Международный союз электросвязи

Руководство по кибербезопасности для развивающихся стран

Издание 2007 **г.**

Международный союз электросвязи

Международный союз электросвязи

Руководство по кибербезопасности для развивающихся стран

Издание 2007 года

Названия и классификации, используемые в данной публикации, не подразумевают какой бы то ни было оценки правового или иного статуса любой территории, а также подтверждения или одобрения какой бы то ни было границы со стороны Международного союза электросвязи. Слово "страна", используемое в данной публикации, охватывает страны и территории.

Отказ от ответственности
Ссылки на определенные страны, компании, продукцию, инициативы или руководства ни в коем случае не предполагают, что МСЭ одобряет или рекомендует упомянутые страны, компании, продукцию, инициативы и руководства как лучшие по сравнению с аналогичными компаниями, продукцией, инициативами и руководствами, которые не были упомянуты. Мнения, высказываемые в данной публикации, являются позицией автора и не касаются МСЭ.

ПРЕДИСЛОВИЕ

Международные организации, правительства стран, представители деловых кругов и гражданского общества собрались на Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО), проходившей в два этапа в Женеве и Тунисе, для того, чтобы сформировать общую концепцию информационного общества.

Однако претворить эту общую концепцию в жизнь во всем мире мы можем, только если обеспечим безопасность электронных транзакций, защитим инфраструктуры важной информации, информационные системы и данные, на которые полагаются бизнесмены, правительства и граждане.

Неоптимальные решения в области кибербезопасности, отсутствие взаимопонимания по определенным вопросам и необходимость решать данную проблему в глобальном масштабе – вот лишь несколько сложных задач, ответы на которые мы должны искать сообща.

Международный союз электросвязи (МСЭ) в качестве ведущей содействующей организации Направление деятельности С.5 – *Укрепление доверия и безопасности при использовании ИКТ* ВВУИО обязуется сотрудничать со всеми участниками, для того чтобы добиться общего понимания стоящих перед нами задач и объединить наши коллективные ресурсы для построения глобальной структуры безопасности и доверия.

Приглашаю Вас присоединиться к нам и работать на благо создания безопасного глобального информационного общества.

Д-р Хамадун И. Туре

Генеральный секретарь
Международного союза электросвязи (МСЭ)

ВВЕДЕНИЕ

Появление глобального и не имеющего границ информационного общества дает всем странам мира новые возможности, поскольку технологии играют все более важную роль в социальном и экономическом развитии. Благодаря применению информационно-коммуникационных технологий (ИКТ) возможно оказание услуг в области здравоохранения, образования, бизнеса, финансов и государственного управления.

Использование ИКТ ставит перед нами новые задачи, которые мы должны решать, если мы хотим безопасно вести дела в области электронного здравоохранения, предоставлять гражданам доступ к услугам электронного правительства, обеспечивать необходимый уровень надежности при ведении коммерческой и деловой электронной торговли и поддерживать целостность наших систем и ресурсов информационных технологий.

Поэтому одной из важнейших задач Бюро развития электросвязи МСЭ является претворение в жизнь оптимальных решений по безопасности и надежности, поскольку Бюро развития электросвязи прилагает усилия для помощи странам в использовании электросвязи, а также ИКТ.

Безграничный характер информационного общества также подразумевает, что все страны должны осознавать потенциал безопасного использования ИКТ и проблемы, с которыми мы сталкиваемся при обеспечении надежности и безопасности. Поэтому необходимо, чтобы кроме работы по ликвидации отставания в области технологий, мы прилагали усилия по преодолению отставания в знаниях путем повышения базовой осведомленности и создания человеческого и институционального потенциала.

Данное руководство предназначено для того, чтобы дать развивающимся странам инструмент, при помощи которого они смогут лучше понять некоторые вопросы, касающиеся безопасности информационных технологий, а также, чтобы предоставить им примеры решений, которые реализовали другие страны в отношении данных проблем. Также в данном руководстве содержатся ссылки на другие публикации, где дается дальнейшая, специальная информация по кибербезопасности. Данное руководство не является исчерпывающим документом или отчетом по данному вопросу, а скорее обзором принципиальных проблем, которые решают в странах, желающих воспользоваться преимуществами информационного общества.

