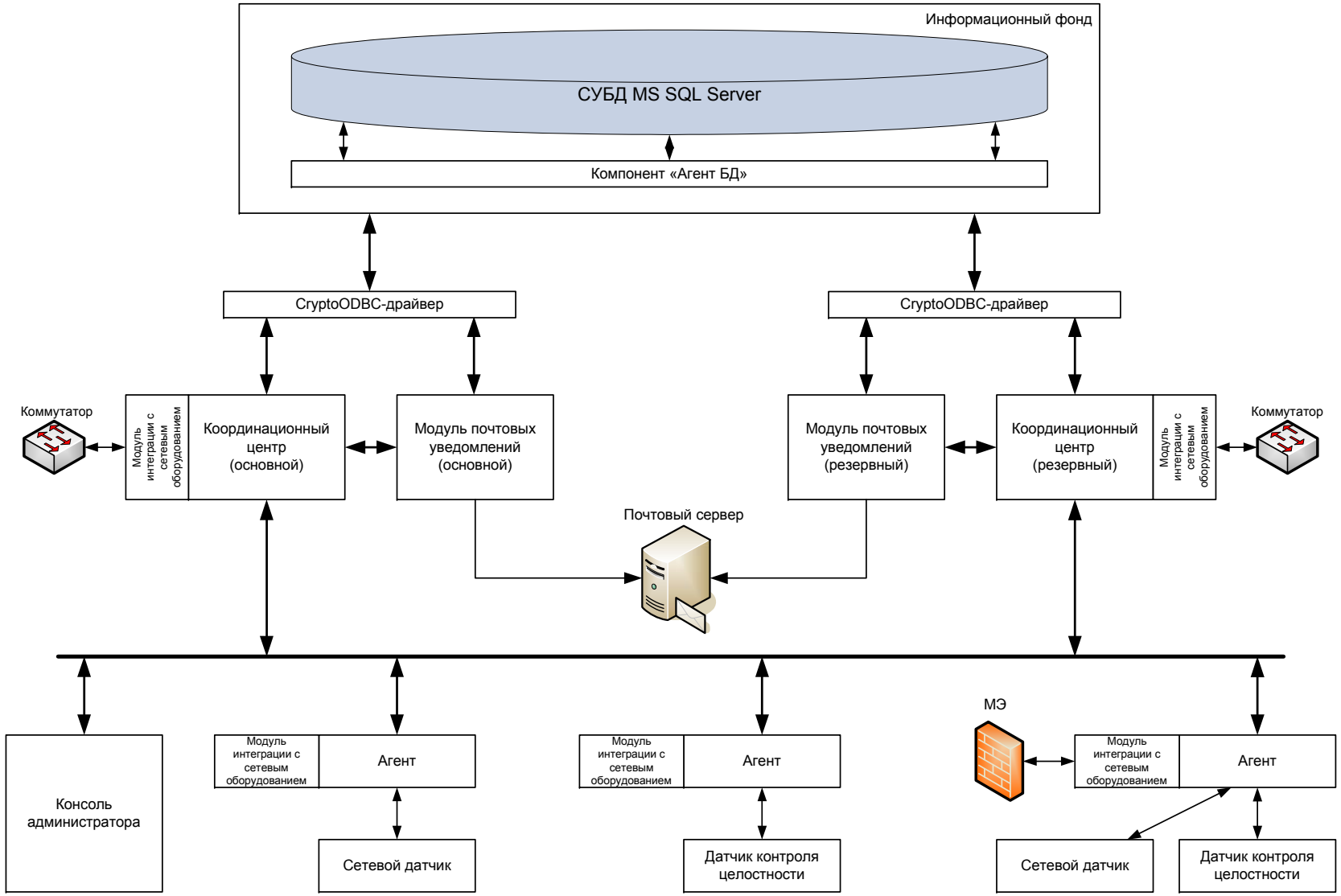


Рисунок 2 – Логическая структура СОА «Форпост»

На сервера и АРМ пользователей защищаемой сети устанавливается датчик контроля целостности СОА «Форпост». Также датчик контроля целостности устанавливается на все узлы, на которых установлены компоненты СОА «Форпост».

В сегменте СОА «Форпост» устанавливаются: информационный фонд, координационные центры (основной и резервный) совместно с модулями почтовых уведомлений (основной и резервный), сетевые датчики. В этом же сегменте должна быть установлена консоль администратора. Данные компоненты могут быть установлены как на один сервер, так и распределены на несколько физических серверов.

Функциональность модуля интеграции с сетевым оборудованием интегрирована в компоненты агент и координационный центр, поэтому управление сетевым оборудованием (модуль управления сетевым оборудованием) возможно с любого узла, на котором установлены компоненты агент и координационный центр. На рисунке 3 предполагается, что управление ведется с узлов, на которые установлен сетевой датчик (агент обязательно устанавливается перед установкой сетевого датчика).

Сбор информации от сетевого оборудования по протоколам SNMP и syslog (модулем приема сообщений от сетевых устройств), взаимодействие с внешними системами по протоколу syslog (модулем интеграции с внешними системами) может вестись с любого узла, на котором установлены компоненты агент и координационный центр (при установке на межсетевом экране соответствующих разрешающих правил).

Необходимо учитывать, что при настройке модуля интеграции с внешними системами на агенте, по протоколу syslog на внешний syslog-сервер передаются только те сообщения, которые генерируются датчиками, расположенными на данном агенте. Аналогичная ситуация происходит при настройке модуля интеграции с внешними системами на координационном центре: на внешний syslog-сервер передаются только те сообщения, которые пересылались через данный координационный центр. Эту особенность необходимо учитывать при реализации схемы резервирования координационного центра.

Координационный центр устанавливается совместно с модулем почтовых уведомлений. Подключение модуля почтовых уведомлений к информационному фонду происходит напрямую минуя координационный центр. Однако каждый модуль почтовых уведомлений отсылает по электронной почте события только того КЦ, на котором он установлен. Это позволяет избавиться от дублирования сообщений от основного и резервного модуля почтовых уведомлений.

Предполагается, что почтовые уведомления будут отсылаться на почтовый сервер, расположенный в сегменте серверов (при установке на межсетевом экране соответствующих разрешающих правил).

В качестве точки включения в АИС (автоматизированную информационную систему) для сетевого датчика могут выступать:

- зеркалирующий порт коммутатора (SPAN-порт) (точки 1 и 2 на рисунке 3); коммутатор при этом настраивается таким образом, чтобы пакеты, поступающие на его порты, копировались в зеркалирующий порт;
- контролирующий порт (Monitor port) специализированного агрегирующего ответвителя трафика (Aggregator Tap) (точка 3 на рисунке 3), который устанавливается «в разрыв» канала связи, подлежащего контролю с помощью сетевого датчика СОА;

- порт сетевого концентратора (hub), который может быть установлен вместо коммутатора, либо «в разрыв» канала связи, подлежащего контролю с помощью сетевого датчика СОА, вместо специализированного агрегирующего ответвителя трафика (Aggregator Tap);
- зеркалирующий порт межсетевого экрана.

Необходимо убедиться, что суммарный пиковый объем трафика, передаваемого через контролируемый сегмент за единицу времени, не превышает пропускной способности сетевого порта, к которому подключен сетевой датчик. В противном случае часть подлежащих анализу данных может быть потеряна.

Установка сетевого датчика
Общие сведения

Узлы, на которые производится установка сетевого датчика, должны быть оснащены минимум двумя сетевыми интерфейсами, при этом «слушающие» интерфейсы должны быть включены, иметь серверное исполнение, и при этом не должны иметь IP-адреса. Сетевой адаптер без IP-адреса подключается к сегменту сети, трафик которой должен анализироваться сетевым датчиком СОА «Форпост». Второй адаптер предназначен для передачи собранной информации координационному центру. Такая схема установки сетевого датчика делает его «невидимым» для возможных нарушителей, что исключает возможность успешной сетевой атаки на сам датчик (рисунок 4).

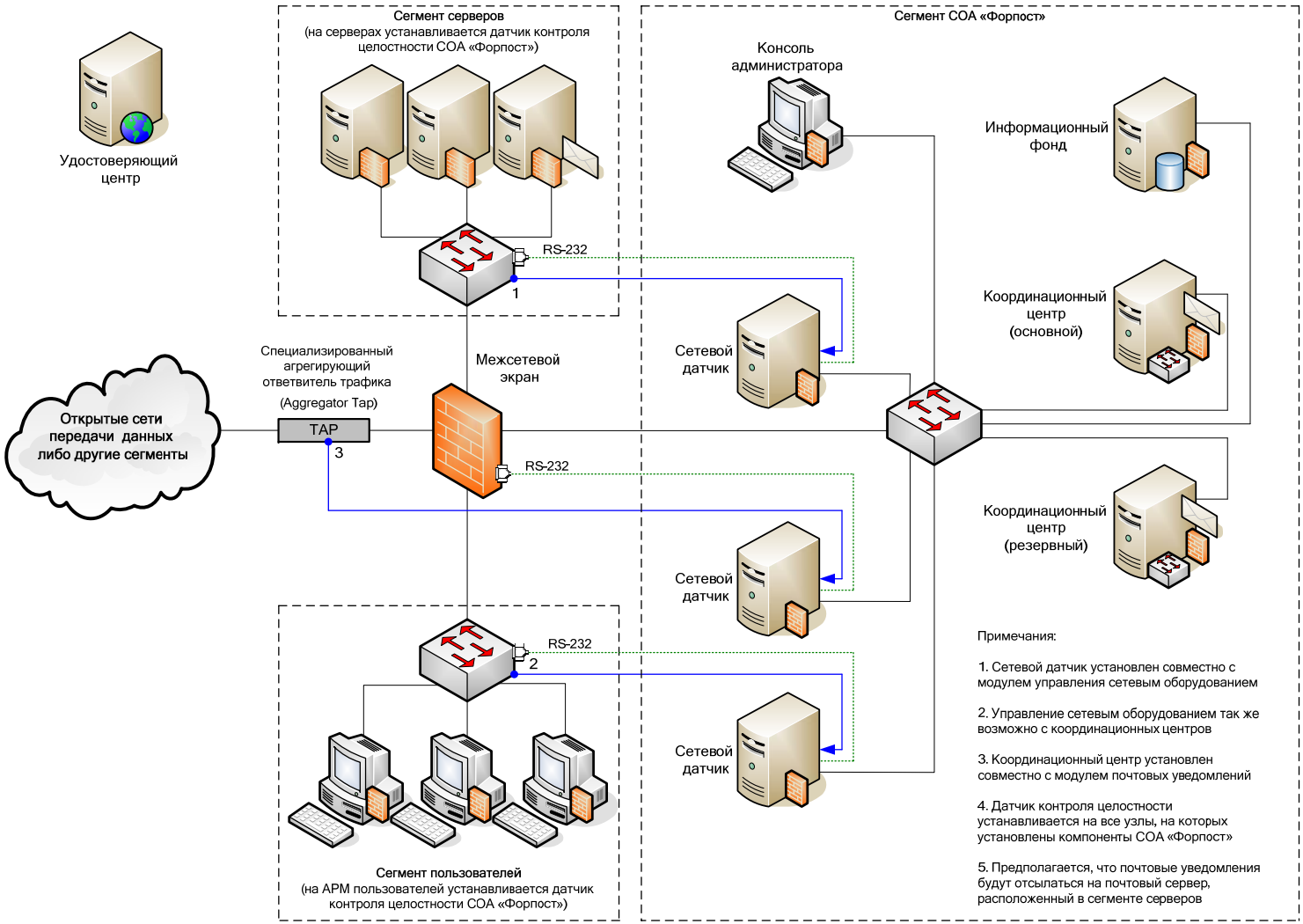


Рисунок 3 – Типовая схема включения СОА «Форпост» в автоматизированную информационную систему

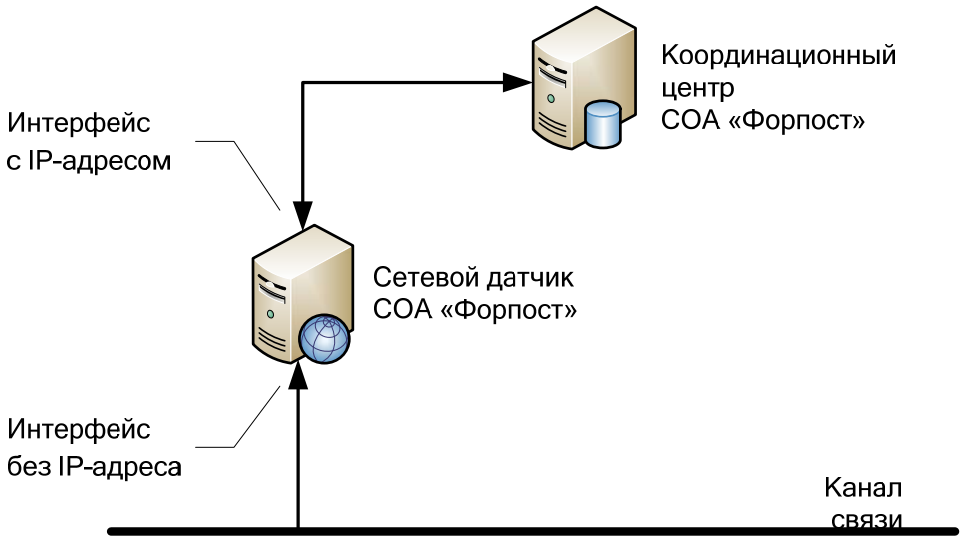


Рисунок 4 - Расположение сетевого датчика

В качестве точки включения в АИС для сетевого датчика могут выступать:

- зеркалирующий порт коммутатора (SPAN-порт); коммутатор при этом настраивается таким образом, чтобы пакеты, поступающие на его порты, копировались в зеркалирующий порт (рисунок 5);
- контролирующий порт (Monitor port) специализированного агрегирующего ответвителя трафика (Aggregator Tap), который устанавливается «в разрыв» канала связи, подлежащего контролю с помощью сетевого датчика СОА (рисунок 6);
- порт сетевого концентратора (hub), который может быть установлен вместо коммутатора (рисунок 5), либо «в разрыв» канала связи, подлежащего контролю с помощью сетевого датчика СОА, вместо специализированного агрегирующего ответвителя трафика (Aggregator Tap) (рисунок 6);
- зеркалирующий порт межсетевого экрана.

При построении системы, содержащей в своем составе сетевые датчики, следует произвести оценку количества трафика, передаваемого через контролируемый сегмент за единицу времени. Полученная величина не должна превышать пропускной способности сетевого порта, к которому подключен сетевой датчик. В противном случае часть подлежащих анализу данных может быть потеряна.

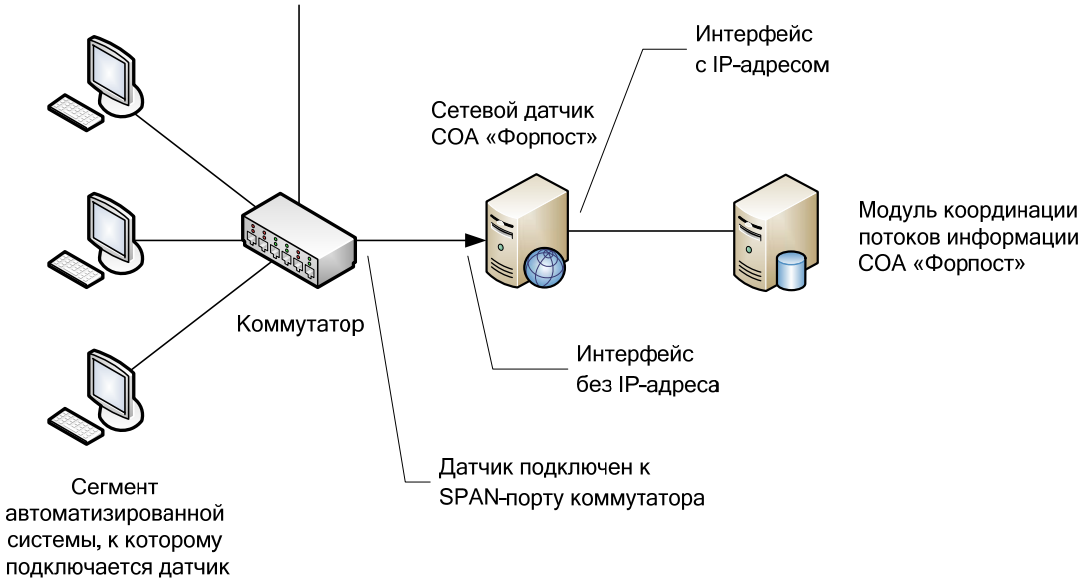


Рисунок 5 - Порт сетевого концентратора, используемый в качестве точки включения в АИС для сетевого датчика

Настройка сетевого датчика

Общие сведения

На схемах для обозначения точки съема информации сетевым датчиком СОА используется условное графические обозначение: TAP.

При построении системы, содержащей в своем составе сетевые датчики, следует произвести оценку количества трафика, передаваемого через контролируемый сегмент за единицу времени. Полученная величина не должна превышать пропускной способности сетевого порта, к которому подключен сетевой датчик. В противном случае часть подлежащих анализу данных может быть потеряна.

Настройка сетевого интерфейса, с которого сетевой датчик получает данные и BPF-фильтра для сетевого датчика производится непосредственно на сервере, на котором установлен сетевой датчик. Настройка параметров сетевого датчика в части анализа сетевого трафика производится в консоли администратора.

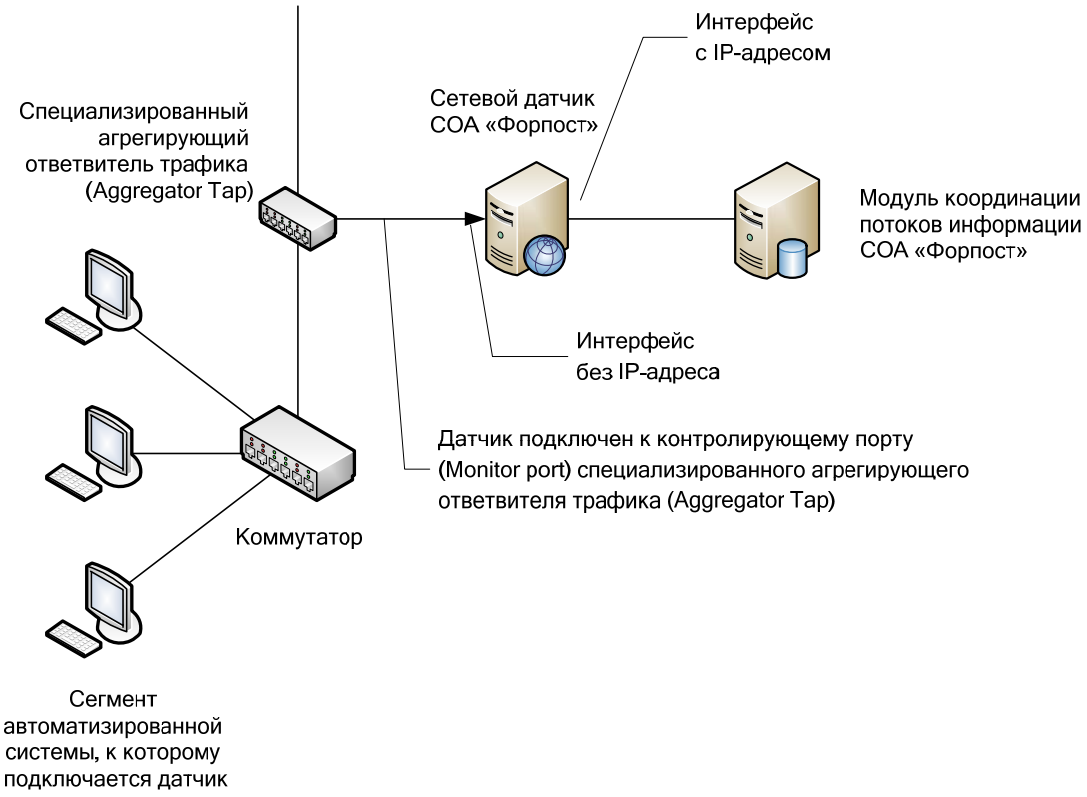


Рисунок 6 - Подключение сетевого датчика к специализированному агрегирующему ответвителю трафика

Настройка балансировки нагрузки на сетевые датчики

Балансировка нагрузки на сетевые датчики может производится двумя методами: автоматически (Сетевой датчик 0.2) и методом наложения на каждый экземпляр сетевого датчика специально сформированного BPF-фильтра (Berkeley Packet Filter) (Сетевой датчик 0.1), таким образом, чтобы каждый экземпляр сетевого датчика обрабатывал только свой небольшой поток трафика от общего потока, поступающего с точки съема информации. Далее будет рассматриваться Сетевой датчик 0.1 с балансировкой с помощью BPF фильтра.

Для того чтобы был охвачен весь поток трафика, поступающий с точки съема информации, целиком, должна работать группа сетевых датчиков (в виде нескольких процессов в рамках одного сервера, либо в рамках нескольких серверов), каждый из которых обрабатывает собственный небольшой поток информации, а все вместе они обрабатывают суммарный поток целиком. BFP-фильтр при этом должен настраиваться соответствующим образом.

Сетевой датчик СОА «Форпост» поддерживает балансировку нагрузки по IP-адресам: с использованием BPF-фильтра из IP-пакета извлекается IP-адрес источника и IP-адрес получателя. По извлеченным значениям BPF-фильтр определяет, должен ли прибывший пакет обрабатываться данным конкретным датчиком. Если должен – пакет передается в ядро сетевого датчика, если не должен – отбрасывается. Отброшенные пакеты BPF-фильтром одного сетевого датчика, должны удовлетворять условиям BPF-фильтра другого сетевого датчика. За счет этого входящий поток информации обрабатывается без потерь.

Производительность одного сетевого датчика СОА зависит от многих факторов. Выделим несколько основных:

- мощность аппаратной платформы;
- количество обрабатываемых пакетов за единицу времени;
- размер обрабатываемых пакетов;

- количество одновременно обрабатываемых TCP-сессий;
- количество и сложность сигнатур, загруженных в сетевой датчик СОА.

В зависимости от этих факторов, которые сами по себе и их сочетание друг с другом зависят от специфики конкретной АИС, производительность одного сетевого датчика СОА может колебаться в диапазоне от 50 до 200 Мбит/с.

Установка датчика контроля целостности

Общие сведения

Датчик контроля целостности, в зависимости от требований конкретной АИС, может (должен) устанавливаться на все узлы, на которых установлены компоненты СОА «Форпост» для контроля их целостности и/или получения сообщений системных журналов.

Датчик контроля целостности из состава СОА «Форпост» может использоваться как для контроля целостности компонентов защищаемой АИС так и для получения сообщений системных журналов.

Контроль целостности файлов производится, в зависимости от настроек, с заданной периодичностью и (или) при обращении к файлу.

Контроль целостности заданных веток реестра производится с заданной периодичностью.

Получение новых сообщений системных журналов производится либо по истечении определенного промежутка времени либо при получении уведомления от операционной системы о новом системном сообщении. Также производится контроль за изменениями в ветке реестра, в которой хранятся настройки системных журналов

Контроль целостности ресурсов производится после успешного запуска операционной системы. Целостность ресурсов до запуска операционной системы и контроль целостности самого датчика контроля целостности должен проводиться другими средствами (в зависимости от требований конкретной АИС для этих целей может применяться контроль целостности, встроенный в аппаратно-программные модули доверенной загрузки (АПМДЗ)).

Настройка датчика контроля целостности

Общие сведения

Датчик контроля целостности осуществляет контроль целостности файлов с заданной периодичностью, либо при обращении какого-либо процесса к ним. Контроль целостности реестра осуществляется с заданной периодичностью. Также датчик контроля целостности способен отслеживать появление сообщений в системных журналах.

Датчик контроля целостности должен устанавливаться на все сетевые узлы, на которые устанавливаются компоненты СОА «Форпост» для контроля их целостности.

Дополнительно с помощью данных датчиков может осуществляться контроль целостности ресурсов защищаемой сети и отслеживание сообщений системных журналов.

При первичной настройке датчик контроля целостности высчитывает контрольные суммы контролируемых файлов и дампов контролируемых веток реестра. Полученные результаты расчетов записываются в файл, располагающийся на узле с установленным датчиком контроля целостности. Затем этот файл подписывается электронно-цифровой подписью (ЭЦП). Подписывание может осуществляться удаленно с консоли администратора, либо локально с использованием оснастки «Управление компонентами Форпост».

Далее, во время работы датчика контроля целостности с помощью ЭЦП проверяется целостность файла, содержащего контрольные суммы. При нарушении целостности этого файла оператор СОА получает соответствующее сообщение. Если целостность этого файла не нарушена, по значениям контрольных сумм, записанным в этом файле, проводится контроль целостности файлов и веток реестра, поставленных на контроль.