Данное руководство составлено таким образом, чтобы удовлетворить потребности развивающихся и, особенно, наименее развитых стран в плане использования информационно-коммуникационных технологий для предоставления услуг в различных областях, развивая при этом местный потенциал и повышая осведомленность среди всех заинтересованных сторон.

Для того чтобы избежать любого дублирования при описании решения данных вопросов, при разработке содержания данной публикации была принята во внимание работа, завершенная в рамках 17-й Исследовательской комиссии МСЭ-Т, а также другие исследования и публикации в данной области.

Сами Аль Башир Аль Моршид

Директор
Бюро развития электросвязи

РЕЗЮМЕ

Социальные вопросы, экономика, государственная политика, гуманитарные проблемы: как на это ни посмотри, как ни назови (IT безопасность, безопасность электросвязи), кибербезопасность затрагивает безопасность цифрового и культурного благосостояния людей, организаций и стран. Возникающие проблемы сложны, и решение их требует политической воли для разработки и реализации стратегии по развитию цифровых инфраструктур и услуг, что включает в себя четкую, эффективную, поддающуюся контролю и управлению стратегию в области кибербезопасности.

Достижение уровня информационной безопасности, достаточного для того чтобы компенсировать технологический и информационный риск, необходимо для правильного функционирования правительств и организаций. Широкое использование цифровых технологий сопровождается увеличением зависимости от этих технологий и взаимной зависимостью важных инфраструктур. Таким образом, функционирование учреждений становится уязвимым, что нельзя игнорировать, учреждения подвергаются потенциальной опасности, что даже может подорвать суверенитет государства.

Целью кибербезопасности является помощь в защите имущества и ресурсов организаций в организационном, человеческом, финансовом, техническом и информационном планах, что позволит им выполнять свою задачу. Конечной целью является гарантирование того, что им не будет нанесено никакого длительного вреда. Это включает в себя снижение вероятности реализации угрозы; ограничение ущерба или неисправной работы и обеспечение того, что после инцидента, связанного с нарушением безопасности, можно будет восстановить нормальную работу за приемлемое время и с приемлемыми затратами.

Процесс кибербезопасности охватывает все общество, в котором реализация кибербезопасности касается каждого человека. Кибербезопасность можно сделать более важной путем разработки кодекса компьютерного поведения для обеспечения соответствующего использования ИКТ и пропаганды подлинной политики безопасности, устанавливающей стандарты, соответствие которым, как ожидается, будут обеспечивать пользователи кибербезопасности (объекты, партнеры и поставщики).

Для формирования процесса кибербезопасности важно правильно определить, какое имущество и ресурсы необходимо защищать, так чтобы точно определить область применения безопасности, необходимую для эффективной защиты. Это требует глобального многодисциплинарного и всеобъемлющего подхода к безопасности. Кибербезопасность не совместима с миром, в котором на первое место ставится вседозволенность. Все, что требуется – это набор основных принципов этичного поведения, ответственности и прозрачности, облеченные в правовую форму и прагматический текст процедур и правил. Конечно, данные правила должны приводиться в исполнение на местном уровне; однако их также нужно применять по всему международному сообществу, они также должны быть совместимы с существующими международными директивами.

Во избежание создания возможностей для роста преступности, существующие инфраструктуры электросвязи должны включать в себя меры безопасности технического и юридического характера. Атаки через киберпространство могут принимать различные формы: тайный захват системы, отказ в обслуживании, уничтожение или похищение важных данных, атака хакеров на сеть, взлом защиты программного обеспечения, фрикинг (включающий в себя саботаж, перехват телефонных звонков и т. п.). Затраты неизменно несут жертвы, т. е. организации и частные лица, на которых была направлена атака.