Наименование параметра	Описание параметра
Группа «Основные настройки»	
Идентификатор компонента	Уникальный идентификатор компонента
Использовать перехват событий открытия/закрытия файлов	Значение «Да» включает контроль целостности файлов по событию открытия, либо закрытия файла
Интервал проверки файлов, мс	Временной интервал, через который производится проверка файлов на целостность (в миллисекундах)
Название сертификата	Имя сертификата компонента
Тип хранилища сертификатов	Тип хранилища сертификатов, в которое установлен сертификат для компонента. Допускаются следующие значения этого параметра: 1. CERT_SYSTEM_STORE_CURRENT_USER (хранилище текущего пользователя); 2. CERT_SYSTEM_STORE_LOCAL_MACHINE (локальное хранилище узла); 3. CERT_SYSTEM_STORE_CURRENT_SERVICE (хранилище конкретного сервиса); 4. CERT_SYSTEM_STORE_SERVICES (хранилище сервисов). По умолчанию поле имеет значение CERT_SYSTEM_STORE_LOCAL_MACHINE
Криптопровайдер	Название используемого криптопровайдера. Для КриптоПро CSP 3.6 поле имеет значение «Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider»
Алгоритм подсчета контрольных сумм	Используемый алгоритм подсчета контрольных сумм файлов. По умолчанию используется алгоритм «GOST R 34.11-94»
Отслеживание системных сообщений Windows	Включение/Отключение режима отслеживания системных сообщений Windows. По умолчанию выключено.

Список контролируемых журналов	Строка с именами контролируемых журналов, разделенных пробелами или табуляциями. Допустим символ "*", означающий все журналы. По умолчанию установлено значение "*".
Список игнорируемых журналов	Строка с именами игнорируемых журналов, разделенных пробелами или табуляциями. Данный параметр обладает большим приоритетом, чем параметр “Список контролируемых журналов”.

Если включено отслеживание системных журналов, то датчик контроля целостности считывает из реестра доступные системные журналы. После этого датчик начинает отслеживать появление новых событий для данного журнала.

В течение всего времени работы датчика происходит постоянный контроль за появлением новых журналов или удалением старых. Также отслеживается факт изменения настроек контролируемых системных журналов.

При появлении нового системного сообщения датчик контроля целостности считывает это сообщение. Далее датчик контроля целостности формирует полный текст сообщения на основе файла-ресурса с описанием сообщений для данного источника событий и отсылает полученное сообщение агенту.

Настройка датчика контроля целостности выполняется в следующей последовательности:

1. В случае необходимости использования для контроля целостности ресурсов отечественных криптоалгоритмов, необходимо предварительно установить на все узлы, на которых присутствуют датчики контроля целостности СОА «Форпост», криптопровайдер КриптоПРО CSP.
2. На все узлы, на которых установлен датчик контроля целостности, необходимо установить сертификат удостоверяющего центра (УЦ) (удостоверяющего центра, на котором будут в дальнейшем выписываться сертификаты для компонентов СОА) и список отозванных сертификатов.
3. Выписать сертификат для датчика контроля целостности, используемый для подписи файла, содержащего список контролируемых на целостность файлов и веток реестра с их контрольными суммами. Сертификат должен быть установлен на все узлы, на которых присутствует датчик контроля целостности. Доступ к закрытому ключу должен быть на тех узлах, на которых предполагается осуществлять подпись списка контролируемых файлов.

Сертификат, выписываемый для датчика контроля целостности должен в своем составе иметь поле «Использование ключа» со значением «Цифровая подпись, шифрование данных».

Параметры настройки датчика контроля целостности с пояснениями приведены в таблице 1.

Таблица 1 – Параметры настройки датчика контроля целостности СОА «Форпост»

Модуль почтовых уведомлений

Модуль почтовых уведомлений позволяет автоматически по электронной почте отправлять заранее заданным адресатам информацию об обнаруженных атаках и событиях, происходящих в системе.

Модуль почтовых уведомлений устанавливается на тот же самый узел, на который устанавливается координационный центр. Если принято решение об использовании резервного координационного центра, то модуль почтовых уведомлений так же должен быть установлен и на него, при этом модуль почтовых уведомлений, установленный на основном КЦ уведомляет только о тех событиях, которые были переданы в информационный фонд основным КЦ, а модуль почтовых уведомлений, установленный на резервном КЦ уведомляет только о тех событиях, которые были переданы в информационный фонд резервным КЦ. Данный алгоритм позволяет исключить дублирование информации, передаваемой по электронной почте от нескольких модулей почтовых уведомлений, установленных на различных серверах КЦ.

Часть параметров настройки модуля почтовых уведомлений обычно вводится во время установки этого модуля. Если этого не было сделано во время установки, то данные параметры должны быть введены после установки СОА.

В случае если в составе системы работает резервный координационный центр, и на нем развернут резервный модуль почтовых уведомлений, настройки этих модулей выглядят идентично.

Подключение модуля почтовых уведомлений к информационному фонду происходит напрямую, минуя координационный центр. Однако каждый модуль почтовых уведомлений отсылает по электронной почте события только того КЦ, на котором он установлен. Это позволяет избавиться от дублирования сообщений от основного и резервного модуля почтовых уведомлений.

Модуль почтовых уведомлений рассылает события, появляющиеся в журнале системных сообщений и журнале модулей-датчиков. Так как сообщения в журналах СОА появляются достаточно часто, и их количество достаточно велико, рекомендуется ограничить перечень сообщений, рассылаемых по электронной почте. Сделать это можно установив фильтр системных сообщений и фильтр сообщений модулей датчиков.

Рекомендуется использовать модуль почтовых уведомлений для рассылки только наиболее важных сообщений. Например, для сообщений модулей-датчиков можно выбрать сообщения со степенью критичности «Высокая». В фильтре системных сообщений можно выбрать круг компонентов, от которых рассылаются почтовые уведомления. Например, чтобы получать уведомления о неудачных попытках аутентификации, необходимо получать сообщения от координационного центра. Необходимость получения уведомлений о конкретных типах событий может быть определена опытным путем на стадии эксплуатации системы.

Так же при использовании фильтрации сообщений необходимо правильно настроить время, за которое будут браться новые события для отправки в почтовом уведомлении.
Настройки модуля почтовых уведомлений с пояснениями представлены в таблице 2.

Таблица 2. – Настройки модуля почтовых уведомлений СОА «Форпост»

Наименование параметра	Описание параметра
Группа «Основные настройки»	
Период отправки новых сообщений рассылки адресантам (сек)	Длительность минимального промежутка времени в секундах между почтовыми уведомлениями
Использовать SMTP-аутентификацию при отправке почты	Включает использование SMTP-аутентификации при отправке почты
Интервал опроса ИФ на наличие новых сообщений (сек)	Промежуток времени в секундах, проходящий между опросом информационного фонда на предмет наличия новых данных

Наименование параметра	Описание параметра
Максимальное количество сообщений в одном письме оповещения	Задает максимальное количество событий, отправляемых в одном письме оповещения
Производить запись отладочных журналов почтового клиента	Включает запись отладочных журналов почтового клиента
Производить запись отладочных журналов сессий	Включает запись отладочных журналов сессий
Параметры подключения к почтовому серверу	
Адрес SMTP-сервера	Доменное имя или IP-адрес SMTP-сервера
Порт SMTP-сервера	Порт SMTP-сервера
Кодовая страница сервера	Кодовая страница сервера
Группа «Параметры подключения к БД СОА	
Имя источника данных (DSN)	Имя системного источника данных для подключения к базе данных (информационному фонду) СОА «Форпост». Если по условиям применения СОА «Форпост» в конкретной АИС предполагается использовать для связи координационных центров с СУБД информационного фонда ODBC-драйвера из состава СОА «Форпост», то поле должно иметь значение IDSCrypto. Если по условиям применения СОА «Форпост» в конкретной АИС предполагается использовать для связи координационных центров с СУБД информационного фонда ODBC-драйвера из состава операционной системы или СУБД, то поле должно иметь значение IDS. Использование ODBC-драйвера из состава СОА «Форпост» вместо драйвера из комплекта поставки операционной системы или СУБД является обязательным, если предполагается шифрование информационного обмена между координационным центрами и информационным фондом с использованием отечественных криптоалгоритмов
Имя пользователя	Имя пользователя для подключения к базе данных
Пароль	Пароль для подключения к базе данных
Настройка параметров учетных записей для отправки сообщений	
Адрес электронной почты	Задает адрес электронной почты модуля почтовых уведомлений
Имя пользователя	Имя пользователя для подключения к почтовому серверу
Пароль	Пароль для подключения к почтовому серверу

Рекомендуемая литература

1. Докучаев В.А., Шведов А.В. Защита информации на корпоративных сетях VoIP. «Электросвязь». - 2012. № 4.- С. 32-35.

2. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов. Под ред. профессора О.И. Шелухина.: 2013. - 220 с.

3. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. –М.: Горячая линия – Телеком, 2006. – 544 с.: ил.

Приложение 7. Исследование негативного влияния на здоровье человека и общества при использовании ИКТ

1. Использование ИКТ человеком и обществом

1.1. Современные аспекты использования ИКТ

В настоящее время ИКТ проникли во все сферы жизнедеятельности человека, став неотъемлемой частью любой области общественных отношений. Обыденным стало широкое использование систем передачи информации в культуре и медицине, социальной сфере, экономике, образовании и транспортной инфраструктуре. На базе современных ИКТ получили развитие новые сферы социальной, экономической и политической деятельности общества, стремящегося к информационному.

ИКТ могут использоваться для разнообразных видов человеческой деятельности, поэтому они преображают буквально каждый сектор общества и экономики. Инновации в ИКТ сфере создают новые возможности для улучшения здоровья и питания людей, удобства доступа к информации, расширения их знаний, стимулирования экономического роста и участия граждан в жизни общества. Определяющая черта ИКТ – это их **способность помогать человеку в сборе, обработке, хранении, извлечении и распространении информации и знаний.** Управление знаниями крайне важно в условиях современной глобальной экономики, где успех часто зависит от умения быстро приобретать и эффективно использовать полезную накопленную информацию, а также оперативным и экономным образом ее использовать и передавать другим людям.

С помощью ИКТ государственные организации, образовательные и научные учреждения и частные компании функционируют более эффективно и продуктивно при меньших затратах. Рост эффективности повышает конкурентоспособность государственной экономики, а также обеспечивает жизнестойкость проектов социально-экономического развития, делая их более рентабельными.

В рамках этапов Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), международное сообщество признало ИКТ факторами, благоприятствующими развитию. Мировые лидеры, представлявшие правительства, гражданское общество, частный сектор и техническое сообщество, разработали стратегическую рамочную концепцию партнерского сотрудничества заинтересованных сторон из различных отраслей, направленную на содействие распространению и использованию ИКТ (http://www.itu.int/net/wsis/index-ru.html).

Эта концепция обеспечивает использование потенциала ИКТ для расширения доступа — особенно уязвимых слоев населения — к образованию, услугам здравоохранения, банковским и другим услугам. В ней признается, что ИКТ открывают дорогу к информации и знаниям, а также **расширяют права и возможности женщин**. Эти технологии создают возможности **охраны окружающей среды, смягчения рисков стихийных бедствий и обеспечения устойчивого производства продовольствия**.

Такие виды использования ИКТ соответствуют согласованным на международном уровне целям в области развития. В частности, ИКТ могут помочь осуществлению стремления международного сообщества **обеспечить устойчивое использование природных ресурсов**, о котором упоминается в Принципах Рио+20 и Повестке дня на XXI век.

Сегодня, через пятнадцать лет после Саммита тысячелетия Организации Объединенных Наций и через двенадцать лет после первого этапа Всемирной встречи на высшем уровне по вопросам информационного общества ландшафт ИКТ претерпел значительные изменения. Высокие темпы инноваций, распространение и внедрение технологий подвижной связи, расширение доступа к интернету — благодаря всему этому многократно расширился спектр возможностей ИКТ по содействию всеобъемлющему развитию. Продолжающийся ход выполнения решений Всемирной встречи на высшем уровне по вопросам информационного общества свидетельствует о том, что благодаря международному сотрудничеству и совместной деятельности множества заинтересованных сторон в области стратегического использования ИКТ накоплен гигантский объем знаний и опыта, а также экспертный потенциал.

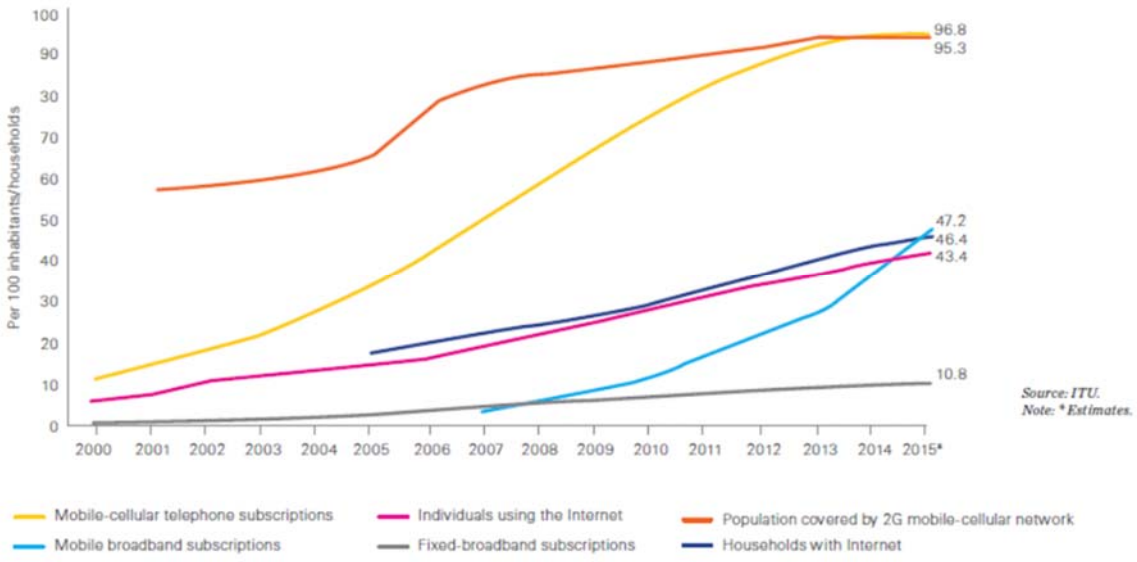
Согласно Совместному заявление Группы Организации Объединенных Наций по вопросам информационного общества (https://itunews.itu.int/ru/Note.aspx?Note=3994), ИКТ служат основой для ускоренного достижения комплексных результатов по всем трем направлениям устойчивого развития, а именно экономическому росту, социальной интеграции и экологической устойчивости. ИКТ в целом и Интернет в частности могут сыграть важную роль в обеспечении развития, опирающегося на права человека. Они **позволяют шире осуществлять свободу выражения мнения и свободу печати**, которые в свою очередь необходимы для борьбы с коррупцией, всестороннего учета гендерных проблем, расширения подотчетности и содействия развитию, обеспечивающему охват всех слоев населения.ИКТ, являющиеся ключевыми факторами и важнейшими инструментами создания рабочих мест и оказания основных государственных услуг, могут также улучшить доступ к знаниям и образованию. Они могут расширить права и возможности женщин, увеличить прозрачность, **предоставить маргинализованным группам населения возможность участвовать в процессах принятия решений**, оказывающих непосредственное влияние на их жизнь. ИКТ могут играть преобразующую роль в управлении и региональном сотрудничестве, а также в повышении технической эффективности деятельности в области развития. Чтобы ИКТ полностью реализовали свой потенциал, необходимы адекватный человеческий потенциал, управление знаниями, разработка контента, создание инфраструктуры и благоприятная среда.

Все шире используются ИКТ- средства для доступа к высокоскоростным сетям, открывающим доступ к другим людям, сообществам и к информации. Интернет представляет собой наиболее важную из существующих в мире глобальных ИКТ- сетей, и которая, в свою очередь, работает на основе множества других физических сетей (например, традиционных телекоммуникационных и IP- сетей).**Сетевой подход к использованию ИКТ** стал неотъемлемым универсальным элементом мирового социально-экономического развития, поскольку фактически обеспечивается универсальный доступ к информации, ресурсам, механизмам распространения и потенциальным клиентам. Этот доступ предоставляется повсеместно и не зависимо от средства доступа, как отдельным

пользователям, так и государственным и частным организациям, учебным и исследовательским институтам, как в развивающихся, так и в развитых странах.

Используемые ИКТ постоянно развиваются. Происходит **постоянная смена технологий и повышение производительности решений**, предоставляющих конечным пользователям все более удобный, скоростной и повсеместный доступ к информации. Современные тренды- потоковое видео, файл обменные сети и облачные сервисы, требующие все более высоких скоростей и практически мгновенных откликов, мобильный широкополосный доступ LTE, технологии SDx, BigData, Internet of Things (IoT) и др. Скорость передачи данных в несколько Гбит/с позволяет синхронизировать локальные хранилища с «облачными» и сетевыми дисками, передавать SHD-видео и поддерживать работу приложений виртуальной и дополненной реальности. Для получения гарантированного уровня услуги, надежности, управления качеством услуги, скорости передачи данных, задержки, минимального затухание предлагаются все более эффективные способы доставки мобильных сервисов, осваиваются новые технологии, частоты, методы модуляции. Уже создана ассоциация 5GPPP − 5G Public-PrivatePartnershipAssociation (5GPPP) по аналогии с ассоциацией 3GPP, занимавшейся последние 15 лет внедрением технологий 3G/4G. Уже прошли обнадеживающие испытания технологий компаниями NTT DoCoMo, Samsung, Alcatel-Lucent, Huawei, Ericsson и др. (http://json.tv/ict_telecom_analytics_view/veduschie-mirovye-ikt-trendy-20150128024138) .

Пользователи ИКТ во всем мире отвечают на вызов производителей. Согласно пресс- релизу МСЭ (http://www.itu.int/net/pressoffice/press_releases/2015/pdf/17-ru.pdf), в течение последних 15 лет происходил беспрецедентный рост ИКТ, открывая колоссальные возможности для социально- экономического развития. Представленные статистические данные “ICT FactsandFigures – Theworldin 2015” (http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx) позволяют отслеживать прогресс в сфере ИКТ за период с 2000 года, когда Организация Объединенных Наций установила Цели развития тысячелетия (ЦРТ).



Основные Индексы развития ИКТ (ICT Development Index — IDI) показывают рост, в частности, число подписок на подвижную связь, которое во всем мире превысило 7 миллиардов, общая численности пользователей Internet, которая составила 3,2 миллиарда. «ИКТ будут играть еще более важную роль в период после 2015 года и в достижении целей в области устойчивого развития, учитывая все ускоряющееся движение мира к созданию цифрового общества», – сказал Брахима Сану, Директор Бюро развития электросвязи МСЭ на прошедшем в Женеве Форуме ВВУИО 2015 года (http://www.itu.int/net/pressoffice/press_releases/2015/16.aspx).

Согласно Cisco Visual Networking Index: (http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html) в 2018 году доля мобильного видео вырастет до 69% от всего мобильного трафика данных. Этому будут способствовать 5 млрд. мобильных пользователей и более 10 млрд. мобильных устройств и соединений, увеличение сетевых скоростей и рост числа умных («smart») устройств. К 2018 году 94% мирового мобильного трафика данных будут формировать смартфоны, ноутбуки и планшеты. Еще, к 2020 году 30-50 млрд. устройств должны подключиться к IoE – Internet of Everything, что составит уже почти по 6 устройств на каждого жителя Земли. Опять же к 2020 году общий объем трафика в ИКТ- сетях превысит, по ожиданиям, 10^{21} байт, и, что должно быть особо интересно традиционным телекоммуникационным компаниям, телефонные разговоры займут лишь 2% от этой величины.

Многие ИКТ- компании все больше внимания уделяют тому, чтобы их продукты и решения были простыми в использовании и могли быть адаптированы для практически неограниченного спектра задач, т.е.**стандартизированы и универсальны**. Эти усилия приводят к тому, что все больше пользователей получает доступ к ИКТ, и им становится легче приспосабливать даже самые сложные технологии для решения собственных задач. Все большее значение для достижения целей социально-экономического развития приобретают технологические стандарты.

Широкое принятие таких стандартов может способствовать **обеспечению функциональной совместимости ИКТ- продуктов и сервисов**, упрощая обмен данными и их совместное использование. Функциональная совместимость в свою очередь может снизить цены и расширить доступ к ИКТ для пользователей из развивающихся стран, позволяя им выбирать конкурирующие продукты и услуги нескольких поставщиков и комбинировать их в единой сети. Кроме того, облегчается передача информации между государственными органами, организациями, занимающимися вопросами социально-экономического развития, и отдельными гражданами.

С другой стороны, ряд OTT (Over the Top) компаний, используя обратную связь с конечным пользователем и механизмы предоставления бесплатных услуг продвигают **проприетарные ИКТ решения**, применяют так называемые бетта- версии продуктов, рассчитанные на диагностику самими пользователями «на свой страх и риск».Быстрые темпы инноваций в сфере ИКТ приводят к тому, что промежуток времени между изобретением и коммерческим применением в этих случаях, как правило, измеряется несколькими месяцами и даже неделями.

С момента своего создания в 1865 году МСЭ-Т применяет к разработке стандартов подход на базе вкладов и на основе консенсуса, при котором все страны и компании, большие или малые, получают равные права на оказание воздействия на разработку Рекомендаций МСЭ-Т. Базирующееся в штаб-квартире МСЭ в Женеве Бюро стандартизации электросвязи(БСЭ) обеспечивает поддержку секретариата исследовательским комиссиям МСЭ-Т, используя передовые электронные методы работы и современное оборудование (http://www.itu.int/ru/ITU-T/about/Pages/default.aspx).

В целом ряде важных вопросов требуется выработка международного многостороннего подхода по **управлению ИКТ**, в частности, управления использованием радиочастотным спектром, подробно рассмотренное на последней Всемирной конференции радиосвязи (http://www.itu.int/dms_pub/itu-r/oth/12/01/R12010000014A01PDFR.pdf), управлении критически важной инфраструктурой Интернета, которое по мнению генерального секретаря МСЭ Хоулиня Чжао, не может ограничиваться регулированием только со стороны ICANN (Корпорация по управлению доменными именами и IP-адресами) и должно более интернациональным(http://www.comnews.ru/node/91554#ixzz3we9srxFx).

Среди глобальных инициатив МСЭ следует отметить Глобальную программу кибербезопасности (http://www.ifap.ru/pr/2008/080908aa.pdf), а также укрепление доверия и безопасности при использовании ИКТ ((http://www.itu.int/net/wsis/outcome/booklet/declaration_Bru.html), ориентированную на упрочение основы для доверия, включая информационную безопасность и безопасность сетей, аутентификацию, защиту неприкосновенности частной жизни и прав потребителей, и являющейся предпосылкой становления информационного общества и роста доверия со стороны пользователей ИКТ.

Рекомендательными и контролируемыми факторами, требующих многостороннего подхода являются также вопросы **надежности, производительности, качества обслуживания, безопасности**.

Несмотря на то, что взаимосвязь ИКТ и экономического роста уже давно является предметом дискуссий экономистов многих стран (например, http://eprints.lse.ac.uk/2575/1/The_link_between_ICT_and_economic_growth_in_the_discourse_of_development_%28LSERO%29.pdf), появляется все больше данных, свидетельствующих о том, что инвестиции в ИКТ – особенно в совокупности с фундаментальными организационными изменениями, могут оказывать существенное позитивное влияние на производительность труда. Таким образом, **ИКТ является одним из основных двигателей роста и развития экономики**. В частности, для России, доля ИКТ в ВВП страны в 2014 году составляла 3.9% (http://json.tv/ict_telecom_analytics_view/perspektivy-rynka-shirokopolosnyh-setey-v-rossii-sravnenie-s-zarubejnym-rynkom). Однако, для большинства развитых стран мира, в ближайшее время, эта доля, очевидно, будет иметь тенденцию к снижению. Это обусловлено как общим насыщением рынка ИКТ услуг, так и падением стоимости оборудования/ программного обеспечения в связи с переносом производства в страны Азии.

С появлением компьютерных сетей и соответствующих средств ИКТ **доступ к информации** приобрел новое качество, связанное в первую очередь с возможностью оперативно получать информацию из любой точки земного шара. Через глобальную компьютерную сеть Интернет возможен мгновенный доступ к мировым информационным

ресурсам (электронным библиотекам, облачным базам данных, хранилищам файлов, и т.д.). Доступ к информации возможен с любого ИКТ устройства (терминала, компьютера, смартфона, софтфона, планшетника и т.п.) в любое время, в любой точке мира.

В сети доступны средства обмена информацией, к числу которых относятся электронная почта, списки рассылки, группы новостей, чат, расширяющие традиционные способы **межличностного общения.** Разработаны специальные программы для общения в реальном режиме времени, позволяющие после установления связи передавать текст, вводимый с клавиатуры, а также звук, изображение и любые файлы. Эти программы позволяют организовать совместную работу удаленных пользователей с программой, запущенной на локальном компьютере.

ИКТ обладают гигантским **потенциалом и средством социального развития**. Универсальная, гибкая природа ИКТ предполагает их использование для решения практически любой задачи развития из целого ряда областей. Здесь мы приводим лишь часть социально- значимых приложений, где ИКТ- приложения уже доказали свою эффективность.

Здравоохранение. ИКТ все шире используются для предоставления медицинских услуг, особенно пациентам в удаленных районах, где имеется большая нехватка специалистов. Здесь можно привести следующие примеры применения современных технологий: для удаленных консультаций между пациентами и врачами, постановки диагнозов и даже лечения; для сбора данных, как в исследовательских целях, так и в целях диагностики; для сотрудничества «в режиме реального времени» между врачами и медиками-исследователями в различных частях планеты; для повышения скорости и эффективности реагирования стран и организаций на эпидемии, а также для общей оптимизации и улучшения качества медицинских услуг. ИКТ также используются для предоставления услуг здравоохранения в удаленных сельских районах, где существует недостаток более традиционных видов медицинского обслуживания (http://swsys-web.ru/information-technology-in-health-care.html). Приложения ИКТ eHealth и mDisease, mAwareness получили глобальное развитие в мировых инициативах МСЭ, например, http://www.itu.int/pub/D-STR-E_HEALTH.06, и http://www.itu.int/en/ITU-D/ICT-Applications/Pages/Be_Healthy_intro.aspx. Кроме того, передовые технологии играют важную роль в программах по борьбе с ВИЧ/ СПИДом, туберкулезом, малярией и другими заболеваниями, в частности под эгидой ЮНЕСКО (http://www.ifap.ru/pr/2004/041125b.htm).

Образование. ИКТ не заменяют собой те важные взаимоотношения, которые складываются между преподавателем и учащимся, они также не могут вытеснить индивидуальное обучение. Однако, ИКТ все шире используются в качестве инструмента, дополняющего традиционные программы и методы обучения и открывающего новые возможности для повышения квалификации в области информационных технологий (http://www.ict.edu.ru/lib/index.php?a=books&c=getForm&d=mod&id_node=315&r=resNode)

Окружающая среда и устойчивое социально-экономическое развитие в удаленных районах. Многие проблемы с изменением климата, окружающей средой, особенно, в развивающихся странах, являются следствием плохой информированности руководящих деятелей о существующих рисках, а также неспособности соответствующих органов заблаговременно давать количественную оценку значимости тех или иных опасностей для окружающей среды. Современные технологии помогают государственным лидерам

оценивать существующие угрозы и вырабатывать стратегии, которые бы обеспечивали более бережное отношение к природным ресурсам, например, для сельской местности (http://www.e-agriculture.org/) .

Государственные органы, как и любые другие организации, все шире используют возможности ИКТ для рационализации и роста эффективности своей деятельности. Например, многие органы власти, как в развитых, так и в развивающихся странах работают над переводом бумажных документов и записей в электронный формат и даже начинают «связывать» базы данных таких документов, чтобы ими могли воспользоваться различные ведомства. Эти усилия повышают оперативность действий государственных органов и упрощают доступ граждан к государственным документам, информации и услугам по сети Интернет. Широкое применение в развитых и развивающихся странах получили проекты **«электронного правительства», «электронного муниципалитета» и т.п**., в частности для Российской Федерации (http://d-russia.ru/elektronnye-municipalitety-v-rossii-ne-abstrakciya-a-realnost.html).

Многие проблемы, традиционно стоящие перед **малообеспеченными сообществами граждан**, частично проистекают от ограниченности их доступа к знаниям и информации. ИКТ могут помочь в преодолении этой проблемы, упрощая и удешевляя сбор и анализ информации, а также ее распространение среди тех категорий граждан, которые особенно в ней нуждаются. Наибольший выигрыш от глобального роста ИКТ- индустрии получили развивающиеся страны. Однако пути, которыми они шли, были различными. Эти расхождения, в значительной степени, отражают разнообразие самой ИКТ-индустрии, состоящей из множества разных секторов, каждый из которых обладает своими собственными уникальными характеристиками (http://www.perspektivy.info/print.php?ID=114058) .

Инвестиции в **человеческий потенциал** играют фундаментальную роль в социально-экономическом развитии, поэтому инвестиции в информационные технологии могут лишь незначительно сократить бедность или улучшить жизнь малообеспеченных слоев общества, если они не сопровождаются усилиями по расширению способностей данных групп граждан использовать возможности, которые им предоставляют ИКТ. **Образование и повышение квалификации в области информационно- коммуникационных технологий** – это два важных элемента, помогающих отдельным людям, сообществам граждан и даже целым странам добиться успеха в глобальной информационной экономике. Именно поэтому они должны являться составной частью любых проектов социально-экономического развития.

ИКТ, как и другие, широко распространенные сегодня технологии и тренды, несмотря на многочисленные позитивные креативные факторы для общества и человека, оказывает **негативное влияние на непосредственного пользователя**. Как показало наше исследование, до сих пор, это влияние изучено не полностью и требует комплексного системного анализа с целью идентификации, классификации, разработке рекомендаций по своевременному обнаружению и принятию определенного комплекса мер каждой из заинтересованных сторон.

1.2. Экосистема ИКТ

1.2.1. Состояние разработок в области экосистемы ИКТ

Рассмотренные выше аспекты современного использования ИКТ, по нашему мнению, в виду очевидной их взаимосвязи и признаков тяготения, а также ориентированности на достижение общей цели могут быть сгруппированы в отдельные элементы и объединены в систему. Это даст возможность произвести их последующий анализ, содержания взаимодействия и оценки влияния на здоровье и жизнедеятельность человека как отдельно, так и как члена формирующегося информационного общества.

В настоящее время нет единства в определении понятия «система». В первых определениях в той или иной форме говорилось о том, что система - это элементы и связи (отношения) между ними. Например, основоположник общей теории систем Людвиг фон Берталанфи (http://grachev62.narod.ru/bertalanffy/bertalanffy_2.html) определял систему как комплекс взаимодействующих элементов или как совокупность элементов, находящихся в определенных отношениях друг с другом и со средой. А позднее в определениях системы появляется понятие цели. Так, в «Философском словаре» (http://www.edudic.ru/fil/1129/) система определяется как «совокупность элементов, находящихся в отношениях и связях между собой определенным образом и образующих некоторое целостное единство». К числу задач, решаемых теорией систем, относятся: определение общей структуры системы; организация взаимодействия между подсистемами и элементами; учет влияния внешней среды.

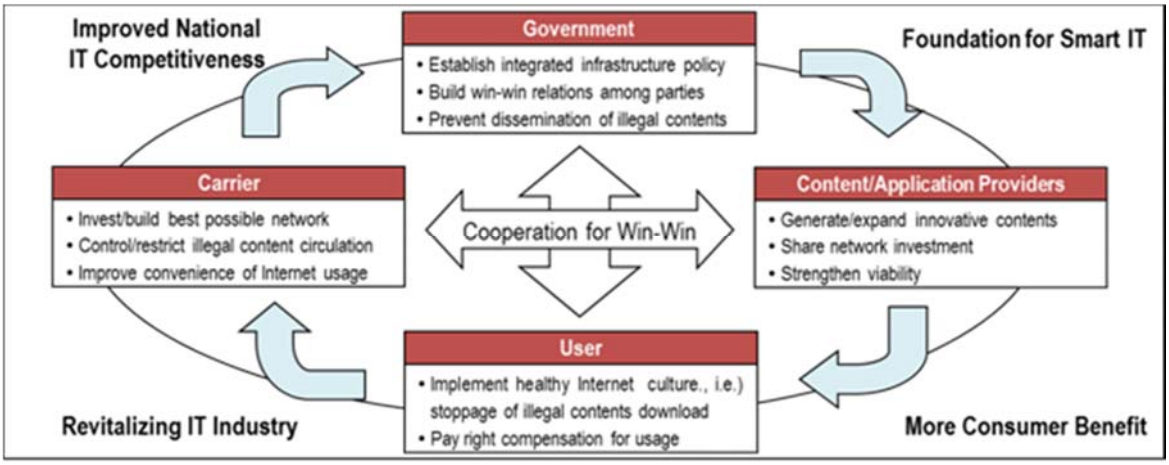
Поскольку элементами системы в нашем случае будут являться как живое существо-человек, так и неживые определим объект исследования как экосистему.

Понятие экосистемы является одним из основных понятий в современной экологии. Существует множество определений. Мы будем придерживаться следующего(http://dic.academic.ru/dic.nsf/ecosystem)-экосистема (от греческого oikos - жилище, местопребывание и система), единый комплекс, образованный живыми организмами и средой их обитания, в котором они связаны между собой обменом вещества и энергии.

Как видно из определения, экосистема представляет собой общую систему живых и неживых компонентов. В большинстве областей физического мира, человек играет доминантную роль в экосистеме. Как для живого существа обладающего сознанием, информационное пространство, в настоящее время отождествляемое с ИКТ, является для него необходимым компонентом среды обитания.

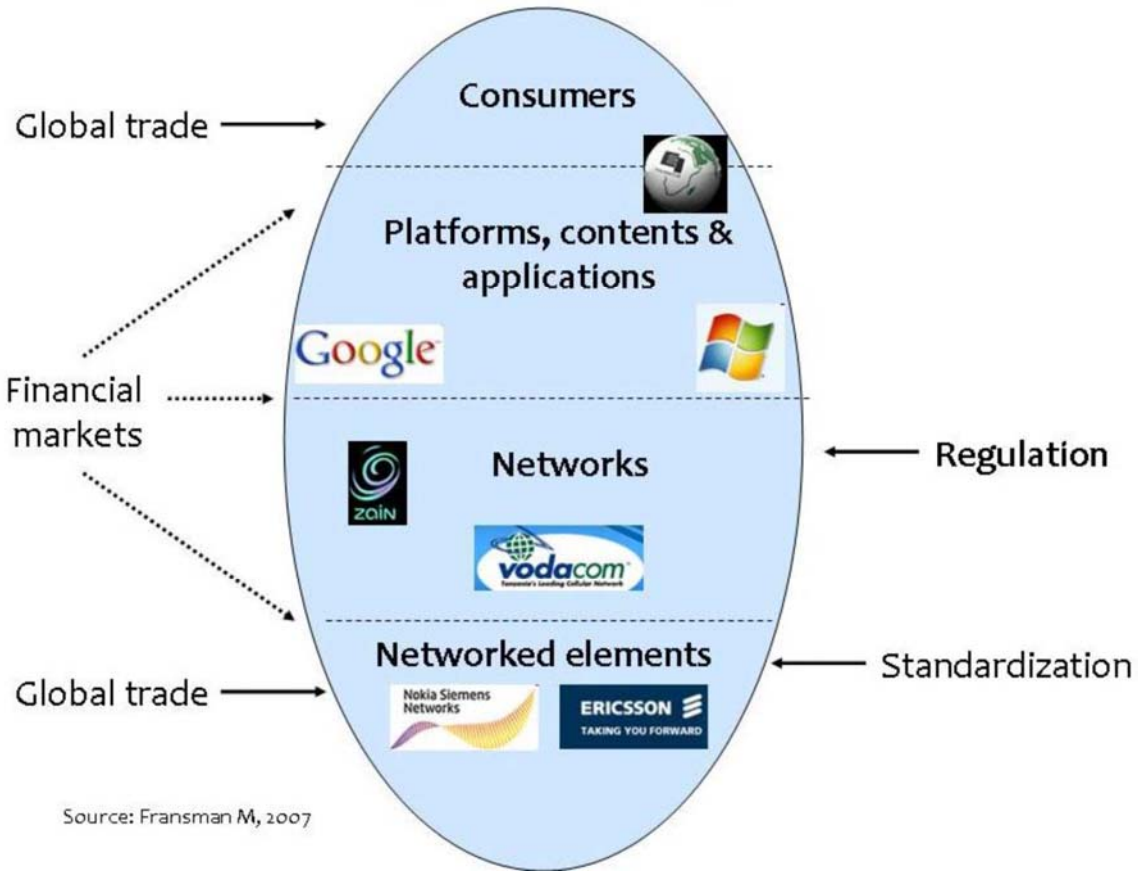
Рассмотрим степень глубины и содержания исследования ИКТ экосистемы по существующим в открытом доступе публикациям.

В связи с возраставшей ролью OTT компаний на рынке услуг, проблемой отвода пользовательского трафика и соответствующего снижения доходов традиционных операторов, в 2012 году опубликовано предложение в ITU: «Win-Win Structure for ICT Industry. Proposal for ICT and Internet Ecosystem.Setting New Rules on Trade Order» (http://www.itu.int/ml/lists/arc/wcit-public/2012-11/msg00012.html).Для описания этой проблемы в экосистеме определены 4 заинтересованные стороны: правительства, поставщики контента и услуг, операторы и конечные пользователи, а также приводятся связи по повышению эффективности взаимодействия.



Похожий подход содержится в «ICT for Economic Growth: A Dynamic Ecosystem Driving The Global Recovery» http://www3.weforum.org/docs/WEF_IT_DynamicEcosystem_Report_2009.pdf)

Прорывной публикацией в этой области стала книга Мартина Франсмана (Martin Fransman) (http://www.ebook3000.com/The-New-ICT-Ecosystem--Implications-for-Policy-and-Regulation_70898.html) ,который показал, что не зависимо от роли каждого «актера» (заинтересованной стороны), будь то отдельный человек, компания или целая нация, он занимает определенную позицию в ИКТ экосистеме и вступает в уникальные взаимоотношения в иерархически организованной экосистеме.



Предложенная экосистема состоит из 4-х уровней, которые пересекаются и взаимозависимы:

1. Элементы сети (коммутаторы, маршрутизаторы, серверы, компьютеры, телефоны и т.п.
2. Конвергентные сети и сети распределения контента (сети подвижной связи, оптические, медные кабельные, спутниковые)
3. Платформы, контент и приложения (провайдеры Интернет приложений и услуг)
4. Конечные пользователи.

На данную структуру накладываются различные связи и взаимодействие между резидентами уровней.

Остальные несколько публикаций содержат развитие работы Мартина Франсмана для конкретных случаев в различных странах и регионах мира, в частности, в Нигерии,http://www.antiessays.com/free-essays/Ict-Ecosystem-In-Nigeria-Impact-Assessment-504471.html. Предполагаем достаточно серьезное исследование в книге Rahul C. Basoleи соавторов «Coopetitionandconvergenceinthe ICT ecosystem», однако, судя по доступному описанию (http://www.sciencedirect.com/science/article/pii/S0308596114000627), исследование опирается на модель ИКТ экосистемы Мартина Франсмана и представляет собой ее расширение.

Исходя из этого, можно сделать следующие выводы:

1. Судя по количеству публикаций, тема ИКТ экосистемы не является достаточно исследованной;
2. В существующих публикациях экосистема ИКТ включает в себя игроков ИКТ рынка и используется для целей описания взаимодействия между ними для оптимизации решения только текущих экономических проблем;
3. ИКТ экосистема представляет собой действенный механизм описания сложных процессов в ИКТ секторе;
4. Целесообразно расширить ИКТ систему за счет включения в нее других элементов для описания также технических и социальных проблем.

1.2.2. Экосистема ИКТ с точки зрения использования ИКТ

На рис.1 представлена предлагаемая экосистема при использовании ИКТ.

Ее основными элементами являются:

1. Заинтересованные стороны (Stakeholders), выполняющие свои роли и обязанности в экосистеме по отношению к использованию ИКТ, а также осуществляющие разработку, производство, поставку, эксплуатацию и утилизацию ИКТ. Основным микроэлементом и макроэлементом здесь является человек;
2. Непосредственно ИКТ;
3. Области использования ИКТ;
4. Факторы использования ИКТ, включающие:

   - положительные аспекты, приносящие эффект, как то повышение производительности труда, оперативность операций, пользу для заинтересованных сторон;

   - факторы, входящие в число регуляторных, рекомендательных вопросов, разрабатываемых отраслевыми международными организациями при участии заинтересованных сторон и содействующих эффективному использованию ИКТ;

   - негативные факторы, вызывающие отрицательное воздействие на здоровье и жизнедеятельность человека, а также заинтересованных сторон;

Между элементами, а также внутри элементов, экосистемы в процессе использования ИКТ возникают связи, имеющие экономический, технический и социальный характер. Так, например, если представитель бизнес- сообщества, частная компания задумала применить разработку в области телемедицины, то она обратиться к соответствующим разработчикам, в соответствующие государственные органы, при этом будут задействованы соответствующие ИКТ (технологии, оборудование, прикладное программное обеспечение). Использование ИКТ в этом случае будет сопряжено с рядом нормативных и регуляторных факторов, плюс, очевидно, с получением преимуществ, по сравнению с традиционным подходом, (например,

удобство, производительность, качество), а также с возможными рисками для здоровья непосредственных пользователей.

1.2.3. Роли и обязанности заинтересованных сторон

Одним из современных подходов управления является теория заинтересованных сторон. Появление этого подхода связано с выходом работы Э. Фримена (http://www.amazon.com/Strategic-Management-Stakeholder-Approach-Business/dp/0273019139) , в которой автор по отношению к отдельной организации вводит новое понятие «заинтересованная сторона» (Stakeholder)- «любая группа или индивид, которые могут повлиять на достижение целей организации или на которые может повлиять достижение целей организации». В последствие этот подход взят на вооружение для решения многих задач стратегического и оперативно- тактического управления задачами, проектами, системами. Применительно к ИКТ сектору, в частности, такие международные организации, как IETF, ICANN, ITUиспользуют, модели, основанные на так называемом мультистейкхолдеризме- решении задач с участием всех заинтересованных сторон: государств, бизнеса, научных и образовательных организаций, гражданского сообщества, и сообщества пользователей.

Каждая заинтересованная сторона осуществляет "соответствующую роль" (Результаты Всемирного саммита информационного общества. World summit on the Information Society Outcome Documents): Geneva 2003 - Tunis 2005; URL: http://www.itu.int/wsis/outcome/booklet.pdf). Без взаимодействия всех "заинтересованных сторон", без принятия согласованных между ними норм, правил и принципов регулирования, как показывает практика развития и использования ИКТ, ни одно из предлагаемых решений или технических требований не может быть эффективно реализовано. Сложившаяся «многосторонняя модель» стала эффективным способом трансграничного функционирования, обеспечивая совместимость, стабильность, безопасность и доступность глобальной инфраструктуры Интернета, в то же время, предоставляя суверенным государствам возможность регулирования использования Интернета в пределах национальной юрисдикции. Такая многосторонняя модель получила закрепление в документах международных межправительственных и международных организаций и форумов (например, Информация о Всемирном саммите Информационного общества (WSIS)). URL: http://www.itu.int/wsis/basic/about.html) .

Мультистейкхолдеризм, т.е. участие всех заинтересованных сторон, является основой трансграничного функционирования и дальнейшего развития ИКТ, включая вопросы их эффективного использования. На основе вышеупомянутых документов, а также документов, посвященных управлению Интернет, например, Доклада Рабочей группы ITU по управлению Интернет (http://www.itu.int/net/wsis/wgig/docs/wgig-report-ru.pdf), роли и обязанности заинтересованных сторон в экосистеме ИКТ можно кратко представить следующими.

Роли и обязанности **государств (правительств)** связаны с такими аспектами деятельности, как разработка, координация и осуществление государственной политики на национальном уровне, координация политики на региональном и международном уровнях; создание благоприятных условий ИКТ; надзорные функции; разработка и принятие законов, положений и стандартов; разработка международных договоров и правил; развитие передового опыта; содействие созданию потенциала в сфере информационно-

коммуникационных технологий и с их помощью; борьба с киберпреступностью; содействие международному и региональному сотрудничеству; решение общих вопросов развития; поощрение многоязычия и культурного разнообразия, и др.

К сфере ответственности **частного сектора** относятся следующие вопросы: саморегулирования информационной индустрии; развития передового опыта; разработки стратегических предложений, руководящих принципов и инструментария для директивных органов и других заинтересованных сторон; научных исследований и опытно-конструкторские разработки в области технологий, стандартов и процессов; участия в разработке национального законодательства и национальной и международной политики; содействия инновационной деятельности и др.

Роль и функции **гражданского общества** включают расширение информированности общественности и создание потенциала (знания, подготовка кадров, обмен опытом); предоставление экспертов, специалистов, обмен опытом и знаниями по вопросам политики в области информационно-коммуникационных технологий; содействие в обеспечении соответствия политических и рыночных факторов потребностям всех членов общества; содействие формированию концепций информационного общества, ориентированного на человека, на основе прав человека, устойчивого развития, социальной справедливости и предоставления широких возможностей и др.

Вклад **научного и образовательного сообщества** является весьма ценным и представляет собой один из главных источников вдохновения, инновационной и творческой энергии. Аналогичным образом, техническое сообщество и его организации активно участвуют в разработке стандартов и развитии ИКТ услуг. Эти группы постоянно вносят ценный вклад в стабильность, безопасность, функционирование и эволюцию технологий. Они широко взаимодействуют со всеми группами заинтересованных сторон и ведут работу внутри этих групп.

Основную роль по организации работы, выработке многосторонней политики и координации усилий всех заинтересованных сторон ИКТ экосистемы выполняют **международные организации**, прежде всего ITU, который является основной международной организацией в процессе WSIS.

1.2.4. Содержание элемента ИКТ экосистемы.

Различные аспекты использования ИКТ рассмотрены ранее.

“Информационные и коммуникационные технологии (ИКТ) – это обобщающее понятие, описывающее различные устройства, механизмы, способы и алгоритмы обработки информации.”-это определение появляется при поиске на большинстве страниц русскоязычного Google, без какой- либо возможности идентифицировать ссылку на первоисточник. В англоязычных поисковиках ИКТ-прежде всего технология, например здесь (http://foldoc.org/) : «ICT refers to technologies that provide access to information through telecommunications. It is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication mediums» (http://techterms.com/definition/ict), т.е. провозглашается близость с Информационными Технологиями, но акцент рассмотрения- прежде всего сетевые технология- ИКТ (буквально) включают Интернет, беспроводные сети, сотовые телефоны и другие средства связи (?). Известно также, что словосочетание впервые публично прозвучало

из уст некого Стивенсона в 1997 году в докладе для английского правительства. В http://www.tutor2u.net/business/reference/what-is-ict отчасти объясняется причина отсутствия универсального определения: «However, apart from explaining an acronym, there's no universally accepted definition of ICT. Why? Because the concepts, methods and applications involved in ICT are constantly evolving on an almost daily basis and it's difficult to keep up.», т.е. все, что образует ИКТ (концепции, методы и приложения) постоянно меняется и «догнать» определение сложно.

ИКТ- отрасль, как и любая, динамично растущая, многокомпонентная и разнородная экосистема- довольно сложный объект для структуризации. Единый подход к ее структуре отсутствует.

1.3. Классификация ИКТ

В России, как и за рубежом, уже сделаны многократные попытки построить модель отрасли ИКТ. Существуют различные классификации сегментов отрасли ИКТ, и в настоящее время российской практике пока не сложилось единого подхода. Министерство связи и массовых коммуникаций РФ рассматривает отдельно отрасль информационных технологий (ИТ) и отрасль телекоммуникационных услуг, для каждой из которых формируется Концепция развития. Так, согласно «Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года» (http://minsvyaz.ru/common/upload/Strategiya_razvitiya_otrasli_IT_2014-2020_2025%5B1%5D.pdf), под отраслью информационных технологий понимается совокупность российских компаний, осуществляющих следующие виды деятельности: (1) разработка тиражного программного обеспечения; (2) предоставление услуг в сфере информационных технологий, в частности, заказная разработка программного обеспечения, проектирование, внедрение и тестирование информационных систем, консультирование по вопросам информатизации; (3) разработка аппаратно-программных комплексов с высокой добавленной стоимостью программной части; (4) удаленная обработка и предоставление информации, в том числе на сайтах в информационно-телекоммуникационной сети "Интернет".

Более широкая классификация предлагается Министерством экономического развития и торговли РФ в отчете «Анализ тенденций развития ИКТ и их применение в социально□ экономической сфере». (http://www.silicontaiga.ru/article/files/2074_1.pdf) . В отчете раскрывается несколько точек зрения относительно структуры отрасли в зависимости от признака, положенного в основу классификации.