Рассматриваемая как система, электросвязь (инфраструктуры и услуги) поднимает проблему безопасности, которая во многом аналогична проблеме IT ресурсов. Те же самые технические, организационные и человеческие ограничения можно наблюдать при попытке решения данной проблемы. Защита информации при передаче необходима, но самой по себе ее не достаточно, поскольку степень уязвимости возрастает, во всяком случае, тогда, когда информация проходит стадию обработки и хранения. Поэтому кибербезопасность нужно рассматривать в более общем смысле. Чисто технические решения в вопросах кибербезопасности не могут компенсировать

отсутствия четкого и точного управления нуждами, мерами, процедурами и инструментами безопасности. Неорганизованный стихийный переход к получению инструментов безопасности будет помехой в использовании, осложнит операции и ухудшит показатели работы IT систем. Правильная IT безопасность – это вопрос управления, и объединенные инструменты и услуги связаны с администрированием операционных систем. Например, шифрование данных для их защиты при передаче бессмысленно, если впоследствии они хранятся незащищенным образом. Таким же образом, установка брандмауэра (защитной системы) будет бесполезной, если устанавливать соединения разрешено в обход данной системы.

Если действия по обработке информации должны будут расширяться и сократят "цифровой разрыв", для этого потребуются:

- надежные и безопасные информационные инфраструктуры (с гарантированной доступностью, наличием, надежностью и непрерывностью услуг);
- меры по повышению надежности;
- соответствующая правовая база;
- законодательные власти и органы безопасности, хорошо знакомые с новыми технологиями и способные сотрудничать с коллегами из других стран;
- инструменты управления безопасностью и информационным риском;
- инструменты защиты, которые будут поощрять доверие в предлагаемых приложениях и услугах (коммерческие и финансовые операции, электронное здравоохранение, электронное правительство, электронное голосование и т. д.) и в процедурах, защищающих права человека, особенно тайну личных данных.

Хорошее управление активами цифровой информации, распространение нематериальных товаров, использование контента и устранение "цифрового разрыва" – все это примеры экономических и социальных проблем, решать которые не возможно путем рассмотрения только технологической стороны IT безопасности. Подход, учитывающий человеческую, юридическую, экономическую и технологическую стороны требований безопасности цифровой инфраструктуры и пользователей, может помочь создать уверенность и вести к экономическому росту, в результате которого преуспеет все общество.

КАК ПОЛЬЗОВАТЬСЯ ДАННЫМ РУКОВОДСТВОМ

Руководство по кибербезопасности представляет собой введение в данную проблему, где подчеркивается, что изменилось с появлением цифровых данных, виртуализации информации и широкого использования сетей электросвязи. То, что на карту поставлено развитие общества, приводится для того, чтобы объяснить необходимость безопасности в мире IT и электросвязи (кибербезопасность).

В части I особое внимание уделяется потребности в кибербезопасности, и в общих чертах описываются некоторые элементы решений. Концепция безопасности инфраструктуры связи анализируется с точки зрения наблюдаемых слабых мест в системе защиты и нехватки безопасности информационно-коммуникационных технологий. На основе уроков, полученных при изучении лучших стратегий, затем определяется повседневная безопасность в интернете, и опыт, полученный международным сообществом, а также особые потребности в кибербезопасности развивающихся стран.

Анализируются управленческая, политическая, экономическая, социальная, юридическая и технологическая стороны кибербезопасности. Формулируются общие рекомендации, касающиеся доступа к инфраструктурам электросвязи, с целью управления рисками – как криминального, так и некриминального происхождения – и поощрения доверия в области электронных услуг, которая является важной движущей силой экономического развития.

Часть II касается проблем контролирования киберпреступности. Элементы, стимулирующие преступную деятельность, рассматриваются здесь для того, чтобы показать ограниченность современных подходов к вопросам безопасности и борьбе против киберпреступности. Также рассматривается сложность и иерархия проблем, с которыми мы сталкиваемся.

Представлены различные нарушения и преступления, которые могут быть совершены через интернет, большое внимание уделяется экономическим преступлениям. Анализируется наблюдаемое поведение преступников, например, профиль преступников-хакеров, общее описание атак и злонамеренного программного обеспечения. Даются некоторые указания по подготовке к борьбе с киберпреступностью.

В части III приводится обзор некоторых важных основных сведений о мире электросвязи. Кроме того, представлены функциональный подход и критический обзор инструментов безопасности инфраструктуры.

В части IV описывается всесторонний подход к кибербезопасности, учитывающий различные юридические аспекты современных технологий. Кроме того, намечаются возможные цели, касающиеся решений по безопасности для инфраструктуры связи.