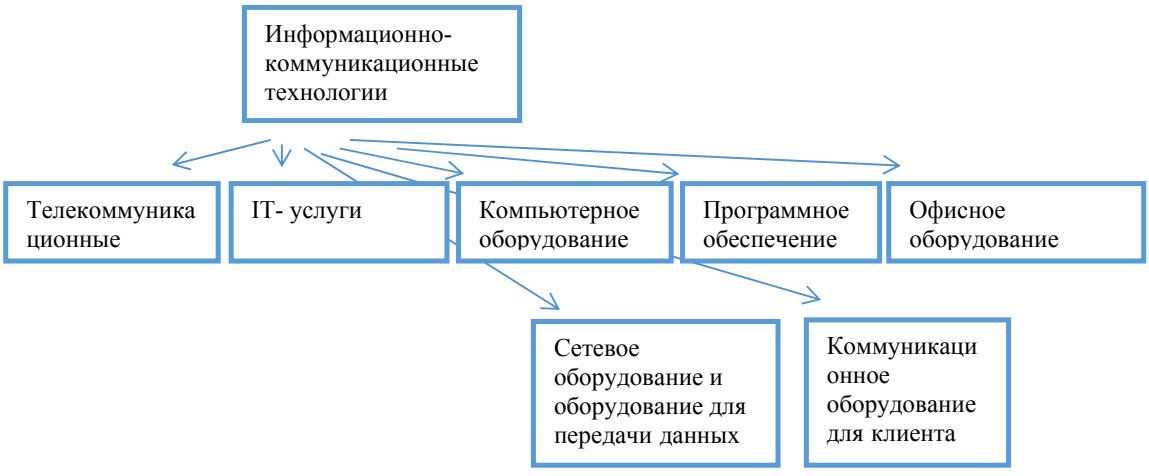
В исследовании МЭРТ обозначено, что наибольшее число участников рынка ИКТ склоняется к варианту классификации по продукции, разделяя ее на материальную (оборудование) и нематериальную (ИТ□ услуги, программное обеспечение). При этом отдельно выделяется сегмент телекоммуникаций (оборудование + услуги) и Интернет (услуги контента, дизайна, электронной коммерции, рекламы и маркетинга).

В следующей таблице приводим результат экспертного мнения, приведенного в вышеупомянутом отчете МЭРТ.

Оборудование	ПО	ИТ- услуги
- ПК (настольные,	- Инфраструктурное/	- Консультирование (в области ИТ,

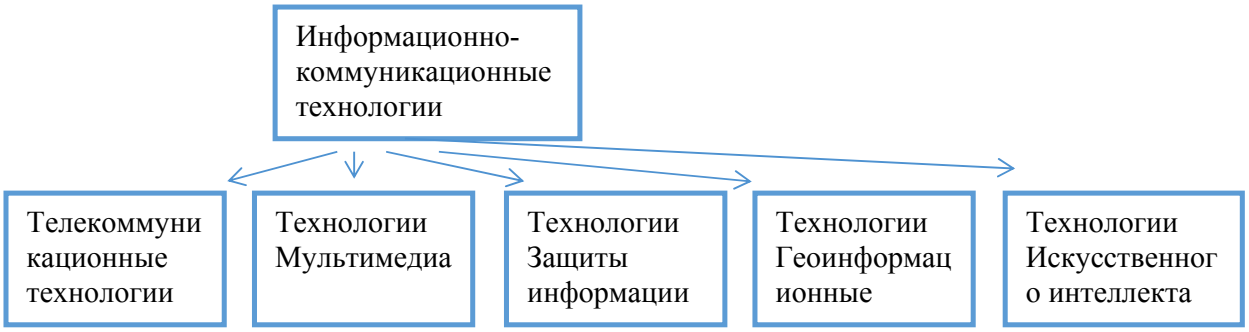
портативные, карманные и др.) - Серверы - Периферийные устройства (мониторы, копиры, принтеры, …) - Комплектующие - Системы хранения данных (SAN, DAS, NAS) - Коммуникационное оборудование (Беспроводные Телеком решения, Телефония, Активное оборудование, Пассивное оборудование)	системное ПО - Средства разработки - MiddleWare - Прикладное ПО - GroupWare	в области бизнеса, по информационной безопасности) - Интеграция (разработка, сетевая интеграция, внедрение) - Обучение и тренинги - Эксплуатация (Обслуживание технических средств, ПО, ИТ-аутсорсинг) - Телекоммуникационные услуги (Телефония, Передача данных, Транспорт, Приложения) - Контент (авторский контент, Сервисы, Средства коммуникации) - Дизайн и Технологии - Электронная коммерция, электронный бизнес(B2C/ B2B/ B2G решения) «Электронное правительство» (G2B/ G2C/ G2G решения) - Реклама и маркетинг

В зарубежной практике распространена более упрощенная, одноуровневая классификация рынка ИКТ. Так, одна из известнейших мировых консалтинговых компаний в области ИКТ European Information Technology Observatory (http://www.eito.com/) разделяет отрасль на следующие сегменты: телекоммуникационные услуги; ИТ□ услуги; компьютерное оборудование; программное обеспечение; сетевое оборудование и оборудование для передачи данных; коммуникационное оборудование для клиента; офисное оборудование.

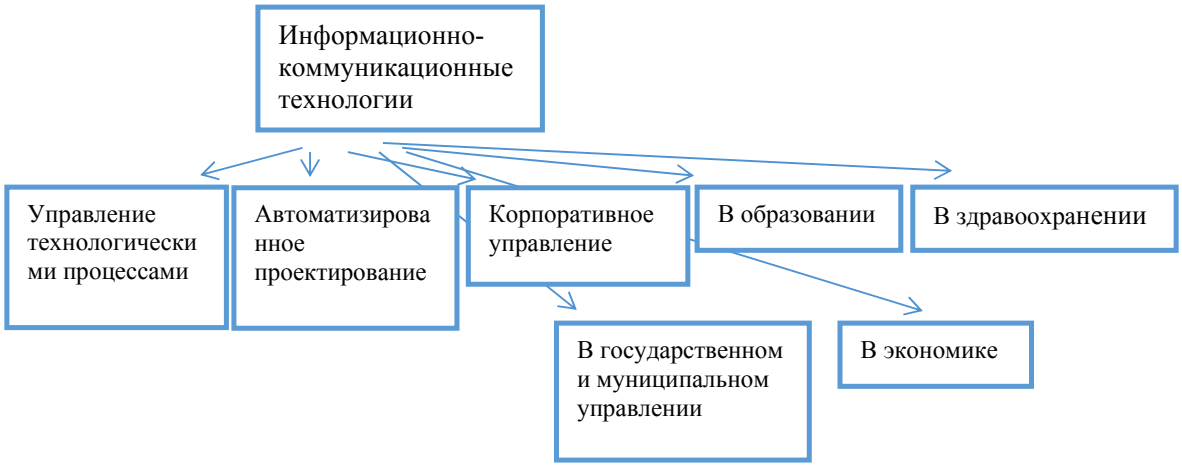


Информационно-коммутационные технологии можно классифицировать еще и с других точек зрения:

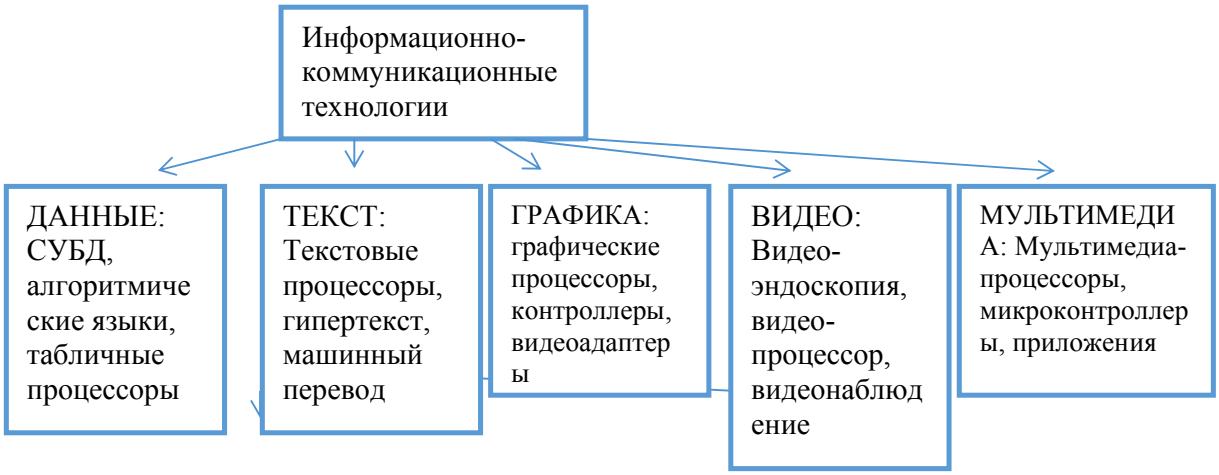
- по образующим ИКТ технологиям:



- в зависимости от предметной деятельности:



- в зависимости от типа обрабатываемой информации;



1.4. Классификация ИКТ с учетом их использования

На основе анализа вышеприведенных классификаций к рассмотрению экспертного со общества предлагается классификация ИКТ с учетом их использования. Пользователями ИКТ являются заинтересованные стороны экосистемы ИКТ.

2. Негативные факторы влияния на здоровье человека и общества при использовании ИКТ

ИКТ, как и другие, широко распространенные сегодня технологии и тренды, несмотря на многочисленные позитивные креативные факторы для общества и человека, оказывает негативное влияние на непосредственного пользователя, его здоровье, жизнедеятельность, как отдельного живого существа, так и элемента сообществ каждой из заинтересованных сторон. Как показало наше исследование, до сих пор, часть этих воздействий изучается, часть только обсуждается, поэтому, в целом, это влияние изучено не полностью и требует комплексного системного анализа с целью идентификации, классификации, разработке рекомендаций по своевременному обнаружению и принятию определенного комплекса мер каждой из заинтересованных сторон.

Очевидно, что человек имеет наибольший риск быть подверженным негативному влиянию ИКТ, непосредственно сталкиваясь с источникамивредных и опасных факторов ИКТ, будучи прямым пользователем соответствующего оконечного оборудования и программного обеспечения. Исходя из предложенной классификации ИКТ с точки зрения использования, на основе проведенного исследования открытых публикацийможно выделить следующие элементы (выделены на рисунке ниже):

- ✓ Телекоммуникационное оборудование/ Абонентское (терминальное) оборудование в части мобильных терминалов (аппаратов);
- ✓ ИТ оборудование/Терминальное оборудование в части компьютеров, планшетов, маршрутизаторов радио доступа и ретрансляторов (WiFi) и Периферийные устройства (принтеры, сканеры);
- ✓ Телекоммуникационные услуги/ Мобильная связь в части услуг передачи речи, SMS/MMS и Услуги передачи данных, включая Internet;
- ✓ Программное обеспечение/ Прикладное программное обеспечение развлекательного назначения (игры, плееры);
- ✓ Информационные услуги/ Пользовательские услуги/ Электронная почта, Социальные сети, Информационные ресурсы.

Условно перечисленные выше источники вредного и опасного(негативного) влияния при использовании ИКТ предлагается сгруппировать следующим образом:

1. Использование оконечного (терминального) ИКТ оборудования, включая компьютеры, планшеты, маршрутизаторы радио- доступа и ретрансляторы (WiFi) и Периферийные устройства (принтеры, сканеры);

2. Пользовательские ИКТ услуги, включая инфокоммуникационные услуги и приложения мобильной связи, электронную почту социальные сети;

3. Использование информационных ресурсов (информации).

Далее рассматривается каждая из перечисленных групп с точки зрения содержания и степени негативного воздействия на здоровье человека, возможные результаты


Телекоммуникационные услуги
Телекоммуникационное оборудование
Местная телефонная
Мобильная связь
Международная и междугородная телефонная связь
Передача данных, телематические услуги, включая Интернет
Телекоммуникационные технологии
Информационно-коммуникационные технологии
Информационные технологии
Абонентское (терминалы)
Пассивное сетевое (ВОЛС, СКС,…)
Системы коммутации
Системы спутниковой
Оборудование
Программное обеспечение
Информационные услуги
Активное сетевое (маршрутизат
Терминальное (PC, планшеты, маршрутизаторы)
Серверы, хранилища БД
Периферийные устройства
Комплектующие
Прикладное (для игр, образования, медицины,…)
Системное ПО
Средства разработки
MiddleWare (Технологическое)
GroupWare (Работа групп)
Прикладное
Общего и спец. назначения (редакторы, САПР)
Развлекательного назначения (игры, плееры)
Пользовательские услуги
Профессиональные услуги
Электронная почта
Социальные сети
Информационные ресурсы
Хранилище файлов и изображений
Голосовая связь
Офисные средства
Муниципальные и госуслуги
Разработка и интеграция
Поддержка и сопровождение
Управление ИТ и бизнес-процессами, проектами
Обучение и повышение квалификации

воздействия и рекомендации по предотвращению и ограничению последствий воздействия.

2.1. Негативное воздействие на здоровье человека при использовании оконечного (терминального оборудования).

Наиболее изученный и «нормированный»негативный фактор- работа с компьютером. Работа пользователей компьютерного оборудования относится к категории работ, связанных с опасными и вредными условиями труда.

Согласно государственным стандартам классификации опасных и вредных производственных факторов при работе за компьютером выделяют следующие вредные факторы (ГОСТ 12.0.003-74, утв. Постановлением Госстандарта СССР от 13.11.1974 № 2551 и ГОСТ 12.0.001-82, утв. Постановлением Госстандарта СССР от 20.12.1982 № 4909 (с изменениями от 25 октября 1989 г.):

- повышенная или пониженная температура поверхностей оборудования, материалов;

- повышенная или пониженная температура воздуха рабочей зоны;

- повышенный уровень шума на рабочем месте;

- повышенный уровень вибрации;

- повышенный уровень ультразвука;

- повышенная или пониженная влажность воздуха;

- повышенная или пониженная ионизация воздуха;

- повышенный уровень ионизирующих излучений в рабочей зоне;

- повышенный уровень статического электричества;

- повышенный уровень электромагнитного излучения;

- повышенная напряженность электрического поля;

- повышенная напряженность магнитного поля;

- отсутствие или недостаток естественного света;

- недостаточная освещенность рабочей зоны;

- повышенная яркость света;

- пониженная контрастность;

- прямая и отраженная блесткость;

- другие вредные факторы, связанные с окружающей средой;

- физические перегрузки;

- нервно-психические перегрузки (умственное напряжение, монотонность труда, эмоциональные перегрузки).

Требования Санитарных правил распространяются на вычислительные электронные цифровые машины персональные и портативные; периферические устройства вычислительных комплексов (принтеры, сканеры, клавиатуру, модемы внешние); устройства отображения информации (видеодисплейные терминалы — ВДТ) всех типов, условия и

организацию работы с ПЭВМ и направлены на предотвращение неблагоприятного влияния на здоровье человека вредных факторов производственной среды и трудового процесса при работе с ПЭВМ. В настоящее время к этой группе риска в гораздо меньшей степени можно отнести также планшеты, ноутбуки, нетбуки, смартфоны.

2.1.1. Классификация вредных и опасных факторов

В многочисленных публикациях, посвященных этому вопросу (например, http://www.scienceforum.ru/2015/814/11718, или http://www.tiensmed.ru/programmer4.html) приводится следующая классификацию факторов:

(1) Физически вредные и опасные факторы

К физическим вредным и опасным факторам относятся: повышенные уровни излучения; статического электричества и запыленности воздуха рабочей зоны; повышенное содержание положительных аэронов и пониженное содержание отрицательных аэройонов в воздухе рабочей зоны; повышенный уровень блескости и ослепленности; неравномерность распределения яркости в поле зрения; повышенная яркость светового изображения; повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека.

(2) Химически вредные и опасные факторы

Химические вредные и опасные факторы следующие: повышенное содержание в воздухе рабочей зоны двуокиси углерода, озона, аммиака, фенола и формальдегида.

(3) Психофизические вредные и опасные факторы

Психофизиологические вредные и опасные факторы: напряжение зрения и внимания; интеллектуальные, эмоциональные и длительные статические нагрузки; монотонность труда; большой объем информации, обрабатываемый в единицу времени; нерациональная организация рабочего места.

Типичные ощущения, которые испытывают к концу рабочего дня операторы ПЭВМ (http://подзаконом.рф/vrednye-i-opasnye-faktory-na-rabote-s-kompyuterom): переутомление глаз, головная боль, тянущие боли в мышцах шеи, рук и спины, снижение концентрации внимания.Длительная и интенсивная работа на компьютере может стать источником тяжелых профессиональных заболеваний, таких, как травма повторяющихся нагрузок (ТПН), представляющая собой постепенно накапливающиеся недомогания, переходящие в хронические профессиональные заболевания нервов, мышц и сухожилий руки.

К факторам негативного воздействия на здоровье человека при использовании оконечного (терминального оборудования) можно отнести и «компьютерную зависимость». Термин «компьютерная зависимость» определяет патологическое пристрастие человека к работе или проведению времени за компьютером (http://www.tiensmed.ru/programmer4.html) .Характерными особенностями этой зависимости, также как и зависимости от мобильных телефонов, других различных гаджетов являются: синдром абстиненции, стремление заполучить объект зависимости, поведение, направленное на приобретение объекта зависимости, снижение критического отношения к негативным сторонам зависимости, потеря интереса по отношению к социальной стороне жизни, внешнему виду, удовлетворению других потребностей.

В связи с этим предлагается дополнить существующую классификацию **(4) социально-патологическими вредными факторами**.

2.1.2. Регламентирующие стандарты

Однако, уже отмечалось вопрос влияния негативных факторов при использовании компьютера и других терминальных устройств изучен достаточно полно- существует целый ряд международных, региональных и национальных стандартов в этой области и регламентирующих требования к оборудованию, эргономике, окружающей среде, рекомендации по оборудованию рабочих мест. В заключение этого раздела приведем основные документы национального (для РФ) и международного значения.

СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы», утв. Постановлением главного государственного санитарного врача РФ 03.06.2003 № 118 (с изменениями на 25.04.2007), введены в действие с 30.06.2003.

СанПин 2.2.4.1294-03 «Гигиенические требования к аэроионному составу воздуха в общественных помещениях», утв. Постановлением главного государственного санитарного врача РФ от 22.04.2003 № 64, введены с 15.06.2003.

Полный перечень требований к организации рабочих мест с ПЭВМ см. в СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы», утв. Постановлением главного государственного санитарного врача РФ 03.06.2003 № 118 (с изменениями на 25.04.2007), введены в действие с 30.06.2003.1. Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы. СанПиН 2.2.2.542-96. Утв.14.07.96. ГКСЭН.

ГОСТ РФ. Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности. Введ. 01.07.1997.

ГОСТ РФ. Средства отображения информации индивидуального пользования. Методы измерения и оценки эргономических параметров и параметров безопасности. Введ. 01.07.1997.

ГОСТ РФ. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения. Введ. 01.07.1997.

Требования СанПиН 2.4.1.2660-10. Постановление Главного государственного санитарного врача РФ от 22 июля 2010 г. № 91. Об утверждении СанПиН 2.4.1.2660-10 "Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы в дошкольных организациях (с изменением N 1 от 20 декабря 2010 г.)

Санитарно-эпидемиологические правила и нормативы СанПиН 2.4.2.2821-10 Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях.

Всемирная организация здоровья ВОЗ (http://www.who.int/ru/) определила исследование биологического действия низкочастотных ЭМП от дисплеев, как одно из приоритетных направлений в науке. В Германии работа с ПЭВМ и ВДТ вошла в список 40 наиболее

вредных и опасных профессий. В США проблема защиты пользователя ВДТ от ЭМИ признана национальной.

Европейское экономическое сообщество ЕЭС в 1992г. выпустило директиву, в которой указано, что «Оператор, работающий с дисплеем, должен быть информирован о мерах безопасности и сохранения здоровья, а также о мерах, принимаемых с целью уменьшения или устранения любого риска» (http://www.viems.ru/asnti/ntb/ntb503/ecobez3.html) .

Общемировая проблема защиты здоровья пользователя потребовала разработки норм, регламентирующих работу с компьютерами и их методическое обоснование.

Компьютерная техника и, в первую очередь мониторы, как любое сложное электронное устройство, должны соответствовать определенным требованиям стандартов, которые можно разделить на две основные группы.

К первой группе стандартов, содержащих требования по электромагнитной совместимости и электрической безопасности, относятся: европейский CE, SEMKO AB, канадский FCC Class B, шведский E-2000, международный EPA EnergyStar.

Вторую группу составляют стандарты, содержащие требования по эргономике: шведские MPR-II, международный ISO 9241, немецкий TUV Ergonomie, VESA DDC, TCO — группа стандартов добровольной сертификации на эргономичность и безопасность электронного оборудования (прежде всего компьютерного), разработанных комитетом TCO Development, который является частью Шведской конфедерации профсоюзов.Первый стандарт описывал только требования к дисплеям, последующие относятся также к мобильным телефонам, офисному оборудованию, системным блокам персональных компьютеров, ноутбукам и головным гарнитурам для телефонов.

Цель стандартов TCO – гарантировать пользователям компьютеров безопасную работу. Этим стандартам должен соответствовать каждый монитор, продаваемый как в Швеции, так и в Европе. Рекомендации TCO используются производителями мониторов для создания более качественных продуктов, которые менее опасны для здоровья пользователей. Суть стандартов TCO состоит не только в определении допустимых значений различного типа излучений, но и в определении минимально допустимых технических параметров мониторов, например, поддерживаемых разрешений, интенсивности свечения люминофора, запаса яркости, энергопотребления и т.д.

ISO 9241-3(ИСО 9241) – Международный стандарт, введенный в действие в Европе с 01.01.1997 и используемый в странах ЕС. Стандарт содержит совокупность эргономических требований, в основном, к визуальным параметрам мониторов (отсутствие мерцаний и искажения изображения, соотношение контрастности и др.).

TUV Ergonomie (TUV/EG, TUV/GS) – стандарт по эргономике, разработанный Объединением технического надзора Германии. Монитор со знаком TUV/EG проходит испытания на электрическую безопасность, эргономические показатели и автоматически означает соответствие требованиям стандартов MPR-II,ISO 9241-3.

Сегодня большинство стран имеют свои национальные нормативы, гармонизированные со шведскими стандартами. Но выработка и методические обоснования существенно различаются из-за различных теоретических предпосылок и неоднозначности критериев оценки последствий воздействия факторов.

Другое оборудование, использование которого вызывает беспокойство мирового сообщества- это мобильный телефон.

Мобильный телефон оказывает тепловое воздействие (энергетическое) и нетепловое (вихревое). В результате теплового воздействия (более 10 мкВт/см2) возможны нарушения различных органов человека (помутнение хрусталика глаза, нарушения в функциональных отделах среднего уха и др.) (http://neitronik.com/index-6.htm) .По требованиям Роспотребнадзора допустимый уровень облучения пользователя сотового телефона (http://pandia.ru/text/78/663/21753.php) не должен превышать 100 мкВт/см2. Очевидно, вероятность превышения норматива пиковыми значениями существует.

Таким образом, мобильный телефон является специфическим источником ЭМИ, действие которого имеет прерывистый локальный характер и, исходя из этого, требует особого подхода к санитарному нормированию по допустимому воздействию ЭМИ.

Биологические информационные взаимодействия изучены недостаточно, достоверные результаты исследований в открытой печати найти сложно. Подводя итог всему вышеизложенному надо отметить, что на сегодняшний день нельзя точно сказать, что использование сотового телефона вредно или безопасно. Исследования в данной области проводятся, но их результаты неоднозначны. Для количественной оценки применяют SAR. SAR –SpecificAbsorbtionRate - единица измерения, показывающая максимальную удельную мощность, поглощаемую человеческим телом (Вт/кг) при обычном разговоре по сотовому телефону. Максимальный безопасный уровень – 2,0 большинство современных телефонов имеет SAR от 0,5 до 1,0. Возможно, что на здоровье оказывает влияние не только излучение сотовых телефонов, но совокупность факторов. Например, излучение и нездоровый образ жизни.

В России допустимая интенсивность электромагнитных полей (ЭМП) регламентируется санитарными правилами и нормами, где установлено, что для населения плотность потока энергии (ППЭ) не должна превышать 10 мкВт/ см2 (для жителей Москвы 2 мкВт/ см2), а на рабочих местах 200 мкВт/см2 (Санитарно-эпидемиологические правила и нормативы СанПиН 2.1.8/2.2.4.1383-03 "Гигиенические требования к размещению и эксплуатации передающих радиотехнических объектов") (http://www.vrednost.ru/2241383-03.php) .

Что касается стандарта LTE, то его основные характеристики не сильно отличаются от существующих мобильных технологий. Особенно это касается мощности излучения и диапазона частот. В частности, предназначаемая для LTE полоса частот уже используется различными службами - например, для показа телепередач. Соответственно, исследования уже привычных нам стандартов передачи данных и их воздействия на здоровье человека можно отнести и к технологии LTE.ВОЗ вынесла следующее заключение по мобильным и беспроводным сетям: "С учетом очень низкого уровня излучения, предположение, что слабые радиочастотные сигналы от базовых станций и беспроводных сетей могут нанести серьезный ущерб здоровью человека, не получило научного подтверждения"(http://telecomideas.com/-/news-705866) .

Но с другой стороны, технология LTE предполагает высокую скорость (а значит, большой объем) обмена данными. Значит ли это, что с ростом трафика возрастет излучение от вышек (антенн), каковы пиковые выбросы, присущие технологии и нужны ли новые

нормативы предельно допустимого уровня излучения для сетей LTE? На эти вопросы ответы найти не удалось.

Вред для здоровья, в принципе, несет любой радиосигнал, например сотового телефона или WI-Fiмаршрутизатора, все зависит от того насколько целенаправленно действует сигнал, его величина, постоянство и амплитуда воздействия(http://www.word4you.ru/interesting/20563/). ВОЗ отмечает, что главный эффект от радиоизлучения - нагревание тканей организма. Правда, излучение мобильного телефона по большей части абсорбируется кожей, а в мозгу или других внутренних органах температура повышается незначительно. Специалисты ВОЗ делают акцент именно на том, что в их распоряжении нет никаких веских доказательств и твердых фактов. Поэтому вред от средств радио- доступа, в частности WiFi и мобильных телефонов остается в качестве недоказанного риска (http://fb.ru/article/157648/vred-wifi-routera-vredit-li-wifi-nashemu-zdorovyu).

2.2. Негативное воздействие на здоровье человека пользовательских ИКТ услуг, включая инфокоммуникационные услуги и приложения мобильной связи, электронную почту и социальные сети.

2.2.1. Интернет зависимость

Кроме «компьютерной зависимости», рассмотренной в предыдущем разделе, родственным фактором зависимости является целый ряд типов Интернет- зависимости. Признаками Интернет-зависимости являются навязчивое желание проверить электронную почту, длительное просиживание в чатах, неконтролируемое желание поиска и чтения информации различного рода в сети. В некоторых случаях люди пристращаются к просмотру порнофильмов и чтению порнолитературы на различных сайтах. Этот феномен нельзя назвать Интернет- зависимостью, если кроме этого человек любит читать обычные порножурналы и смотреть порнофильмы по телевизору. В данном случае Интернет является лишь источником информации, а само пристрастие следует рассматривать как нарушение сексуального поведения или сексуальную зависимость.

Немного по-другому обстоит дело с видеоиграми и зависимостью по отношению к ним. В данном случае, как и в случае просмотра порносайтов, компьютер является лишь средством реализации доступа к желаемой информации, сама по себе работа за компьютером, людей страдающих игровой зависимостью, не привлекает (http://www.tiensmed.ru/programmer4.html) .

По данным ряда изданий, например (http://www.m24.ru/articles/74278) Всемирная организация здравоохранения (ВОЗ) планирует признать интернет-зависимость психическим расстройством. Сейчас готовится новая Международная классификация болезней (МКБ-11), куда должны включить и эту проблему. Как только интернет-зависимость попадет в официальный список болезней, ее смогут лечить врачи с помощью препаратов и психотерапии.В мае 2015 года Всемирная ассамблея здравоохранения начала рассмотрение МКБ-11. Окончательный вариант классификации болезней должен быть принят в 2017 году. По данным психологов, такой диагноз смогут ставить зависимым от селфи, онлайн-игр, SMS и соцсетей.

Как свидетельствует опрос (http://wciom.ru/index.php?id=459&uid=114515), проведенный Всероссийским центром исследования общественного мнения (ВЦИОМ) примерно пятая часть (22 процента) россиян признали, что считают себя интернет-зависимыми. В свою очередь, 16 процентов респондентов не могут слишком долго обходиться без общения в социальных сетях, а 11 процентов тратят много времени на проверку электронной почты. Кроме того, каждый пятый респондент сообщает, что много времени проводит за просмотром телевизора или используя мобильный телефон или смартфон. Если говорить об активных пользователях интернета, то из них почти половина, а именно 48 процентов, признаются, что слишком много времени проводят, блуждая по просторам "всемирной паутины"; 34 процента отметили, что склонны засиживаться в социальных сетях. У молодых людей эти показатели еще выше - зависимыми от интернета себя назвали 53 процента, а от соцсетей - 44 процента. Эта же категория страдает излишним пристрастием к мобильным гаджетам - около 39 процентов опрошенных в возрасте от 18 до 24 лет признались, что слишком много времени глядят в экран смартфона.

Данные крупнейшего Научно- исследовательского центра Интернет- зависимости http://netaddiction.com/показывают, что 1 из 8 американцев страдает от чрезмерного использования Internet (Internet Addiction Disorder), а в Китае, Тайване и Кореи эти цифры достигают 30% (http://netaddiction.com/faqs/).

Интернет-зависимость - одна из самых быстро распространяющихся зараз XXI в.: врачи бьют тревогу по всему миру. Только по официальным данным, в Европе и России сейчас от этой болезни страдают от 2 до 4% населения, в Америке - уже больше 10%. В группе риска - более 25% всех жителей развитых и развивающихся стран, говорит еще один источник (http://newsland.com/news/detail/id/321102/).

В Московской городской психологической службе http://msph.ru/выделяют семь типов интернет-зависимости:

- Зависимость просмотра порно-сайтов. Порнозапросы лидируют в поисковиках: 70% взрослых мужчин и 38% женщин время от времени просматривают страницы непристойного содержания.
- Киберсексуальная зависимость. Это онлайн романы, переписка и «киберсекс». Опасность в том, что виртуальный партнер всегда будет лучше реального. Он становится для пользователей интернета идеалом, замещает образ реального супруга, что приводит к конфликтам в семье.
- Зависимость от соцсетей. Для интровертов, одиноких и закомплексованных людей общение в киберпространстве создает иллюзию дружбы и семьи.
- SMS-зависимость. Потребность в обмене моментальными сообщениями, создающая чувство безопасности, востребованности в обществе.
- Зависимость от веб-серфинга. Беспорядочный, хаотичный поиск разнообразной информации в сети. Человек «забивает» мозг ненужными сведениями, чтобы отвлечься от насущных проблем.
- Зависимость от компьютерных игр. Самая опасная для подростков и молодых людей. Известны случаи, когда азартные игроки кончали с собой из-за проигрыша, засиживались до инфаркта или истощения перед экраном.

- Игромания с элементами реальности. Навязчивая потребность играть интернет-казино, аукционы, бирж и азартных игры обычно совмещенная с навязчивым желанием обогатиться.

Надо отметить, что по сравнению с зависимостями от алкоголя и наркотиков, Интернет-зависимость в меньшей степени вредит здоровью человека, не разрушает его мозг, и казалась бы достаточно безопасной, если бы не явное снижение трудоспособности, эффективности функционирования в реальном социуме. Как наркотик, общение в Интернете может создавать иллюзию благополучия, кажущуюся возможность решения реальных проблем (согласно O.Egger, M.Rauterberg “InternetBehaviorandAddiction” http://www.ipo.tue.nl/ipo/people/mrauterb.html).

2.3. Негативное воздействие на здоровье человека использования информационных ресурсов (информации)

Как показал анализ открытых источников, в настоящее время нет достаточно обоснованной и подробной общей классификации влияния информации на человека. Это связано с новизной и сложностью этой проблематики, а также с тем, что сама процедура и результат классификации зависят от тех задач, которые необходимо решить, и в связи с этим — от избираемых оснований и критериев, которые используются при классификации.

2.3.1. Информационная зависимость

Повышенная потребность в информации, а также информационное поле, в котором живет человек, порождают множество проблем. С одной стороны, входящий поток информации, который обрушивается на человека, настолько велик, что с ним временами тяжело справиться. С другой – привычка жить в нем порождает потребность в ее получении – так возникает информационная зависимость.

Речь сейчас не идет об интернет–аддикции, когда человек испытывает потребность находиться в онлайне, а о зависимости от потребления информации, причем в любом виде – бумажном, электронном, аудио или видео (хотя следует отметить, что такая зависимость возникла именно в эпоху Интернета с его огромным информационным потоком).

Результатом этого является притупление восприятия информации – информация не остается в голове, не превращается в знания, а значит, и опыт, не вызывает реакции в виде мыслей.

Мозг, который привык только получать, теряет способность к другим видам мыслительной деятельности – анализу и творческой работе. Подобные ситуации приводят к усталости, в частности, являются одной из причин возникновения синдрома хронической усталости (http://zope.net.ru/publications/computer_and_health_45.html).

2.3.2. Информационно- зависимые заболевания

Стремительный рост использования ИКТ в обществе обозначило отдельные тенденции, которые можно связать с информацией, как фактором риска: увеличение заболеваемости населения психическими расстройствами, неврозами, болезнями системы кровообращения, рост количества самоубийств, высокая доля в структуре смертности информационно-зависимых причин (Увеличение объёма информации в обществе обозначило тенденции, связанные с информацией, как фактором риска для общественного здоровья (http://www.top-technologies.ru/ru/article/view?id=22837).

Наблюдаемые увеличение заболеваемости и инвалидности в связи с психическими расстройствами — прямо, а увеличение заболеваемости болезнями системы кровообращения, рост смертности и высокая доля в структуре смертности информационно-зависимых причин — косвенно, могут быть связаны с неблагополучной информационной средой в стране, регионе и в мире и свидетельствовать о процессах отрицательного воздействия информации на здоровье человека и общества в целом.

По прогнозам ВОЗ, к 2020 году психические заболевания выйдут на первое место в структуре заболеваемости, обогнав сердечно-сосудистую патологию.По статистике ВОЗ, сейчас психическим заболеванием страдает каждый 4-5-й житель планеты, к 2020 году ситуация грозит ухудшиться: будет болен каждый 3-й. Речь, конечно, не идет о серьезных психических заболеваниях, но доля мягких форм и пограничных состояний значительно увеличится.К 2020 году депрессия выйдет на второе место среди причин инвалидности и смертности. Сейчас это заболевание на первом месте по количеству дней нетрудоспособности, которые вынуждены давать врачи в связи с ним.В России официальная статистика сильно расходится с реальным положением дел, но есть данные, согласно которым депрессию той или иной степени тяжести за свою жизнь перенес каждый пятый взрослый. 50% больных депрессией вообще не обращаются за медицинской помощью, в то время как от 45 до 60% всех самоубийств совершаются ими (http://www.rg.ru/2011/05/16/depressiya.html) или (http://www.vigivanie.com/health/2743-psihicheskie-rass.html) .

При анализе структуры причин смертности учитывались, приведенные выше данные источников, по которым возникновение ряда заболеваний сердечно-сосудистой системы, пищеварительной, иммунной систем организма, онкологических болезней, травм и суицидных попыток напрямую или косвенно связано с возникновением у людей психо-эмоционального перенапряжения и стресс- обусловленных последствий в результате воздействия на них социально отягощенной неблагоприятной информации. В соответствии с этим такие причины смерти, как болезни кровообращения, травмы, новообразования, болезни органов пищеварения, самоубийства, были условно отнесены к информационно-зависимым причинам смерти.

В международной классификации болезней 10-го пересмотра (МКБ-10) (http://mkb-10.com/) определены нозологические формы, имеющие этиологическую связь с влиянием информации: психические расстройства и расстройства поведения (классF,F00- F99), острая реакция на стресс (F43), реакция на тяжелый стресс и нарушения адаптации (F43.0), посттравматическое стрессовое расстройство (F43.1), депрессивные эпизоды (F32), рекуррентные депрессивные расстройства (F33); лудомания (игромания)– патологическое влечение к азартным, компьютерным играм, может быть сходно с расстройством поведения, аддиктивным поведением, в том числе интернет-зависимостью (F63.0) и др.; факторы, влияющие на состояние здоровья населения и обращения в учреждения здравоохранения (Класс XXI, Z00- Z99): потенциальная опасность для здоровья, связанная с социально-экономическими и психосоциальными обстоятельствами (Z55-Z65), проблемы, связанные с работой и безработицей (Z56), угроза потерять работу (Z56.2), напряженное рабочее расписание (Z56.3), конфликт с начальником и сослуживцами (Z56.4), неподходящая работа (Z56.5), другое физическое и психическое напряжение в работе (Z56.6).

Кроме того, по информационной теории происхождения эмоций П.В. Симонова (http://www.persev.ru/book/pv-simonov-informacionnaya-teoriya-emociy) и Г. Селье (http://psyera.ru/koncepciya-stressa-g-sele_7517.htm) , социально значимая информация приводит к развитию эмоционального стресса и его последствий в виде заболеваний: сердечнососудистой системы (ИБС, атеросклероз, инфаркты, инсульты и др.), пищеварительной системы (язвенная болезнь), иммунной системы, онкологических болезней, психических заболеваний, повышение уровня травматизма и суицидов (это относится к классам II, IV, V, VI, VII, VIII МКБ-10).

В Международной классификация функционирования, ограничений жизнедеятельности и здоровья (МКФ) ВОЗ (https://extranet.who.int/iris/restricted/bitstream/10665/85389/1/924454542X.pdf) определены функции, связанные с получением, обработкой, производством информации и здоровьем: интеллектуальные функции (код b117); умственные функции (b140-189); преодоление стресса (d240); определены отношения семейные (d760), интимные (d770), романтичные (d7700), супружеские (d7701) и сексуальные (d7702), а также отношения родители – дети (d7600) и дети – родители (d7601),— в формировании которых участвует информация.

Рассмотрим другие сторонынегативного воздействия информации на человека и общество.

2.3.3. Информационно- психологическое воздействие.

Доступ к широкомасштабному использованию новых информационных технологий и контролю за средствами массовой коммуникации многократно усиливает возможности информационно-психологического влияния на людей посредством изменения информационной среды общества. В наибольшей степени это возможно для разнообразных социальных организаций — различных объединений людей, социальных групп, общественных, политических и государственных структур, некоторых социальных институтов общества.

В связи с этим возможно выделить самостоятельных группы источников влияния информации на человека.

Так, для личности может представлять информационно-психологическую опасность деятельность различных группировок и объединений людей, в частности, некоторых политических партий, общественно-политических движений, националистических и религиозных организаций, финансово-экономических и коммерческих структур, лоббистских и мафиозных групп и т.п.

Их деятельность становится опасной, когда для достижения своих целей они начинают применять различного рода средства информационно-психологического воздействия, изменяя посредством этого поведение людей таким образом, что наносится ущерб их же интересам.

В качестве доминантного источника влияния информации, при определенных условиях следует выделить само государство, органы государственной власти и управления. Это связано с действиями государственных лидеров, правящей элиты. Опасность возникает, когда они, реализуя собственные интересы, а иногда и просто амбиции, используют мощь государственного аппарата для оказания информационно-психологического влияния на

людей, маскируя свои действия и истинные цели, которые не соответствуют интересам государства, общества и населения страны.

2.3.4. Искаженная информация (дезинформация)

Если информация подверглась модификации, осуществленной в деструктивных целях, то такая информация определяется как искаженная или дезинформация (http://www.slovochel.ru/dezinformacija.htm) . В социально-политическом аспекте искаженная информация - это информация, претерпевшая под действием определенных способов трансформации и искажения информационных потоков качественные изменения, в результате которых она начинает оказывать негативное воздействие на функционирование политической системы общества. Искаженная информация, таким образом, является деструктивной разновидностью социально значимой информации, искажающей адекватность политической реальности. Трансформация и изменение информации или процессов ее функционирования используется некоторыми субъектами для оказания воздействия на психику людей и их поведение, для психологических манипуляций и оказания манипулятивного воздействия на личность и общество.

В кризисных изменениях общества повышается внушаемость людей, и, соответственно, возрастает подверженность информационно-психологическим влияниям. Она также возрастает в условиях нахождения человека в массовых скоплениях людей, в толпе, на митинге, демонстрации. С человеком происходит своеобразное психическое заражение определенным психоэмоциональным состоянием, что, например, достаточно ярко проявляется на различных зрелищных мероприятиях (http://polbu.ru/grachev_manipul/ch05_all.html).

3. Информационная экология

Таким образом, в современных условиях актуальными вопросами продолжают оставаться взаимосвязь здоровья человека и информационных технологий, нарушения соматического и психического здоровья населения, обусловленные информационными и психоэмоциональными перегрузками.

Все изложенные выше данные вполне соотносятся с выдвигаемой концепцией информационной экологии. Она исходит из признания того, что помимо природной среды обитания человека объективно существует информационная среда его обитания, роль, и значение которой все время возрастает по мере дальнейшего развития средств массовой информации и массовых коммуникаций. Эта среда оказывает на человека активное влияние. Она влияет на формирование и функционирование его личности, на его духовное, интеллектуальное и психическое развитие, состояние психического здоровья.

Неблагоприятная, «загрязненная», деструктивная информационная среда будет отрицательно влиять на личность и психическое здоровье человека по тем же закономерностям, по которым влияет на человека природная среда его обитания. Проблемы информационной экологии не менее важны и практически значимы в эпоху информационного общества, чем вопросы экологии природной среды, которым уделяется постоянное внимание во всем мире(http://www.wayofsociology.ru/wospgs-643-1.html).

Информационная экология – это молодая наука, формирующая свой методологический статус. Из большого объема проанализированных баз научных данных с использованием современных методов информационного поиска удалось найти лишь небольшое количество публикаций по направлению информационной экологии. Причем найденные данные носят разрозненный характер, демонстрируют то, что научный поиск ведется в разных направлениях, и не представляют собой системы знаний. Это может свидетельствовать о начальной стадии разработок в таком перспективном направлении науки, каким может являться «информационная экология».

Согласно Юджину Овумв работе «Экология» (http://dfiles.ru/files/90ip46lsc) и А.П. Парахонскому (http://cyberleninka.ru/article/n/informatsionnaya-ekologiya), информационная экология – «это наука, изучающая закономерности влияния информации на формирование и функционирование человека, человеческих сообществ и человечества в целом, на индивидуальные и общественные взаимоотношения с окружающей информационной средой, а также межличностные и межгрупповые информационные взаимодействия».Таким образом, предметом информационной экологии является изучение взаимодействия человека с информационной средой.

А.Л. Ереминым в работе «Ноогенез и теория интеллекта» (http://a-eremin.ru/rus/) сформулированы основные цели информационной экологии. «Цель: предупреждение отрицательного воздействия и оптимизация благоприятного влияния информации на психическое, физическое и социальное благополучие отдельного человека, социальных групп, и населения в целом, профилактика заболеваний населения, связанных с информацией, оздоровление окружающей информационной среды.

Исходя их анализа работ Шапцева В.А. «Проблематика информационной экологии» (http://www.ipdn.ru/rics/pdf/681.pdf), Еремина А.Л. « Ноогенез и теория интеллекта» (http://a-eremin.ru/rus/), Мизинцевой М.Ф. «Информационная экология и вопросы теории и практики развития информационного общества» (http://ims2000.nw.ru/thes_set.html) и других современных экспертов, пока в информационной экологии, «гигиене информационной среды»остаются не определены следующие вопросы:

- какая по объему и качеству информация для человека полезна, а какая вредна для его здоровья; - гигиенически обоснованные стандарты и рекомендации по «вредной» и «здоровой» информации;

- профилактическая стратегия и рекомендации по устранению такой информации или ее дефицита, что ведет к возникновению эмоционального стресса и его отрицательным влияниям на здоровье человека;
- алгоритмы, кодексы информационного поведения в производственной деятельности различных
профессиональных групп с целью сохранения здоровья людей;

- влияние изменений, наблюдаемых за последние годы в национальной информационной среде, на здоровье населения;

- информационные причины межнациональной ненависти, агрессии отдельного человека, с точки зрения необходимого и достаточного объема и качества информации о другой нации, о другой культуре, о другой вере с целью определения стратегий по сохранению здоровья людей и этносов, приоритеты информационной стратегии в реальной политике при

разрешении конфликтов и кризисов, экстремальных и чрезвычайных ситуаций с целью сохранения жизни и здоровья людей.

Таким образом, информационная экология представляет собой действенное средство защиты человека и общества от негативных воздействий при использовании ИКТ. На основе методологически и методически адекватного анализа степени и качества «загрязненности» информационной среды, ее агрессивности и деструктивности по отношению к личности и психическому здоровью человека необходимо приступить к научно обоснованному определению понятия и категорий предельно допустимых, экстремально высоких и высоких концентраций негативно влияющей информации.

3.1. Основные роли и обязанности заинтересованных сторон экосистемы ИКТ в области информационной экологии

Рассмотрим основные роли и обязанности заинтересованных сторон экосистемы ИКТ в области информационной экологии.

Заинтересованная сторона	**Роли и обязанности в экосистеме ИКТ в области информационной экологии**
Государство (правительства)	- Разработка государственной политики в области профилактики, предотвращения негативных воздействий на человека и общество при использовании ИКТ. Поддержка ее реализации в виде самостоятельных целевых национальных программ, либо как составной части доктрины и/или государственной политики в области здравоохранения и информационной безопасности государства; - Поддержка на государственном уровне всестороннего развития информационной экологии как науки. Создание законодательной базы правового, методического, научно-технического, образовательного, медико- профилактического и организационного обеспечения практической реализации ее целей и задач; - Создание законодательной базы кодексов и правил информационного обеспечения и поведения органов управления, специализированных федеральных и региональных служб. - Создание и координация деятельности межведомственных региональных центров (например, госсаннадзора), осуществляющих комплексный социально-гигиенический мониторинг информационной среды, в частности негативных факторов воздействий при использовании ИКТ. - Содействие корректности, правдивости и гуманности трансляции массовой информации для предотвращения межэтнических, межнациональных, религиозных войн, революционных процессов в гражданском обществе, социальных и финансовых катаклизмов.

Бизнес- сообщество	- Организация постоянного мониторинга за информационно-зависимыми факторами воздействия и информационной средой и влиянием на человека на производстве; - Участие в разработке национального законодательства, стандартов и инструментария в области информационной экологии. Поддержка научных исследований и образования. - Разработка предложений по кодексам правил и профессиональной компетенции, а также деонтологии профессиональных групп; - Разработка принципов эколого- гигиенического информационного поведения на производстве и его реализация на предприятиях и в организациях отраслей экономики, а также в лечебно- профилактических учреждениях.
Образовательные и научные организации	- Создание на основе компьютерных технологий единой информационной системы статистики влияния информационной среды на здоровье человека и общества; -Разработка научно- обоснованных предложений, рекомендаций для стратегии государственной политики здравоохранения и информационной безопасности в области оптимизации информационно- зависимого здоровья населения; - Проведение исследований характеристик и закономерностей информационных воздействий при использовании ИКТ. Исследование механизмов восприятия, переработки, хранения и производства новой информации, зависимости индивидуального и общественного здоровья от информации; - Разработка гигиенических нормативов безопасной информационной среды и использования ИКТ. Разработка научно- обоснованного гигиенического информационного поведения человека и общества; - Разработка модулей образовательных программ в области информационной экологии для включения в учебный процесс. Проведение курсов повышения квалификации, семинаров, конференций.
Международные (межправительственные) организации	- Координация действий государств и правительств различных стран в области предупреждения и противодействия негативным воздействиям при использовании ИКТ; - Принятие международно-правовые конвенций, создание специальных рабочих групп, комитетов и других органов в

	области стратегий политики информационной экологии и практической реализации ее целей и задач; - Организация обмена мнениями между государствами, межправительственными и неправительственными организациями и отдельными экспертами, представляющими различные специальности и смежные области знаний информационной экологии. Выявление новых тенденций и проблем, предоставление странам эффективной помощи, разработка и представление рекомендаций по соответствующим вопросам.
Гражданское сообщество	- Расширение информированности общественности, пропаганда вредности и опасности негативных воздействий и средств их профилактики и предотвращения; - Личное участие в оздоровление окружающей информационной среды; - Участие в курсах повышения квалификации, семинарах, конференциях, посвященных информационной экологии. Распространение опыта и знаний в обществе; - Предоставление экспертов, специалистов, опыта и знаний по ряду направлений политики в области информационной экологии; - Участие в опросах общественного мнения, в исследованиях, в натурных экспериментах, посвященных вопросам информационной экологии.

4. Модель оценки негативных воздействий на здоровье человека и общества при использовании ИКТ

На вход модели поступает суммарный поток, характеризующий рассмотренные выше негативные воздействия от использования ИКТ, а именно возникающие от:

1) Использования оконечного (терминального) ИКТ оборудования, включая компьютеры, планшеты, маршрутизаторы радио доступа и ретрансляторы (WiFi) и Периферийные устройства (принтеры, сканеры);

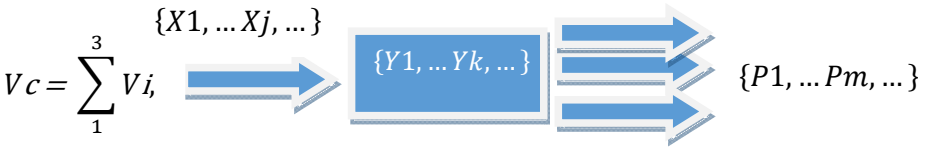
2) Пользовательских ИКТ услуг, включая инфокоммуникационные услуги и приложения мобильной связи, электронную почту социальные сети;

3) Использования информационных ресурсов (информации).