В конце Руководства по кибербезопасности читатель найдет глоссарий терминов по безопасности и список необходимой справочной литературы и других документов.

ВЫРАЖЕНИЕ ПРИЗНАТЕЛЬНОСТИ

Бюро развития электросвязи МСЭ хотело бы выразить признательность г-же Соланж Гернаоути-Хелие и благодарность ее коллегам за их поддержку, в особенности Мохаммеду Али Сфакси, Игли Таши, Сарре Бен Лага, Хенд Мадхур и Арно Дюфуру (консультант по интернет-стратегии).

Данное руководство составлено на основе информации и исследований, предоставленных различными организациями, в частности организациями по кибербезопасности "Clusif" (*Club de la sécurité informatique français*) и "Cert" (Computer Emergency and Response Team). Они заслуживают нашу искреннюю признательность.

Подготовка данного руководства была бы невозможна без сотрудничества с работниками Отдела электронной стратегии МСЭ и в особенности Александром Нтоко. Нам также хотелось бы выразить признательность Рене Збинден Мослэн (Служба компановки документов МСЭ) и ее команде за работу по публикации данного Руководства по кибербезопасности.

СОДЕРЖАНИЕ

Стр.

Стр.

Стр.

Стр.

ЧАСТЬ I

Кибербезопасность – Задачи, стоящие в данном контексте, решения

Раздел I.1 – Мировое информационное пространство и информационное общество

I.1.1 Преобразование в цифровую форму

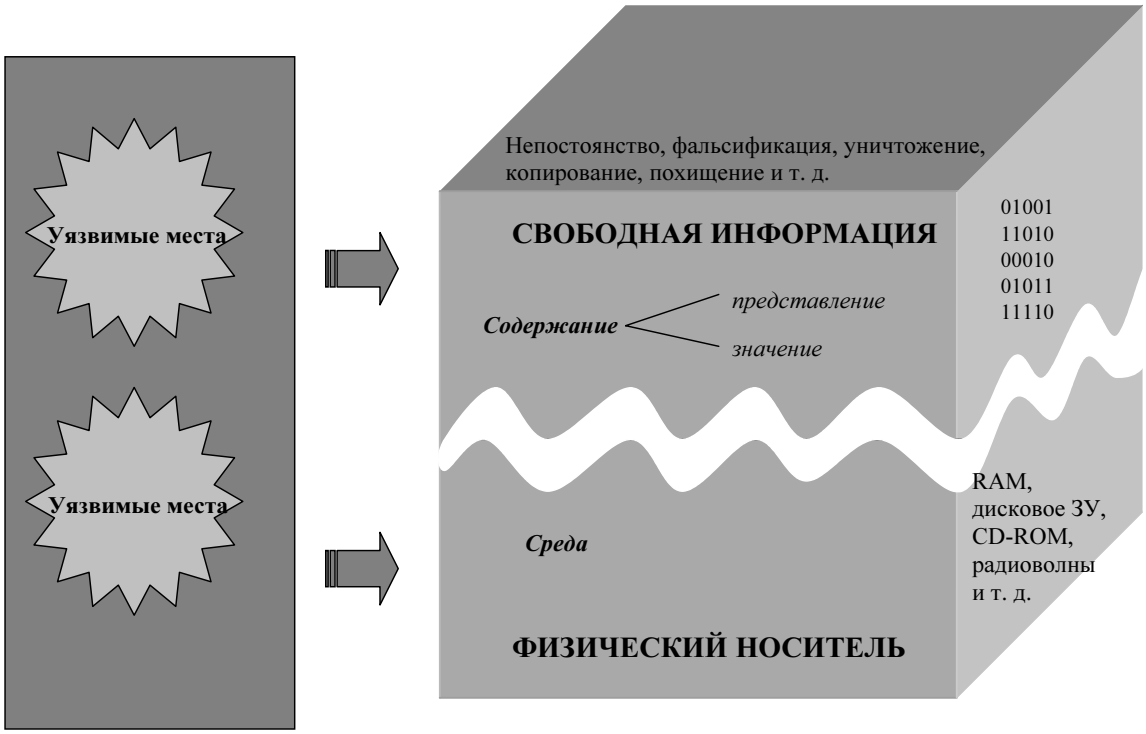
Информационные технологии преобразуют наш образ мыслей и соприкасаются почти со всем в нашей жизни. Они вызывают важные структурные изменения, позволяя нам моделировать любые *объекты* в форме информации, а затем управлять ими посредством электроники.