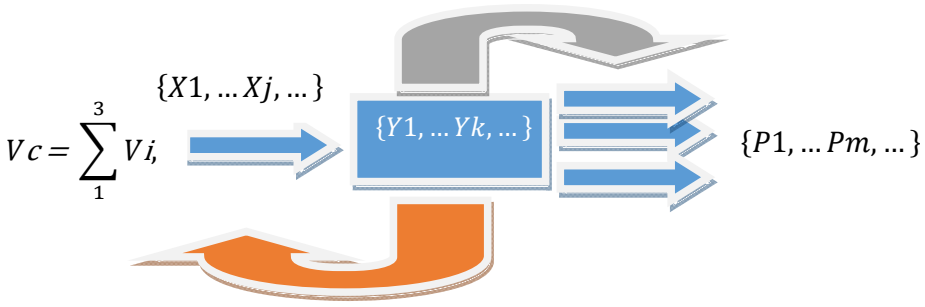
Суммарный поток негативных воздействий $Vc = \sum_1^3 Vi,$ где i- тип источника воздействия. Каждый тип воздействия характеризуется параметрами $Vi = \{X1, \dots Xj, \dots\}$, такими как направленность, интенсивность, продолжительность. Значения параметров определяем как дискретные, например, используя следующие: допустимые, опасные, предельно- допустимые или незначительные, средние, высокие…

Суммарный поток воздействий направлено на человека, который характеризуется набором состояний $Sc = \{Y1, \dots Yk, \dots\}$, таких как возраст, профессиональная принадлежность, образование, доход, семейное положение, условия проживания, состояние здоровья,…

На выходе модели–прогнозируемые последствия воздействий на человека $\{P1, \dots Pm, \dots\}$ например, в виде усталости, психических заболеваний, ухудшения зрения и т.п.



Данная модель еще больше усложнится, если учитывать состояния группы людей, общества, другие заинтересованные стороны, что предполагает взаимодействие между ними для достижения цели- профилактики и предотвращения эффекта негативного воздействия, например за счет разработки нормативов, рекомендаций, ограничительных мер на уровне государства (правительств). Кроме того, в модели можно предусмотреть меры по смягчению или ликвидации последствий воздействий за счет, например, лечебной физкультуры, процедур, психологической помощи, лечения.



Очевидно, что дальнейшее формализованное описание модели, а также получение результатов моделирования представляет собой сложнейшую задачу. Ее решение предполагает привлечение различных методов и средств, математического, имитационного аппарата.

4.1. Методы и средства исследования.

Анализ открытых источников (например, http://www.ipdn.ru/rics/doc1/OD/1-sha.htm, http://gtmarket.ru/concepts/7111, http://npar.ru/journal/2003/1/influence.htm, http://www.science-education.ru/ru/article/view?id=13738) позволил определить следующие методы и средства:

1) Системный анализ процессов восприятия человеком информации с целью создания хотя бы упрощенных математических, алгоритмических, компьютерных моделей восприятия информации. Здесь могут быть использованы самые разнообразные подходы, наработанные в прикладной математике, теории вероятностей и механике.

2) На начальном этапе исследования развития, возможно, придется использовать разнообразные идентификационные эксперименты, специализированные лабораторные комплексы, применимы психофизиологические методы, социологические исследования.

3) С помощью психологических тестов и шкал, методик, фиксирующих вегето-сосудистые реакции на эмоционально значимые информационные воздействия, с помощью методов нейровизуализации (позитронно-эмисионная томография, ЭЭГ картографирование) можно разработать допустимые и недопустимые с точки зрения влияния на психическое здоровье качественные и количественные параметры информационных воздействий.

4) Для решения задач информационной гигиены, особенно в ходе натурных исследований, рекомендуется использовать такие методы, как хронометраж (в том числе самонаблюдение), методы экспертных оценок, интервьюирование и анкетирование (в том числе оценку качества жизни). В рамках лабораторного эксперимента, с участием волонтеров возможно применение более сложных нейрофизиологических исследований.

5) Основные методы оценки влияния среды на здоровье человека: методы клинической эпидемиологии, статистического анализа данных и DataMining (например, http://www.statistica.ru/local-portals/data-mining/) . Это совокупность методов обнаружения в данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности.Основу методов Data Mining составляют всевозможные методы классификации, моделирования и прогнозирования, основанные на применении деревьев решений, искусственных нейронных сетей, генетических алгоритмов, эволюционного программирования, ассоциативной памяти, нечёткой логики.

5. Основные результаты.

1. Исследование современных аспектов использования ИКТ
2. Анализ содержания и элементов экосистемы ИКТ
3. Разработка представления экосистемы ИКТ с точки зрения использования ИКТ
4. Разработка рекомендаций по содержанию ролей и обязанностей заинтересованных сторон экосистемы ИКТ
5. Исследование существующих подходов к классификации ИКТ
6. Разработка классификации ИКТ по образующим ИКТ технологиям, в зависимости от предметной области, в зависимости от типа обрабатываемой информации
7. Разработка классификации ИКТ с точки зрения использования ИКТ
8. Разработка классификации источников негативного влияния на здоровье человека при использовании ИКТ
9. Анализ негативного воздействия на здоровье человека при использовании оконечного (терминального) оборудования
10. Анализ вредных и опасных факторов воздействия при использовании оконечного (терминального) оборудования и дополнение существующей их классификации социально- патологическими факторами
11. Анализ существующей базы в области стандартов
12. Анализ негативного воздействия на здоровье человека пользовательских ИКТ услуг и приложений

13. Анализ негативных воздействия на здоровье человека использования информационных ресурсов (информации), включая информационную зависимость, информационно- зависимые заболевания, информационно- психологическое воздействие, искаженную информацию (дезинформацию)
14. Анализ состояния разработок в области информационной экологии, ее целей и задач
15. Разработка рекомендаций по содержанию ролей и обязанностей заинтересованных сторон в области информационной экологии
16. Разработка модели оценки негативного воздействия на здоровье человека и общества при использовании ИКТ
17. Рекомендации по применению методов и средств исследования в рамках модели.

Приложение 8. Деятельность МСЭ и РСС по укреплению доверия и безопасности при использовании ИКТ

В период с 30 марта по 10 апреля 2014 г. в городе Дубай, ОАЭ состоялась Всемирная конференция по развитию электросвязи МСЭ (ВКРЭ-14).

Конференция рассмотрела основные документы по вопросам развития информационно-коммуникационной инфраструктуры и технологий, кибербезопасности, приложений на базе ИКТ, Интернета, электросвязи в чрезвычайных ситуациях и изменения климата, по вопросам финансирования деятельности МСЭ.

В работе Конференции приняли участие делегации администраций связи Республики Таджикистан, Азербайджанской Республики, Республики Армения, Республики Беларусь, Грузии, Республики Казахстан, Кыргызской Республики, Республики Молдова, Российской Федерации, Республики Узбекистан, Украины, а также Исполкома РСС.

В период с 20 октября по 7 ноября 2014 года в Пусане (Республика Корея) прошла Полномочная конференция МСЭ 2014 года (ПК-14).

В работе Конференции приняли участие администрации связи полноправных членов: Республики Таджикистан, Азербайджанской Республики, Республики Армения, Республики Беларусь, Грузии, Республики Казахстан, Кыргызской Республики, Республики Молдова, Российской Федерации, Туркменистана, Республики Узбекистан, Украины и наблюдателей: Республики Болгария, Латвийской Республики, Литовской Республики, Республики Словения, МОКС «Интерспутник» и МО «Евтелсат» и представители Исполкома РСС.

Доверие и безопасность при использовании ИКТ имеют основополагающее значение при построении безопасного, глобального и открытого для всех информационного общества. Доверие и безопасность имеют важнейшее значение для эффективного использования ИКТ, что было подтверждено на Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО).

Юридические, технические и институциональные проблемы, возникающие в связи с кибератаками и киберпреступностью, носят глобальный характер и имеют далеко идущие последствия, и поэтому они могут быть решены только путем принятия согласованной стратегии, в которой учитывается роль различных заинтересованных сторон, а также существующие инициативы в рамках международного сотрудничества.

Предпринимающиеся попытки решить эти проблемы на национальном и региональном уровнях являются неэффективными, поскольку киберпространство не имеет пределов и ограничено лишь человеческим воображением. Границы информационного общества точно не соответствуют существующим географическим границам, и поэтому киберугрозы могут возникнуть где угодно и в любое время и нанести громадный ущерб за очень короткий промежуток времени, прежде чем они будут устранены.

Глобальная программа кибербезопасности (ГПК) представляет для МСЭ основу международного сотрудничества, цель которого состоит в том, чтобы предложить стратегии для поиска решений в области укрепления доверия и безопасности в условиях информационного общества. Программа будет основываться на существующих национальных и региональных инициативах, для того чтобы избежать дублирования в работе и поддержать сотрудничество всех соответствующих партнеров.

Вопросы, связанные с киберугрозами, носят глобальный характер. Страны не могут просто закрыть свои границы перед лицом надвигающихся киберугроз. Временные и географические факторы, а также местонахождения потенциальных жертв больше не являются препятствием для места и времени совершения этих атак киберпреступниками. Все попытки решить эти проблемы на национальном и региональном уровнях оказались недостаточными. Юридические и технические меры на национальном и региональном уровнях необходимы, однако их недостаточно, для того чтобы преодолеть эти глобальные угрозы.

Для того чтобы разработать глобальное решение по преодолению этих проблем, важно, чтобы все страны достигли общего понимания в вопросе о том, что означает кибербезопасность. Кибербезопасность обеспечивает защиту от несанкционированного доступа, манипулирования критически важными ресурсами и активами, например данными, и их разрушения. Ценность этих ресурсов и активов в разных странах различна, и частично она зависит от уровня развития и вида экономической деятельности. Она зависит также от того, что каждая страна считает своими критически важными ресурсами, усилий, которые она готова и способна приложить, а также ее оценки рисков, на которые она готова пойти в сопоставлении с мерами, которые она готова осуществить в области кибербезопасности.

Многие наименее развитые страны рассматривают кибербезопасность главным образом как одно из средств распространения преимуществ ИКТ посредством поставки безопасных и высоконадежных услуг в таких секторах, как здравоохранение, торговля, государственное управление и финансы. Их потребности, приоритеты и стратегии в области кибербезопасности необязательно являются такими же, что и у большинства развитых стран. Однако многие развитые страны, помимо прочих угроз, таких как онлайновое мошенничество, угроз в сфере защиты потребителя и конфиденциальности, также рассматривают решения в области кибербезопасности в качестве одного из средств защиты и сохранения целостности своих критически важных инфраструктур в финансовом секторе, секторах здравоохранения, энергетики, транспорта, электросвязи, обороны, а также других секторах. Поэтому защита критической информационной инфраструктуры (CIIP) является основным вопросом в повестке дня большинства, или может быть всех, стран.

В настоящее время, когда в мире, по приблизительным оценкам, услугами интернета пользуются порядка одного миллиарда человек, становится очевидным, что страны с различными уровнями развития, различными приоритетами и различными проблемами могут иметь различные точки зрения по таким глобальным вопросам, как киберугрозы и неэффективные решения по вопросам кибербезопасности.

МСЭ, насчитывающий 191 Государство-Член и свыше 700 Членов Секторов и Ассоциированных членов, имеет уникальные возможности, для того чтобы попытаться достичь консенсуса относительно основ для международного сотрудничества в области кибербезопасности. Среди его членов: наименее развитые страны, развивающиеся страны и страны с формирующейся рыночной экономикой, а также промышленно развитые страны. Поэтому МСЭ является важнейшим форумом, в рамках которого можно обсуждать различные мнения, касающиеся кибербезопасности и киберпреступности, в том числе мнения представителей частного сектора, для того чтобы достичь понимания между всеми заинтересованными сторонами и обсудить вопросы о том, каким образом эффективнее всего решать эти проблемы на глобальном уровне.

Мандат МСЭ в области стандартизации и развития электросвязи был признан мировыми лидерами, назначившими МСЭ ведущей/содействующей организацией по Направлению деятельности С5 ВВУИО. Такое признание подтверждает, что МСЭ является идеальным форумом для разработки и претворения в жизнь решений, направленных на устранение глобальных проблем в области обеспечения кибербезопасности.

Стратегия по выработке решения должна определять существующие национальные и региональные инициативы, работу со всеми соответствующими сторонами для выявления приоритетов и объединения партнеров с целью выработки глобальных решений по преодолению глобальных проблем, с которыми мы сталкиваемся сегодня.

Единственным способом решения этих глобальных проблем и построения надежного и безопасного информационного общества для всех наций и народов является работа с ключевыми партнерами по вопросам, по которым можно достичь общего понимания.

Совместно с партнерами – представителями правительственных учреждений, отрасли, соответствующих региональных/ международных организаций, научно- исследовательских институтов, академических учреждений, а также индивидуальных экспертов, МСЭ, таким образом, создал глобальную систему для ведения диалога и осуществления международного сотрудничества, для того чтобы предложить стратегии для выработки решений в целях укрепления безопасности и доверия в условиях информационного общества. Глобальная программа кибербезопасности (ГПК) объединит существующие инициативы, а также партнеров, для того чтобы предложить глобальные стратегии по решению современных проблем в борьбе с киберпреступностью и поддержанию кибермира. Конечная цель Глобальной программы кибербезопасности состоит в достижении значительного прогресса в отношении согласованных целей в борьбе с киберпреступностью и повышения уровня доверия и безопасности в информационном обществе. Она основана на международном сотрудничестве и нацелена на то, чтобы привлечь все соответствующие заинтересованные стороны к участию в согласованной работе по укреплению безопасности и доверия в информационном обществе.

Пять принципов, лежащих в основе Глобальной программы кибербезопасности МСЭ Глобальная программа кибербезопасности МСЭ основывается на 5 (пяти) стратегических принципах:

- Правовые меры;
- Технические и процедурные меры;
- Организационные структуры;
- Создание потенциала;
- Международное сотрудничество.

Правовые меры

Создание соответствующей правовой инфраструктуры является неотъемлемым компонентом любой национальной стратегии в области кибербезопасности. В рамках Дохинского плана действий (ДПД) 2006 года Бюро развития электросвязи (БРЭ) МСЭ оказывает содействие Государствам-Членам в понимании правовых аспектов кибербезопасности в целях согласования их нормативно-правовых баз.

Издание "Понимание киберпреступности: руководство для развивающихся стран", опубликованное в мае 2009 года, является важной составляющей этой работы и разработано в качестве инструмента для развивающихся стран, который поможет им лучше понимать и оценивать национальные и международные последствия возрастающих киберугроз. В том же году БРЭ опубликовало "Комплект материалов по законодательству в области киберпреступности", разработанный группой экспертов, с тем чтобы предоставить Государствам-Членам типовые тексты законов и справочный материал для содействия в согласовании законов и процессуальных норм в области киберпреступности. БРЭ разработало также вспомогательный документ под названием "Кибербезопасность: роль и обязанности эффективного регуляторного органа" для представления его на Глобальном симпозиуме для регуляторных органов, который состоялся в Бейруте, Ливан, в ноябре 2009 года.

Технические и процедурные меры

Работа МСЭ в области безопасности охватывает широкий спектр деятельности — от сетевых атак, отказа в обслуживании, хищения идентификационных данных, несанкционированного извлечения информации, телебиометрической аутентификации до обеспечения безопасности электросвязи в случае чрезвычайных ситуаций.

Наряду со многими ключевыми рекомендациями по вопросам безопасности, МСЭ–Т составил обзор требований в области безопасности, разработал руководящие указания по обеспечению безопасности для авторов протоколов, требования к защите систем, базирующихся на IP, а также руководство по способам определения киберугроз и ответных мер для смягчения рисков. МСЭ–Т также обеспечивает международную платформу для разработки протоколов, защищающих существующие сети и сети последующих поколений (СПП).

В процессе перехода к услугам на базе протокола Интернет (IP) в Рекомендациях МСЭ серии H.235.x по теме "Безопасность H.323" определяются инфраструктура и услуги по обеспечению безопасности (включая аутентификацию и конфиденциальность) для использования базирующимися на IP мультимедийными системами по Рекомендации серии H.300 (такими, как VoIP и видеоконференц-связь) в приложениях на основе связи пункта с пунктом и связи со многими пунктами. Стандарты H.235.x обеспечивают конфиденциальность для поставщиков услуг и предприятий, гарантируя при этом взаимодействие мультимедийных продуктов. Идентификационные данные пользователей, обменивающихся информацией через IP-носитель, надлежащим образом аутентифицируются и авторизуются с помощью H.235.x, что защищает их сеансы связи от разных серьезных угроз безопасности.

В Рекомендации МСЭ X.805 определяется архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами. Эта Рекомендация позволяет операторам точно определять и устранять уязвимые точки в сети, а структура безопасности МСЭ дополняет это с помощью соответствующих руководящих указаний по защите от кибератак.

В Рекомендациях МСЭ–Т X.1205 "Обзор кибербезопасности" представлены определение кибербезопасности и таксонометрия угроз безопасности. В ней описывается

характер условий и рисков в аспекте кибербезопасности, возможные стратегии сетевой защиты, методы защищенной связи и живучесть сети (даже в случае атаки).

За прошедший с сентября 2009 года период были созданы семь групп, работающих по переписке, по вопросам, касающимся координации в целях обеспечения безопасности, электронного здравоохранения, безопасности "облачных вычислений" и "умных" электросетей, национальных центров сетевой безопасности (NCNS), стратегии обеспечения безопасности онлайновых транзакций, децентрализованной архитектуры для глобальной системы разрешения имен в IP-сетях и системы обмена информацией по кибербезопасности (CYBEX).

Обращение к радиосвязи, беспроводным приложениям, таким как 3G (или IMT-2000), становится неотъемлемой частью повседневной жизни, а глобальное использование и управление использованием частот требуют высокого уровня международного сотрудничества. Глобальное управление использованием частот приобретает все большее значение для укрепления доверия и безопасности при использовании ИКТ.

Это выдвигает на передний план функцию МСЭ–R по обеспечению рационального, справедливого, эффективного и экономного использования радиочастотного спектра всеми службами радиосвязи, включая те, которые используют спутниковые орбиты, а также по проведению исследований и принятию Рекомендаций по вопросам радиосвязи.

Защита качества обслуживания от ухудшения или отказа в обслуживании имеет решающее значение для безопасного функционирования сетей, и многие из последних Рекомендаций МСЭ–R по общим требованиям и защите радиосвязи от помех касаются проблем безопасности. МСЭ продолжает свою деятельность в области стандартизации радиосвязи, обеспечивая ее соответствие постоянной эволюции современных сетей электросвязи.

МСЭ–R утвердил Рекомендации по принципам и механизмам обеспечения безопасности для сетей 3G (в частности, Рекомендацию МСЭ–R M.1078, а также Рекомендации M.1223, M.1457 и M.1645). Кроме того, он выпустил Рекомендации по вопросам безопасности в архитектуре сетевого управления для цифровых спутниковых систем (Рекомендация МСЭ–R S.1250) и по улучшению качественных показателей протокола управления передачей по спутниковым сетям (Рекомендация МСЭ–R S.1711).

Организационные структуры

Нехватка организационных структур для урегулирования киберинцидентов (атак, мошенничества, уничтожения информации, распространения неподобающего контента) является настоящей проблемой при реагировании на киберугрозы. БРЭ, совместно с ИМПАКТ, разворачивает имеющиеся средства в целях создания потенциала на национальном и региональном уровнях. В настоящее время осуществляется координация деятельности с рядом Государств — Членов МСЭ, причем основное внимание уделяется оказанию помощи в создании национальных групп реагирования на компьютерные инциденты (CIRT).

При поддержке, полученной от правительства Австралии, и в партнерстве с другими организациями (например, AusCERT и ИМПАКТ) МСЭ оказывает помощь островным странам Тихоокеанского региона в создании Тихоокеанской группы реагирования на

компьютерные чрезвычайные ситуации (CERT). МСЭ, в сотрудничестве с ИМПАКТ, также оказал Афганистану помощь в изучении возможностей создания национальной группы CERT.

Создание потенциала

Самым слабым звеном являются люди. Одна из ключевых проблем кибербезопасности — это обучение конечного пользователя. Понимание потенциальных опасностей и информированность о них являются крайне важными аспектами обеспечения того, чтобы конечный пользователь в безопасности получал пользу от ИКТ.

Эта проблема касается всех заинтересованных сторон — от органов государственного управления и отрасли до образования как в школе, так и дома. Огромное значение имеет информированность о возможностях, предлагаемых безопасной киберсредой, и об угрозах, присущих киберпространству. Важным моментом является выполнение программ, нацеленных на повышение информированности и создание потенциала на всех уровнях, и такие программы необходимо также осуществлять в международном масштабе.

Чтобы оказать помощь Государствам-Членам, желающим разработать собственный национальный подход к вопросам кибербезопасности и защиты важнейшей информационной инфраструктуры (CIIP), БРЭ разработало Набор средств для самостоятельной оценки состояния национальной кибербезопасности/CIIP, и в настоящее время обновляет текущую версию. БРЭ разработало также Набор средств МСЭ для защиты от бот-сетей с целью отслеживать бот-сети и смягчать их воздействие, причем особое внимание уделяется проблемам, характерным для стран, экономика которых лишь начинает базироваться на интернете.

БРЭ организует региональные форумы по кибербезопасности для всех регионов МСЭ, используя их в качестве средства создания потенциала для различных программ и видов деятельности, а также как рабочие платформы для сотрудничества на региональном и международном уровнях.

Международное сотрудничество

Интернет и ИКТ позволили организовать присоединение между странами, которое раньше было невозможным. Страны не могут просто закрыть свои границы для входящих киберугроз, а также не могут удержать киберугрозы, исходящие изнутри. Попытки решить эти проблемы на национальном или региональном уровнях представляются важными, но поскольку кибербезопасность является столь же глобальной и масштабной, как и интернет, решения необходимо согласовывать через все границы. Для этого необходимо международное сотрудничество не только на правительственном уровне, но и с отраслью, неправительственными и международными организациями.

Международное многостороннее партнерство против киберугроз (ИМПАКТ)

Сотрудничество МСЭ–ИМПАКТ — это глобальное, с участием многих заинтересованных сторон, партнерство государственного и частного секторов, которое является физической и оперативной базой для реализации Глобальной программы кибербезопасности (ГПК) МСЭ. На август 2010 года более 50 Государств-Членов официально согласились принять участие в развертывании услуг, предлагаемых МСЭ–ИМПАКТ. МСЭ проводит в Женеве "виртуальную демонстрацию" системы раннего

оповещения, управления кризисными ситуациями и анализа в режиме реального времени глобальных киберугроз.

Портал кибербезопасности МСЭ

Портал кибербезопасности МСЭ был обновлен в 2009 году в целях обеспечения лучшего доступа к информации, ее распространения и сотрудничества в онлайновом режиме между заинтересованными сторонами, работающими в области кибербезопасности, с возможностями осуществления обратной связи, предусмотренными в этом портале.

Защита ребенка в онлайновой среде

В рамках Программы глобальной кибербезопасности МСЭ, в сотрудничестве с другими учреждениями ООН и партнерскими организациями, в ноябре 2008 года приступил к выполнению программы "Защита ребенка в онлайновой среде" (COP) в рамках международной совместной инициативы для принятия мер по содействию обеспечения кибербезопасности детей и молодежи путем подготовки руководящих указаний по безопасному поведению в онлайновой среде. Было организовано несколько мероприятий, примерами которых являются Стратегический диалог по более безопасной среде интернета для детей, проведенный в июне 2009 года в Токио, Япония, и Открытый форум по защите ребенка в онлайновой среде, организованный в ходе проведения 4-го Форума по вопросам управления использованием интернета (ФУИ) в ноябре 2009 года. Руководящие указания по защите детей в онлайновой среде были разработаны для директивных органов, отрасли, преподавателей, родителей, опекунов и детей. Они были подготовлены МСЭ в тесном сотрудничестве со многими организациями, в том числе Межрегиональным научно-исследовательским институтом Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ), Детским фондом Организации Объединенных Наций (ЮНИСЕФ), Управлением по наркотикам и преступности Организации Объединенных Наций (ЮНОДК), Институтом Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР), Интерполом и Европейским агентством по вопросам сетевой и информационной безопасности.

Не только киберпреступники угрожают интернету. Уязвимые аспекты ИКТ привлекают и потенциально более опасные виды деятельности, такие как шпионаж. Появились такие явления, как война и шпионаж в киберпространстве, и они могут представлять серьезную угрозу для важнейшей информационной инфраструктуры.

Киберугрозы носят глобальный характер, и поэтому решения также должны быть глобальными. Крайне важно, чтобы все страны достигли общего понимания по вопросам кибербезопасности в целях обеспечения защиты от несанкционированного доступа, мошенничества и уничтожения важнейших ресурсов.

МСЭ полагает, что стратегия при принятии того или иного решения должна включать выявление существующих национальных и региональных инициатив, для того чтобы установить приоритеты и эффективно работать со всеми игроками, имеющими отношение к данному вопросу. МСЭ, с учетом входящих в его состав 192 Государств-Членов и более чем 700 компаний и ассоциаций частного сектора, служит прекрасным форумом для принятия мер и реагирования в целях содействия кибербезопасности и борьбы с киберпреступностью. Его широкий членский состав включает наименее развитые страны, развивающиеся страны и страны с формирующейся рыночной экономикой, а также развитые страны.

Правовая база, технические меры и организационные структуры должны быть реализованы на национальном и региональном уровнях, однако согласованы на международном уровне. Последние два основополагающих принципа, а именно создание потенциала и международное сотрудничество, проходят по всем областям (см. рисунок на последней странице). Чтобы выполнить свою программу, МСЭ полностью вовлечет в этот процесс свои Государства- Члены и всех действующих лиц на мировой арене. Он будет тесно сотрудничать со своими партнерами, для того чтобы выявить имеющиеся проблемы, изучить возникающие и будущие угрозы и предложить глобальные стратегии для достижения целей Программы.

Глобальная программа кибербезопасности будет способствовать реализации деятельности, направленной на достижение Стратегических целей МСЭ в этой области, путем разработки и предложения прогрессивных глобальных стратегий, опираясь на обширный опыт и учитывая существующие инициативы.

Установление достижимых целей. Глобальная программа кибербезопасности преследует семь основных стратегических целей:

1) Формирование стратегий для разработки типового законодательства по борьбе с киберпреступностью, которое можно было бы применять в глобальном масштабе и которое было бы совместимо с действующими национальными и региональными мерами законодательного характера.

2) Формирование глобальных стратегий для создания надлежащих национальных и региональных организационных структур и политики в области борьбы с киберпреступностью.

3) Разработка стратегии для установления приемлемых на глобальном уровне минимальных критериев безопасности и схем санкционирования для аппаратных средств и программных приложений и систем.

4) Разработка стратегий для создания глобальной структуры для наблюдения, оповещения и реагирования на инциденты для обеспечения международной координации деятельности в рамках новых и существующих инициатив.

5) Разработка глобальных стратегий для создания и утверждения общей и универсальной системы цифровой идентификации, а также необходимых организационных структур в целях обеспечения признания цифровых удостоверений личности без учета географических границ.

6) Разработка глобальной стратегии в целях содействия созданию человеческого и институционального потенциала для увеличения знаний и ноу-хау в секторах и во всех вышеупомянутых областях.

7) Подготовка предложений по основе глобальной стратегии, основанной на участии многих заинтересованных сторон, в целях налаживания международного сотрудничества, диалога и координации деятельности во всех вышеупомянутых областях.

Доверие и безопасность сохраняют свое важное место среди основ создания информационного общества:

- Поощрение дальнейшего укрепления доверия и основ безопасности посредством дополняющих и взаимоукрепляющих инициатив в областях безопасности при использовании ИКТ, инициатив или руководящих указаний в отношении прав на конфиденциальность, защиту данных и потребителей;
- Поддержка дальнейшего развития и поощрение осуществления международных стандартов безопасности, в частности открытых стандартов. Дальнейшая помощь развивающимся и наименее развитым странам для их участия в разработке глобальных стандартов и связанных с этим процессах;
- Обеспечение особого внимания защите детей и расширению их прав и возможностей в онлайновой среде. В связи с этим правительствам и другим заинтересованным сторонам следует работать вместе, чтобы сделать возможным использование всеми преимуществ ИКТ в безопасной и защищенной среде;
- Укрепление поддержки создания национальных групп реагирования на компьютерные инциденты (CIRT), в том числе CIRT, ответственных за межправительственное сотрудничество при управлении операциями при инцидентах, где это необходимо, и координации их действий на региональном и международном уровнях, для действий и реагирования на инциденты в режиме реального времени, в особенности в отношении критически важных национальных инфраструктур, в том числе информационных инфраструктур, с учетом национального законодательства.
  е) Дальнейшее содействие развитию основ оценки для измерения подготовленности стран по различным аспектам доверия и безопасности при использовании ИКТ;
- Содействие исследованиям и сотрудничеству, делающим возможным эффективное использование данных и программного обеспечения, в частности электронных документов и транзакций, включая электронные средства аутентификации и совершенствование методов обеспечения безопасности.

Во время сессии Совета МСЭ 2015 года была дана высокая оценка деятельности МСЭ по укреплению доверия и безопасности при использовании ИКТ. Была подчеркнута важность регионального и международного взаимодействия, а также широкой основы для сотрудничества, осуществляемого МСЭ. Секретариат согласился с Советом в том, что взаимодействие на всех уровнях является неотъемлемой частью работы в этой сфере, особенно в том, что касается максимального повышения эффективности деятельности различных организаций.

Большую роль в укреплении доверия и безопасности при использовании ИКТ в государствах СНГ и Грузии играет деятельность Регионального содружества в области связи (РСС) стран СНГ, Совета глав государствСНГ и Совета глав правительств СНГ по вопросам дальнейшего сотрудничества в области ИКТ.

Реализация решений Совета глав государств СНГ от 5 октября 2007 года о Концепции дальнейшего развития Содружества Независимых Государств и о Плане основных мероприятий по реализации Концепции дальнейшего развития СНГ, а также Решения Совета глав правительств СНГ от 14 ноября 2008 года о Стратегии экономического развития Содружества Независимых Государств на период до 2020 года открыли новые возможности

для сотрудничества в построении информационного общества и развитии информационно-коммуникационных технологий в рамках СНГ.

Отличительными чертами информационного общества являются: увеличение роли информации и знаний в жизни общества; возрастание доли ИКТ в объеме ВВП, создание глобального информационного пространства, обеспечивающего эффективное информационное взаимодействие, свободный доступ к мировым информационным ресурсам и удовлетворение потребностей граждан в информационных продуктах и услугах.

В инновационной сфере информационные услуги и ИКТ, реализуемые на основе технологической модернизации, становятся приоритетными направлениями социально-экономического развития общества.

Решением Совета глав правительств СНГ от 24 ноября 2006 года утверждены Стратегия сотрудничества государств – участников СНГ в сфере информатизации (Стратегия) и План действий по ее реализации на период до 2010 года (План действий), которые определяют перспективы взаимовыгодного сотрудничества в области развития ИКТ и построения информационного сообщества в государствах – участниках СНГ. В реализации Стратегии и Плане действий принимают участие семь государств – участников СНГ (кроме Азербайджанской Республики, Туркменистана, Республики Узбекистан и Украины).

Указанным Решением Совета глав правительств СНГ от 24 ноября 2006 года Координационный совет государств – участников СНГ по информатизации при Региональном содружестве в области связи (Координационный совет) определен координатором мероприятий по реализации Стратегии, и ему поручено ежегодно рассматривать ход выполнения Плана действий и принимать соответствующие решения, а также содействовать его успешному выполнению.

Основными направлениями реализации Стратегии являются национальные стратегии, программы и проекты информатизации, а также межнациональные программы и проекты, осуществляемые на двух- и многосторонней основе в составе Плана действий.

Ход выполнения Стратегии и Плана действий ежегодно рассматривается на заседаниях Координационного совета с принятием соответствующих решений.

Координационным советом в целях выполнения Стратегии и Плана действий подготовлены проекты документов по созданию и развитию сети информационно-маркетинговых центров (ИМЦ), телемедицины, паспортно-визовых документам нового поколения, информационной безопасности и другим приложениям ИКТ.

Важное значение государствами – участниками СНГ придается созданию Межгосударственной сети ИМЦ, отнесенной Концепцией дальнейшего развития Содружества Независимых Государств к приоритетным направлениям экономического сотрудничества.

Построение сети ИМЦ в 2002–2008 годах осуществлялось в соответствии с Межгосударственной программой создания сети ИМЦ для продвижения товаров и услуг на национальные рынки государств – участников СНГ (далее – Программа), утвержденной Решением Совета глав правительств СНГ от 29 ноября 2001 года. В реализации Программы принимали участие восемь государств – участников СНГ (кроме Республики Армения, Туркменистана и Республики Узбекистан).

Вопросы сотрудничества государств – участников СНГ по реализации Программы ежегодно рассматривались на заседаниях Экономического совета СНГ, Координационного совета, Рабочей группе высокого уровня Программы и Комиссии Регионального содружества в области связи по информатизации.

В настоящее время государства – участники СНГ находятся на различных этапах готовности по проведению мероприятий по созданию национальных ИМЦ и объединения их в межгосударственную сеть ИМЦ государств – участников СНГ в качестве товаропроводящей сети по организации торгов.

Учитывая, что срок реализации Программы истек в 2008 году, в целях продолжения работ по созданию сети ИМЦ в соответствии с поручением Экономического совета СНГ от 12 декабря 2008 года Координационный совет представил в Исполнительный комитет СНГ для рассмотрения в установленном порядке проект Соглашения о сотрудничестве государств – участников СНГ в создании, использовании и развитии межгосударственной сети информационно-маркетинговых центров для продвижения товаров и услуг на национальные рынки (Соглашение) и проект Положения о Рабочей группе высокого уровня по развитию межгосударственной сети информационно-маркетинговых центров и электронной торговли для продвижения товаров и услуг на национальные рынки государств – участников СНГ (Положение).

Проектом Соглашения предусматривается возложение функций по ее реализации на уполномоченные органы, представители которых будут определены заинтересованными государствами в Рабочую группу по развитию межгосударственной сети ИМЦ для продвижения товаров и услуг государств – участников СНГ на национальные рынки.

Одной из основных целей проекта документа является обеспечение наполнения межгосударственной сети ИМЦ информационными ресурсами о товарах и услугах, проводимых в государствах – участниках Соглашения.

Следует отметить, что в проекте Соглашения заложены основные принципы организации электронной торговли, предусмотренные в Модельном законе «Об электронной торговле», принятым Межпарламентской Ассамблеей государств – участников СНГ.

Соглашение и Положение рассмотрены и приняты главами правительств семи стран СНГ 21 мая 2010 года.

Учитывая важность введения систем ПВД НП в рамках Содружества, РГВУ были разработаны проекты Дополнений в Стратегию сотрудничества государств – участников СНГ в сфере информатизации и План действий по реализации Стратегии на период до 2010 года, которые утверждены Решением Совета глав правительств СНГ от 22 мая 2009 года в установленном порядке.

Дальнейшая работа по внедрению ИКТ в сферы деятельности государств – участников СНГ для построения информационного общества должна осуществляться с учетом происходящих изменений в их дальнейшем развитии. В связи с этим представляется целесообразным внести изменения и дополнения в Стратегию сотрудничества государств – участников СНГ в сфере информатизации и принять План действий по ее реализации на период до 2015 года.

Обновление Стратегии и принятие Плана действий по ее реализации на период до 2015 года станут важными факторами формирования общего информационного пространства на базе ИКТ, что окажет положительное воздействие на модернизацию экономики государств – участников СНГ, развитие конкуренции и рост товарооборота между ними.

Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года (далее – Стратегия) представляет собой совокупность согласованных взглядов государств – участников Содружества Независимых Государств (далее – СНГ, Содружество), отражающих их общее видение путей формирования информационного общества.

Настоящая Стратегия подготовлена с учетом Концепции дальнейшего развития Содружества Независимых Государств и Плана основных мероприятий по ее реализации (решение Совета глав государств СНГ от 5 октября 2007 года), Стратегии экономического развития Содружества Независимых Государств на период до 2020 года (решение Совета глав правительств СНГ от 14 ноября 2008 года), Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности (решение Совета глав государств СНГ от 10 октября 2008 года), Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года.

В настоящей Стратегии учтены основные положения Декларации принципов построения информационного общества (Женева, Швейцария, 2003 год), Плана действий Тунисского обязательства (Тунис, Тунисская Республика, 2005 год), а также отражены подходы и перспективы развития ИКТ, содержащиеся в Заявлении ВВУИО+10 о выполнении решений, принятых в 2003-2005 годах и в разработанной ВВУИО+10 Концепции ВВУИО на период после 2015 года (Женева, Швейцария, 10-12 июня 2014 года).

В Стратегии закрепляются цель, задачи, принципы и основные направления сотрудничества государств – участников СНГ в области использования информационно-коммуникационных технологий для продвижения по пути построения и развития информационного общества.

Реализация Стратегии обеспечит новое направление технологического развития – практическое воплощение концепции «интернета вещей».

Государства – участники СНГ должны выйти на новый уровень сотрудничества и широкой кооперации в области использования ИКТ, получит дальнейшее развитие общий рынок продукции и услуг в сфере ИКТ.

Совместными усилиями государств Содружества будет сформировано трансграничное пространство доверия на основе сети Интернет. Население государств-участников СНГ получит возможность пользоваться межгосударственными услугами в электронном виде.

На базе современной цифровой мультимедийной платформы будет развиваться специализированный круглосуточный информационный канал.

Существенно улучшатся показатели государств – участников СНГ в международных рейтингах в области развития информационного общества, а также по уровню доступности

национальной информационно-коммуникационной инфраструктуры для субъектов информационной сферы. В основном будет решена проблема «цифрового разрыва» между регионами на национальном уровне и между государствами – участниками СНГ.

Региональное содружество в области связи стран СНГ является открытой международной региональной организацией в области связи, в состав которой наряду с полноправными членами – администрациями связи стран СНГ – входят наблюдатели: администрации связи Болгарии, Латвии, Литвы, Словении, операторы связи Эстонской Республики, Финляндии и международная организация МОКС «Интерспутник».

РСС имеет статус наблюдателя в Международном союзе электросвязи и Всемирном почтовом союзе (ВПС).

Необходимость расширения взаимодействия в вопросах обеспечения информационной безопасности и выработки общих подходов к их решению поставила перед координационным советом вопрос об образовании соответствующей структуры – комиссии по информационной безопасности (комиссия).

Основные направления деятельности комиссии:

- проведение анализа существующих и потенциальных угроз;
- решение вопросов защиты государственных информационных систем от несанкционированного доступа и обеспечение их безопасного взаимодействия на национальном и межгосударственном уровне;
- сближение нормативной правовой базы стран Содружества в области ИБ;
- проработка вопросов обеспечения защиты баз данных и персональных данных, борьбы с киберпреступлениями и др.

Принимая во внимание тот факт, что киберпространство не имеет пределов и границ, а киберугрозы могут возникнуть в любой стране и за считанные минуты способны нанести огромный ущерб, чрезвычайно актуальны предложения членов комиссии о создании центра по обеспечению безопасности в киберпространстве. Данная структура должна стать единым центром для пользователей национальных информационных систем и сегмента сети Интернет, обеспечивающим сбор и анализ информации по компьютерным инцидентам, консультативную и техническую поддержку пользователям в предотвращении угроз компьютерной безопасности в рамках пространства СНГ.

По предложению членов комиссии, АС Молдовы, был подготовлен доклад на Всемирную конференцию по развитию электросвязи Международного союза электросвязи 2010 г. (ВКРЭ-10) «О создании совместного центра по обеспечению безопасности в киберпространстве стран СНГ».

Создание центра является продолжением деятельности комиссии, направленной на развитие сотрудничества с международными организациями, Международным союзом электросвязи в рамках реализации решений всемирной Встречи на высшем уровне по вопросам информационного общества (ВВУИО) в части «Укрепление доверия и безопасности при использовании ИКТ».

Помимо комиссии по информационной безопасности, в рамках РСС существуют рабочая группа по информационной безопасности взаимодействующих сетей связи при Совете операторов электросвязи РСС (РГ) и группа действий по почтовой безопасности при Совете операторов почтовой связи РСС.

В частности, РГ внесла значительный вклад в дело выработки единых подходов операторов электросвязи к обеспечению информационной безопасности сетей связи участников РСС. Одним из значимых наработок группы явилось подписание Меморандума о взаимодействии операторов электросвязи – участников РСС в сфере обеспечения информационной безопасности информационных и телекоммуникационных сетей и систем, а также использование «Требований к обеспечению базового уровня информационной безопасности информационных и телекоммуникационных сетей и систем» в качестве рекомендательного документа РСС.

Относительно правового поля в области ИКТ важное значение по формированию и осуществлению согласованной законодательной деятельности, укреплению интеграционного взаимодействия на основе сближения национальных законодательств стран Содружества в области связи и информатизации имеет подписанное в декабре 2002 года «Соглашение о взаимодействии между Региональным содружеством в области связи и Советом Межпарламентской Ассамблеи государств – участников СНГ». С этой целью в 2003 году был создан и действует Экспертный совет МПА СНГ – РСС. За период деятельности Экспертного совета по предложениям участников РСС разработаны и приняты более 19 модельных законов. Разрабатываемые МПА СНГ модельные законы становятся реальной базой, которую парламенты стран СНГ могут использовать в своих странах при изменении и совершенствовании национального законодательства. Так по предложениям и при экспертной поддержке участников МПА СНГ – РСС был подготовлен и 16 мая 2011 года принят модельный закон «Об основах регулирования Интернета» (в России в июле 2012 году был принят закон о защите детей в сети Интернет).

Основными задачами РСС в области развития людских ресурсов в 2014 году были:

- осуществление тесного сотрудничества в образовательной сфере, Координация взаимодействия АС РСС, высших учебных заведений СНГ при участии и реализации совместных с другими международными и региональными организациями проектов по созданию инновационной модели университетского образования в странах СНГ;
- расширение обмена опытом и организация более тесного взаимодействия в области развития людских ресурсов, подготовки и повышения квалификации кадров в области связи и информационных технологий, а также мероприятий, направленных на создание взаимоувязанного образовательного пространства стран СНГ.

РСС подготовлены Предложения по созданию центров мониторинга с целью укрепления доверия и безопасности при использовании ИКТ.

С целью обеспечения доверенного трансграничного обмена электронными данными РСС с 2011 года проводит комплексную и систематическую работу по формированию трансграничного пространства доверия с привлечением лучших мировых экспертов.

Примеры деятельности:

- создана Рабочая группа по внедрению протокола IPv6 в странах участников РСС при Совете операторов электросвязи и инфокоммуникаций и Комиссии РСС по инфокоммуникациям;
- активизирована деятельность Рабочей группы по управления сетями связи при Комиссии РСС по инфокоммуникациям.
- Каждый год подготавлевают и проводят боьшое колличество заседаний на которых обсуждаются вопросы связанные с информатизацией, электросвязью, инфокоммуникациями, радиосвязью и др.

Рабочей группой по информационной безопасности взаимодействующих сетей связи при СО ЭСИ РСС за 2014 год были подготовлены:

- проект Меморандума о взаимодействии операторов электросвязи стран участников РСС в сфере обеспечения информационной безопасности;
- проект Меморандума о взаимодействии операторов электросвязи стран участников РСС в сфере противодействия мошенничеству на сетях электросвязи;
- Положение о Рабочей группе по информационной безопасности взаимодействующих сетей связи при СО ЭСИ РСС.

Также Исполком РСС провел подготовительную работу по активизации деятельности Рабочей группы по управлению сетями связи при Комиссии РСС по инфокоммуникациям.

В рамках научно-исследовательской работы (НИР) по теме «Проведение регионального мониторинга инфокоммуникационного развития» (РМИКР) был разработан новый Перечень статистических показателей (утвержден Решением Совета глав АС РСС от 15-16 июля 2014г. № 49/20-15) для Статистического сборника. По предложению Исполкома РСС в 2014 году в новом формате вышел в свет Статистический сборник о деятельности АС РСС в области связи и информатизации за 2013 год.

Инициируя данную работу, Исполком РСС руководствовался, прежде всего, задачами по совершенствованию показателей, характеризующих инфокоммуникационное развитие и движение стран участников РСС к информационному обществу:

- единство информационно-статистической и методической основы формирования отчетности;
- унификация показателей для проведения анализа развития электросвязи, почтовой связи и инфокоммуникационного развития в региональном и международном аспектах;
- приведение существующих показателей в соответствие с достигнутым уровнем научно-технического прогресса, процессов цифровизации сетей связи, внедрения ИКТ.

Новый Статистический сборник включает 197 унифицированных показателей. Основные отличия нового Статистического сборника состоят в следующем:

- скорректированы названия большинства показателей Статсборника РСС в соответствии с методикой МСЭ по системе показателей всемирной электросвязи/ИКТ;

- в систему показателей Статистического сборника РСС включены дополнительные показатели, соответствующие компонентам подындексов Индекса развития ИКТ (IDI) в целях обеспечения международного сопоставления с результатами МСЭ;
- достигнута увязка регионального мониторинга ИКР с международным мониторингом развития ИКТ МСЭ и имеется возможность проверки всех относительных показателей на основе абсолютных данных;
- заменен ряд показателей ИКР и их компонентов в рамках РМИКР в соответствии с эволюцией формирования информационного общества;
- значительно сокращен объем анализируемых показателей за счет уменьшения числа показателей по почтовой связи, по наличию технических средств связи, качеству работы и услуг связи;
- исключено Справочное приложение «Показатели, характеризующие бизнес-климат, человеческий капитал, государственное регулирование в сфере ИКТ стран участников РСС», заполнение которого было сопряжено с трудностями существующего национального статистического учета по ряду показателей.

С целью определения экономической эффективности интеграционных процессов в странах участников РСС проводится Региональный мониторинг инфокоммуникационного развития (РМИКР).

Региональный мониторинг инфокоммуникационного развития стран участников РСС показал, что на региональном пространстве продолжается активная работа по развитию и совершенствованию инфокоммуникационной инфраструктуры, внедрению ИКТ во все сферы общественного производства, социума и государственного управления.

За анализируемый период страны участники РСС достигли значительного прогресса: по всем мониторинговым показателям ИКР наблюдалась положительная динамика с разными уровнями прироста.

Особенно высокими темпами повышались: пропускная способность сети Интернет – на 20,2%; плотность абонентов широкополосного доступа – на 19,3 %; плотность пользователей Интернет и компьютеров – соответственно на 13,5% и 10,3%; уровень многоканального (цифрового) телевидения - на 11%; охват сетями подвижной связи новых поколений – 13,5%, доля ВВП, создаваемого с применением ИКТ – на 6,3%, доля хозяйствующих субъектов, применяющих ИКТ в экономической деятельности – на 3,2%; душевые доходы от услуг инфокоммуникационного сектора – на 3%; охват сферы управления ИКТ – на 3%.

Государства – участники СНГ проводят работу по совершенствованию системы статистических показателей развития информационного общества и методов их формирования

Приложение 9. Создание центров мониторинга

В МСЭ-Т принята международная рекомендация (проект которой активно продвигала Российская Федерация) X. NCNS-1 – Supplement on guidance for creating national IP-based public network security center for developing countries («Руководство по созданию Национальных центров безопасности сети связи общего пользования, базирующейся на протоколе IP, для развивающихся стран»). Рекомендация ориентирована на содействие обеспечению безопасного и устойчивого функционирования национальной ИКТ-инфраструктуры, включающей сети операторов подвижной и фиксированной связи и национальный сегмент сети интернет. Ее концептуальный принцип – сотрудничество ради безопасности.

Рекомендация описывает структуру Национального центра и схему его внешних связей. Составляющие Рекомендации – организация функционирования межоператорской группы анализа инцидентов (МЕГА), интеграция функциональных компонентов и компонентов обеспечения безопасности, формирование координирующих воздействий для обеспечения непрерывности оказания услуг в рамках национальной ИКТ-инфраструктуры гражданам, бизнесу и органам государственной власти как в повседневном режиме работы, так и в условиях чрезвычайных ситуаций природного и техногенного характера.

В Рекомендации также описываются модели работы национальных центров, которые можно использовать для обеспечения защищенности, стабильности и восстанавливаемости национальной ИКТ-инфраструктуры развивающихся стран, работающей на основе протокола IP. Эти модели могут быть федеративными или виртуальными и имплементироваться по отдельности или комбинированно. В рамках одного государства могут функционировать несколько подобных равнозначных центров.

Последовательное применение принципа «Сотрудничество ради безопасности» приводит к формированию распределенной, федеративной интеграционной среды (ФИС), или так называемого федеративного пространства доверия, где размещаются сервисы, доступные всем участникам системы коллективной безопасности на национальном уровне.

Наличие такой федеративной интеграционной среды обеспечивает операторам возможность присоединения к ней, размещения своих сервисов и получения доступа ко всем сервисам безопасности, развернутым в ФИС другими операторами и администрацией NCNS. Федеративная интеграционная среда организуется в виде стека управляющих плоскостей (control planes): Security control plane, Information Exchange Plane, Service Exchange Plane.