I.1.1.1 Цифровая информация

Преобразование в цифровую форму создает цифровой образ чего-то реального (виртуальная версия объекта). Вся информация любой природы, будь то звук, данные или изображение, может быть преобразована в цифровую форму и представлена в определенном стандартном виде.

Цифровая информация отделяется от конкретного воплощения, то есть она больше не привязана к среде, в которой она воспроизводится и хранится. Ценность информации самой по себе (содержания) повышается, потому что совместно использовать и хранить информацию стоит гораздо дешевле, чем производить ее (рисунок I.1). Кроме того, данные можно хранить и обрабатывать в нескольких местах одновременно. Возможность безупречного копирования до бесконечности обесценивает понятие "исходных" данных, что обычно затрудняет реализацию охраны авторского права.

Рисунок I.1 – Виртуализация и цифровая информация



I.1.1.2 Цифровая технология

Цифровая технология сделала возможным создание непрерывной цепи цифровой информации путем стандартизации производства, обработки и передачи данных. В комбинации с технологиями сжатия данных эта цифровая конвергенция создает возможности для совместной деятельности IT, электросвязи и аудиовизуальных средств, примером чего является явление интернета. Таким образом, настоящая технологическая революция была вызвана преобразованием информации в цифровую форму, поскольку последствия этого преобразования выходят за рамки мира электросвязи.

Эта новая сторона обработки информации влияет на все сферы человеческих стремлений и работы. В последние годы были разработаны как определение начисления стоимости, так и способы производства, начиная от разработки продукции до ее распределения. Это привело к реорганизации цепочек начисления стоимости среди различных участников экономики.

I.1.1.3 Инфраструктура и содержание

Управление цепочкой цифровой информации, т. е. инфраструктурой и содержанием, стало основной задачей XXI века. Новый рынок, открытый для всех, характеризуется беспрецедентной мобилизацией всех участников экономики: операторов электросвязи, организаций кабельного телевидения, производителей аппаратного и программного обеспечения, телевизионных компаний и т. д.

Новая экономическая задача для современной организации – это задача, созданная при помощи свободной конкуренции и реорганизации ролей и деятельности.

Когда Гуттенберг напечатал свою первую книгу, он не мог даже представить себе промышленных последствий, которые будет иметь его изобретение; в данном случае это событие стало первым шагом на пути к промышленной автоматизации. Нечто похожее произошло в конце 1960-х годов XX века, когда университеты и военные для своих, по-видимому, противоречащих друг другу целей начали создавать сеть связи, которая в последствии стала интернетом. Как и их предшественники XV века, они действовали, не осознавая полностью, последствий своего изобретения. В наши дни, киберпространство возвещает о переходе общества в век информации.

I.1.2 Информационная революция

Информационная революция основательно меняет способ обработки и хранения информации. Она изменяет работу организаций, да и всего общества в целом. В последние годы это была не единственная техническая инновация, она выделяется среди других, т. к. оказывает влияние на обработку информации и, следовательно, на знания. Поскольку информационная революция влияет на механизмы, при помощи которых создаются и совместно используются знания, ее можно рассматривать как источник инноваций будущего, которые затронут и развивающиеся страны.

Эволюция информационных технологий и технологий электросвязи ведет к настоящей революции в нашем представлении об экономическом, социальном и культурном обмене. Эта эволюция дает нам также и новую модель информационной технологии на основе сети, в которой необходимо гарантировать защищенность потока информации, если нужно разработать новые приложения, которые сделают работу организаций еще эффективнее. Ни одна из форм деловой активности не может существовать без обмена и взаимодействия между участниками; обмен информацией невозможен без основных гарантий безопасности; не одну услугу нельзя планировать без учета качества этой услуги. Однако мы также должны помнить, что успех коммуникации зависит от способности участвующих сторон справляться с техническими ограничениями и управлять клиентурой, которая входит в любой обмен информацией.