NCNS проектируется и формируется как система организационно-технического управления национальной ИКТ-инфраструктурой в процессе межоператорского взаимодействия и включает и уже существующие центры управления сетями связи (NOC/SOC), и вновь создаваемые центры управления безопасностью операторов связи. NCNS обеспечивает координацию как в повседневной деятельности, так и во время чрезвычайных ситуаций.

Формирование NCNS предполагает создание специального пула операторов связи, отобранных и сертифицированных в соответствии с национальными требованиями и/или международными X.Sup2: ITU-T X.800-X.849 series – Supplement on security baseline for

network operators. Применение открытых и формализованных процедур, и условий отбора операторов связи способствует расширению круга участников взаимодействия.

В основе создания NCNS лежат архитектура и методика организации и сопровождения системы поддержки операционной деятельности во взаимодействии с центрами управления сетями связи NOC/SOC, составляющими национальную ИКТ-инфраструктуру. Такой подход предполагает, что NCNS создается как распределенная система межоператорского взаимодействия.

В состав NCNS входят администрация центра, подразделение мониторинга и управления информационной безопасностью, подразделение анализа и развития. К функциям подразделения мониторинга и управления ИБ относят:

- создание и ведение базы данных по инцидентам безопасности на сетях связи, поддержка ее в актуальном состоянии;
- информационная поддержка протокольного обмена событиями безопасности и положительными практиками противодействия с другими центрами сетевой безопасности и с центрами безопасности взаимодействующих операторов;
- контроль (с применением технических и программных средств) состояния информационной безопасности сетей и систем существенных операторов;
- взаимодействие с оперативными подразделениями операторов при локализации и устранении аварий на сетях связи, вызванных деструктивными воздействиями на сеть и ресурсы систем управления сетью связи;
- организация взаимодействия с центрами безопасности взаимодействующих операторов при отражении массовых атак на системы управления сетями связи;
- организация взаимодействия с центрами компетенций и службами поддержки компаний – производителей телекоммуникационного и сетевого оборудования.

В функции подразделения анализа и развития входит:

- разработка нормативно-методической базы безопасности национальной ИКТ-инфраструктуры;
- анализ угроз безопасности и формирование мер и рекомендаций по противодействию им;
- формирование базы лучших практик и рекомендаций по обеспечению безопасности и реагированию на инциденты безопасности;
- разработка технических решений и сопровождение проектов и работ по информационной безопасности на сетях связи и информационных ресурсах;
- сертификация присоединяемых операторов.

Объектами информационного взаимодействия NCNS являются центры управления безопасностью операторов связи, другие NCNS, организации федеральных регуляторов в области безопасности и связи, центры реагирования на инциденты безопасности (CERT, CSIRT, CIRT) и другие структуры, заинтересованные в повышении устойчивости сетей связи (вендоры, общественные организации и т.д.).

В целях информационного обмена NCNS с внешними объектами может быть использован весь спектр механизмов обмена информацией о событиях. В случае центров управления безопасностью операторов связи это протоколы взаимодействия, поддерживаемые операторскими системами управления и автоматизированными системами управления инцидентами. Для других NCNS предназначен новый протокол обмена, отвечающий требованиям взаимодействия NCNS. Обмен с организациями регуляторов в области безопасности и связи происходит в соответствии с национальным законодательством и особенностями технического оснащения регуляторов. Для взаимодействия с центрами реагирования на инциденты безопасности (CERT, CSIRT, CIRT и т.д.) используются механизмы обмена информацией, указанные в Рекомендации X.1500 (CYBEX). В случае вендоров, общественных и других организаций, заинтересованных в повышении устойчивости сетей связи, протоколы обмена целесообразно определять по договоренности с ними.

NCNS ведет собственную электронную базу данных об угрозах и методах защиты (с учетом национальных нормативных актов в части защиты конфиденциальной информации). Для автоматизации деятельности NCNS используется совокупность технических и программных средств.

Межоператорская группа анализа инцидентов (МЕГА) представляет собой архитектурную составлящую NCNS, выделенную для сбора, обработки и обмена информацией об инцидентах и событиях безопасности между операторами связи, потребителями услуг связи, производителями оборудования, государственными органами, а также для ведения базы данных «лучших практик» по выделенным инцидентам ИБ.

Цель создания МЕГА – консолидация усилий по выявлению угроз информационной безопасности (кибербезопасности) национальной ИКТ-инфраструктуры, обнаружению и локализации инцидентов, относящихся к сфере информационной безопасности, принятию мер по устранению негативных последствий инцидентов и их недопущению в дальнейшем.

МЕГА формирует и рассылает присоединенным к NCNS операторам связи рекомендации по обеспечению базового уровня информационной безопасности (ITU-T X.800-X.849 series – Supplement on security baseline for network operators); проводит экспертизу и мониторинг инфокоммуникационных систем (по запросу) операторов связи на наличие уязвимостей и выдает рекомендации по их устранению и повышению уровня устойчивости предоставления услуг; оказывает поддержку пользователям – операторам связи в повышении устойчивости и информационной безопасности (консультирует их по вопросам борьбы с вредоносными программами, безопасных настроек, по случаям недоступности узлов и сегментов сети связи, нарушения авторских прав при работе в интернете и т. д.); принимает круглосуточно обращения операторов связи по поводу событий и инцидентов безопасности, в том числе жалобы на действия пользователей и операторов связи, а также на инциденты с использованием средств связи оператора (пример: фрод на сетях связи); ведет анализ (расследование) зафиксированных инцидентов и событий безопасности во взаимодействии с операторами связи, производителями оборудования, государственными органами и предоставляет оперативную информацию об угрозах, инцидентах и событиях безопасности для ликвидации их вредных последствий; организует взаимодействие между операторами связи и сервис-провайдерами при эксплуатации программно-технических средств поддержки информации об актуальности присоединенных

сетей; способствует повышению устойчивости, а также информационной безопасности средств коллективного пользования; выдает рекомендации производителям оборудования в том, что касается требований к повышению устойчивости сетей связи и кибербезопасности средств связи; проводит информационно-аналитическую работу по сбору данных о произошедших атаках, актуальных методах атак, ресурсах злоумышленников, сигнатурах атак и т.д.

Список инцидентов, на которые реагирует МЕГА, включает (но не ограничивается ими) DDoS-атаки, несанкционированный доступ к сетевым ресурсам, наличие известной критичной уязвимости на имеющем существенное значение ресурсе, эпидемии компьютерных вирусов, функционирование в сети связи вредоносных программ, нарушение функций маршрутизации, приводящих к недоступности подсетей, сегментов, автономных систем, ошибочное или злонамеренное переконфигурирование сетевого оборудования, приводящее к нарушению связности телекоммуникационных сетей, фишинг, рассылку различных видов спама, несанкционированный пропуск трафика («серый» трафик).

Принятие Рекомендации МСЭ-Т по созданию Национальных центров безопасности – важный этап формирования содружества государств в интересах обеспечения информационной безопасности на сетях связи. Теперь эффективность этого процесса зависит от дальнейшей разработки более конкретных подстандартов на базе данного «зонтичного» стандарта, а также конкретных пошаговых руководств по их развертыванию.

CERT (англ. computer emergency response team) – международная система координационных центров в сфере безопасного использования информационно-коммуникационных технологий.

CERT существует на государственном уровне в 27 странах мира: Аргентине, Австралии, Канаде, Испании, Польше, Финляндии, Италии, Венгрии, Индии, Тунисе, Бразилии, Чили, Китае, Дании, Нидерландах, Израиле, Японии, Южной Корее, Норвегии, Катаре, Словении, Швеции, Шри-Ланке, Сингапуре, Тайване и Тайланде.

Основные задачи таких Служб - своевременное выявление фактов атак на объекты информационной инфраструктуры (компьютерные системы и информационные ресурсы); обеспечение взаимодействия между экспертами, работающими в области обеспечения информационной безопасности; выявление уязвимых мест в компьютерных системах; международное сотрудничество в этой сфере.

В Республике Казахстан техническим решением по линии взаимодействия государства и общества стало создание Службы реагирования на компьютерные инциденты (KZ-CERT) при Министерстве связи и информации Республики Казахстан.

Одним из направлений работы KZ-CERT является профилактика правонарушений, связанных с киберпреступностью, в т.ч. противодействие ботнетам, проверка Интернет-ресурсов на наличие уязвимостей и вредоносного кода, отслеживание хакерской активности и т.д. Функционирование KZ-CERT позволит создать условия для осуществления профилактики, выявления и, при необходимости, нейтрализации атак на критические узлы и ресурсы национальной ИТ-инфраструктуры, имеющих целью нарушение их конфиденциальности, целостности и доступности.

Сервисы, предусмотренные в KZ-CERT:

- Оповещение. Объявления о новых угрозах в Интернете (вирусах, атаках и других угрозах), сообщения об уязвимостях в аппаратном или программном обеспечении на сайте и по электронной почте. Предоставление рекомендаций по устранению угроз, минимизации негативного воздействия инцидентов.
- Обработка инцидента. Прием заявок об инцидентах кибербезопасности, их обработка, классификация. Оказание помощи в сборе необходимых сведений об инциденте. Предоставление рекомендаций по защите систем и сетей, подвергшихся атаке, по восстановлению подвергшихся атаке систем. Обработка инцидента совместно с операторами связи и правоохранительными органами.
- Анализ инцидента. Включает изучение всех доступных данных, вещественных доказательств и следов взломщика. Целью анализа является определение масштаба повреждений, причины инцидента и возможные ответные действия.
- Консультации по информационной безопасности. KZ-CERT осуществляет взаимодействие с правоохранительными органами, собственниками Интернет-ресурсов, государственными органами (ГО), операторами связи и хостинг-провайдерами, а также с международными профильными организациями по вопросам ИБ и совместной обработке инцидентов ИБ. В этом году заключено соглашение о сотрудничестве KZ-CERT с правоохранительными органами РК по реагированию на компьютерные инциденты. В рамках обеспечения профилактики правонарушений в сфере высоких технологий KZ-CERT активно взаимодействует с МВД РК. В июле 2011г. подписаны Регламенты взаимодействия МСИ РК с МВД РК, КНБ РК по вопросам реагирования на компьютерные инциденты.

В рамках мероприятий по взаимодействию с ГО МСИ Республики Казахстан проводятся семинары по вопросам выявления угроз безопасного использованию ИКТ.

В настоящее время собственники интернет-ресурсов, подвергшиеся атакам и другим угрозам в Интернете, могут отправлять заявки об инцидентах на email: info@kz-cert.kz или обращаться в KZ-CERT по телефону: +77172793192.

С целью повышения мер доверия в сфере информационно-коммуникационных технологий подписана Декларация Операторов связи и Хостинг-провайдеров Республики Казахстан о безопасном Интернете. Данная декларация устанавливает основные принципы для эффективного исполнения законодательства Республики Казахстан, регулирующего отношения в сфере использования улучшения координации действий операторов связи и хостинг-провайдеров, а также иных участников отношений, связанных с сетью Интернет, в том числе, государственных органов и общественных организаций, патронирующих сферы безопасного использования ИКТ и противодействия противоправного контента.

Для контроля за состоянием технологических процессов, связанных с информационной безопасностью, в МСИ Республики Казахстан организована деятельность Центра мониторинга информационной безопасности «электронного правительства» РГП «ЦТСАТ» МСИ Республики Казахстан, основными задачами которого являются выявление уязвимостей серверов «электронного правительства», регистрация и анализ событий и угроз информационной безопасности в компонентах «электронного правительства». Мониторинг информационной безопасности проводится на периодической основе с формированием соответствующих отчетов, а также с выработкой соответствующих рекомендаций по предупреждению и устранению возможных «дыр» в системах защиты информационных

систем. Выполнение этих рекомендаций поднимает уровень защищенности информационных систем инфраструктуры электронного правительства путем упреждающего устранения уязвимостей, которые могут быть эксплуатированы злоумышленниками.

В 2012 году между Казахстанской (KZ-CERT) и Румынской (CERT-RO) Службами реагирования на компьютерные инциденты был подписан Протокол сотрудничества. Планируется сотрудничество со Службами CERT других стран с целью обмена опытом и информацией об инцидентах. Сотрудничество по указанным направлениям будет способствовать обеспечению кибербезопасности, в том числе и по противодействию осуществления компьютерных атак в террористических и экстремистских целях через сеть Интернет. Подписаны Меморандумы о взаимопонимании и сотрудничестве в сфере информационной безопасности с Индийской (CERT-In), Российской (RU-CERT), Узбекской (UZ-CERT), Армянской (CERT.AM), Латвийской (CERT.LV), Литовской (CERT-lt), Азербайджанской (CERT.GOV.AZ), Австралийской (CERT AUSTRALIA) службами реагирования на компьютерные инциденты, Российской Группой информационной безопасности (GROUP-IB), Оперативно-аналитическим центром при Президенте Республики Беларусь и Исследовательской фирмой, специализирующаяся на Интернет-безопасности "Team Cymru Community Services" (США), Национальной Китайской технической Службой реагирования на компьютерные инциденты (CNCERT/CC), Корейским агентством «Интернет и безопасность» (KISA), Международной группой - ЗАО Лаборатория Касперского (Россия), СайберСекьюрити Малайзия (CyberSecurity Malaysia).

Республика Узбекистан является членом «Компьютерной группы реагирования на чрезвычайные ситуации» (CERT) - группы экспертов по компьютерной безопасности, занимающихся сбором информации об инцидентах, их классификацией и нейтрализацией и носит название UZ-CERT.

В настоящее время в Российской Федерации создается GOV-CERT.RU – центр реагирования на компьютерные инциденты в информационно-телекоммуникационных сетях (ИТС) органов государственной власти РФ, призванный решать следующие задачи: оказание консультативной и методической помощи при проведении мероприятий по ликвидации последствий компьютерных инцидентов в ИТС органов государственной власти; анализ причин и условий возникновения инцидентов в ИТС органов государственной власти; выработка рекомендаций по способам нейтрализации актуальных угроз безопасности информации; взаимодействие с российскими, иностранными и международными организациями, отвечающими за реагирование на компьютерные инциденты; накопление и анализ сведений о таких инцидентах.

Кроме того, в России уже действуют три аналогичных центра – CERT-GIB, WebPlus ISP и RU-CERT. Первый из тройки был создан совсем недавно, его основатель – компания Group-IB. Это частный центр реагирования, обслуживающий сторонние организации, но претендующий на звание «прогосударственного», так как именно с ним Координационный центр национального домена сети Интернет заключил соглашение о противодействии киберугрозам в доменах .RU и .РФ (наряду с подразделением Лиги безопасного Интернета – фондом «Дружественный Рунет»). Центр работает в режиме 24x7 и оказывает услуги (на основе абонентского договора или договора оферты) реагирования на следующие типы инцидентов: отказ в обслуживании (DoS, DDoS), компрометация информации, компрометация актива, внутренний или внешний несанкционированный доступ, создание и

распространение вредоносного программного обеспечения, нарушение политик информационной безопасности, фишинг и незаконное использование бренда в интернете, мошеннические действия с системами ДБО и электронными платежными системами.

Центр Webplus ISP CERT занимается обслуживанием только собственных ресурсов.

Четвертый центр, RU-CERT (Russian Computer Emer-gency Response Team) – это автономная некоммерческая организация «Центр реагирования на компьютерные инциденты», официально зарегистрированная как Computer Security Incident Response Team (CSIRT). RU-CERT занимается сбором и анализом информации по фактам компьютерных инцидентов (попыток или фактов нарушений российского законодательства, или принятых международных нормативных правовых актов при обработке информации в открытых телекоммуникационных сетях, которые имеют отношение к сетевым ресурсам, расположенным на территории Российской Федерации), а также реагированием на них с целью выявления, предупреждения и пресечения подобной деятельности на территории РФ. RU-CERT на территории России также выступает в качестве контактной стороны для всех пользователей, которым необходимо содействие в обращении к российским интернет-провайдерам и официальным государственным структурам, проводящим предусмотренное российским законодательством расследование компьютерных преступлений. При этом RU-CERT не обладает правами на прекращение деятельности лиц, причастных к компьютерным инцидентам, закрытие ресурсов, блокирование адресов и т.п.

Кроме того, в настоящее время создается межотраслевой CSIRT на базе Ассоциации руководителей служб информационной безопасности.

Как отмечалось выше, на сегодняшний день в Российской Федерации уже функционирует несколько центров реагирования на инциденты информационной безопасности.

Например, при Координационном центре национального домена сети Интернет работает центр реагирования на компьютерные инциденты. Есть центр при ФСБ РФ, но он позиционируется как структура, обслуживающая интересы государства и государственно-значимых структур.

К сожалению, на практике их услугами сейчас пользуется минимальное число компаний. Это обусловлено отсутствием понятной схемы взаимодействия и некоторыми другими факторами.

Следует отметить, что у многих компаний созданы свои операционные центры безопасности (Security operation center - SOC). Задачей функционирования такого центра является обнаружение попыток несанкционированного доступа к ИТ-инфраструктуре оператора связи, предотвращение попыток вторжения внутрь защищаемого периметра и управление инцидентами ИБ.

Однако было бы намного эффективнее, если бы все такие центры\операторы имели бы общий добровольный инструмент для взаимодействия (обмена информацией). Единую «базу знаний».

В настоящее время обсуждается вопрос о возможности создания межоператорского центра сбора и обмена информацией об инцидентах информационной безопасности

(МЦСОИБ - TEL CERT) который станет «центром знаний» в вопросах информационной\кибербезопасности для всех операторов связи Российской Федерации

В мировой практике сложился термин CSIRT - Группа Реагирования на Инциденты Компьютерной Безопасности. Существуют различные аббревиатуры, обозначающие данные группы:

- CERT или CERT/CC (Группа Оперативного Реагирования на Компьютерные Инциденты / Координационная Группа),
- CSIRT (Группа Реагирования на Инциденты Компьютерной Безопасности),
- IRT (Группа Реагирования на Инциденты),
- CIRT (Группа Реагирования на Компьютерные Инциденты),
- SERT (Группа Оперативного Реагирования на Инциденты Безопасности).

Создаваемый межоператорский центр сбора и обмена информацией об инцидентах информационной безопасности (МЦСОИБ - TEL CERT) должен быть «центром знаний и решений» в вопросах информационной\кибербезопасности для операторов связи Российской Федерации.

Предполагается, что организационно МЦ СОИБ будет включать в себя: центр компетенций, центр анализа и сбора, базу «знаний». МЦСОИБ должен обеспечивать:

- централизованную координацию вопросов информационной\кибер безопасности в рамках всей отрасли Связь,
- централизованную и специализированную систему обработки сообщений об инцидентах и реакции на них,
- возможность экспертизы и поддержки в процессе быстрого восстановления после возникновения инцидентов безопасности,
- возможность взаимодействия в правовых вопросах, сохранение доказательств в случае судебных процессов,
- разработка стандартов и рекомендаций для операторов связи;
- формирование набора метрик и показателей информационной\кибер безопасности;
- проведение тестирования телекоммуникационной инфраструктуры на устойчивость к кибератакам, а также средств защиты с возможностью присвоения класса кибербезопасности,
- подтверждать соответствие систем управления информационной безопасностью оператора связи требованиям основного уровня информационной безопасности для операторов связи в системе сертификации «Связь-Эффективность»,
- стимулирование взаимодействия клиентов (операторов) по вопросам информационной безопасности (повышение осведомлённости).

В отличие от других подобных центров МЦСОИБ не будет устанавливать никакие системы контроля на сетях операторов связи, а будет взаимодействовать на основе

добровольности, взаимовыгодного сотрудничества и совместного обеспечения устойчивости, целостности и безопасности сети связи общего пользования (ССОП) Российской Федерации.

При создании центра за основу предлагается взять модель центра на основе международной Рекомендации МСЭ-Т X.800-X.849 «Руководство по созданию национальных открытых центров сетевой безопасности на протоколе IP для развивающихся стран» (разработка Российской Федерации).

Предлагаемые этапы создания центра:

- Создание рабочей группы из представителей операторов связи;
- Разработка принципов взаимодействия (документ);
- Согласование финансовой модели центра в части работы с операторами связи;
- Разработка инвестиционной модели.

Понятно, что иметь единственную систему невозможно — центр должен взаимодействовать с множеством себе подобных, в том числе с международными организациями.

Если у компании нет своего центра, можно покупать данные услуги у такого центра. Предполагается, что центр будет включать в себя центр компетенций, центр анализа и сбора, базу знаний.

Для того чтобы найти источник заражения, проследить всю цепочку, необходимо наличие таких центров в каждой стране, входящей в РСС, и их действенное взаимодействие.

При Минестерстве по развитию информационных технологий и коммуникаций Республики Узбекистан существует Центр мониторинга в сфере массовых коммуникаций.

В обязанности центра мониторинга входит:

- системный мониторинг национального информационного пространства и деятельности средств массовой коммуникации, включая современные информационно-коммуникационные технологии, спутниковые системы, глобальную сеть Интернет, другие электронные средства доставки и распространения информации, а также печатную продукцию;
- анализ соответствия содержания распространяемых в средствах массовой коммуникации информационных материалов требованиям актов законодательства республики, направленных на обеспечение защиты интересов личности, общества и государства в информационной сфере, предупреждение деструктивного негативного информационно-психологического воздействия на общественное сознание граждан, сохранение и преемственность национально–культурных традиций;
- выявление проблем, препятствующих эффективному функционированию отечественных средств массовой информации и коммуникации, выработку предложений по созданию необходимых условий для всестороннего развития национального информационного рынка;
- обобщение и выдачу рекомендаций, предупреждений и заключений по результатам мониторинга деятельности субъектов, оказывающих услуги в сфере массовых коммуникаций, по выявленным нарушениям требований законодательства;

- совершенствование, по мере внедрения новых технологий, системы мониторинга в сфере массовых коммуникаций, формирования информационных ресурсов, систем и средств доставки и распространения информации;
- разработку предложений по совершенствованию законодательных актов, нормативно-правового обеспечения в информационной сфере, развитию материально-технической базы средств массовой коммуникации и подготовке квалифицированных кадров с учетом передового зарубежного опыта, современных требований и стандартов.

На Украина в настоящее время прорабатываются вопросы создания собственных центров мониторинга ИКТ. Введение таких центров позволит своевременно следовать мировым тенденциям развития инфокоммуникационных технологий для поддержания надлежащего уровня доверия и безопасности граждан при использовании ИКТ.

Центры мониторинга позволят не только контролировать динамику развития сфер электросвязи, почтовой связи, но и заниматься другими важными аспектами влияющими на использование ИКТ, такими как защита детей в онлайновой среде, поддержание высокого уровня технологического развития страны, выявление потребностей и быстрое введение новых технологий для лиц с ограниченными возможностями.

Центры мониторинга позволят контролировать состояние и перспективы развития инфокоммуникационных сетей (проводного и беспроводного широкополосного доступа, сетей подвижной радиотелефонной связи, спутниковых систем связи, систем телевизионного и радиовещания), производить мониторинг центров обработки данных и облачных вычислений, наблюдать за перспективами в инфокоммуникационных технологиях и услугах, экономических аспектах внедрения новых технологий и услуг.

---

[1] Профессиональный стандарт «Специалист по информационной безопасности информационно-коммуникационных систем»:

1. не применяется к отношениям, связанным с осуществлением деятельности по защите государственной тайны;
2. используется исключительно для нужд оценки квалификации специалистов, занимающихся вопросами информационной безопасности инфокоммуникационных систем в целях обеспечения собственных нужд юридического лица или индивидуального предпринимателя и работа которых (специалистов) не требует наличия допуска к государственной тайне оформленного надлежащим образом;
3. не используется для нужд оценки квалификации специалистов эксплуатирующих инфокоммуникационных системы, которые в соответствии с регламентами Федеральной службы по техническому и экспортному контролю (ФСТЭК России) являются «системами двойного назначения».

Кроме того, предполагается, что профессиональный стандарт «Специалист по информационной безопасности информационно-коммуникационных систем» не распространяется на лиц:

1. участвующих в разработке, производстве, распространении шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполняющих работы, оказывающих услуги в области шифрования информации, осуществляющих техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (крипто графических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств,

информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

2. осуществляющих разработку, производство, реализацию и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;
3. осуществляющих деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
4. осуществляющих разработку и производство средств защиты конфиденциальной информации;
5. осуществляющих деятельность по технической защите конфиденциальной информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя и не выходит за рамки Федерального закона от 27 июля 2006 г. №149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)).

В силу приведённых выше ограничений проект профессионального стандарта «Специалист по информационной безопасности информационно-коммуникационных систем» не содержит трудовых функций подлежащих обязательной сертификации и лицензированию (Федеральный закон Российской Федерации от 4 мая 2011 г. №99-ФЗ "О лицензировании отдельных видов деятельности") и в соответствии с действующим законодательством не подлежит обязательному согласованию.