I.1.2.1 Инновации и развитие

Если организации и страны хотят выжить и утвердиться в качестве долговременных участников в новом конкурентном окружении, им необходимо сконцентрироваться на инновационных возможностях и быстрой способности адаптироваться при поддержке мощной и защищенной информационной системы.

Появляются новые сферы деятельности на основе диверсификации электросвязи и возможностей, создаваемых развивающейся информационной технологией, преимущества которой должны также возрастать и для развивающихся стран.

Технологический и экономический прогресс, осуществляемый при помощи развертывания надежных IT инфраструктур, открывает перед обычными людьми широкие перспективы. В то же время он имеет беспрецедентную степень технической и управленческой сложности. Во избежание искажения самой сути прогресса нужно контролировать важные сопутствующие риски. Технологическому риску, например, авариям систем связи и обработки информации, вызванным неполадками случайного или злонамеренного характера, сопутствует информационный риск подрыва способности организации использовать информацию.

Важно помнить, что несмотря на то, что доступ к информационной технологии широко распространен, информационная революция еще не затронула значительную часть населения. Причины этого сложны, они включают в себя культурный и финансовый факторы, а также, в некоторых случаях, элементарные трудности такие, как неграмотность. Больше, чем в любой другой области, образование и профессиональная подготовка являются ключевыми факторами в демократизации информационной технологии и борьбе с информационным вакуумом. Также необходимо заново продумать интерфейс связи так, чтобы он лучше служил населению и уважал различия между культурными контекстами. Компьютеры следует адаптировать к человеческой среде, в которую они интегрируются, а не создавать новую систему взаимодействия.

I.1.2.2 Поддержка информационной революции

Информационно-коммуникационные технологии, как и все технологии, возникают и работают в определенной исторической и географической ситуации, что в общем виде отражает соотношение сил в обществе. Обязанностью людей, участвующих в информационной революции, является поддержка ее при помощи инструментов, процедур, законов и моральных правил, необходимых для создания безопасности и оправдания ожиданий и удовлетворения нужд общества.

В настоящее время использование средств связи и свобода отправлять и получать сообщения частично охватываются большим количеством мер частичного регулирования от МСЭ, ЮНЕСКО, ООН, Организации экономического сотрудничества и развития, Совета Европы и др. Достижения в области информационно-коммуникационных технологий и то, как люди используют их, опередило регулирование, которое управляет ими. Поэтому необходимо создать подходящую правовую базу для решения таких проблем, как: нетерриториальная природа сетей таких, как интернет, проблемы ответственности и защита частной жизни и прав собственности. Технологическая революция должна идти параллельно с эволюцией социальной, политической и юридической ситуации. Это беглое замечание уже дает представление о важности проблем, возникающих в век информации, ключевой роли электросвязи в их решении и важности рассмотрения вопросов безопасности до того, как они стали помехой развитию.

Переход в век информации показывает важность информационной технологии и необходимость ее совершенствования. При рассмотрении новых сторон, создаваемых IT, в технических и социоэкономических показателях, становится ясно, что безопасность IT систем и систем электросвязи стала основной потребностью. Подчеркивается стратегическая и критическая природа того, что поставлено на карту при планировании и реализации кибербезопасности для стран, организаций и частных лиц.

С точки зрения финансовых, материальных и человеческих ресурсов, которые страны вложили в создание своей информационной инфраструктуры и структуры электросвязи, для стран важно гарантировать, что инфраструктура защищена, хорошо управляется и контролируется.

Раздел I.2 – Кибербезопасность

I.2.1 Контекст безопасности в инфраструктуре связи

Понимание важности преодоления эксплуатационных рисков IT возрастает при растущем использовании новых технологий, существовании глобальной инфраструктуры IT и появлении новых рисков.

Превращение общества в *информационное* общество, ставшее возможным благодаря интеграции новых технологий в каждую сферу деятельности и во все типы инфраструктур, увеличивает зависимость частных лиц, организаций и стран от информационных систем и сетей. Это является основным источником рисков, который следует рассматривать как риск безопасности.

Развивающие страны сталкиваются с проблемой необходимости присоединения к информационному обществу, не игнорируя риски зависимости от технологий и поставщиков технологий, и стараясь избежать опасности того, что "цифровой разрыв" вызовет "разрыв" в области безопасности или даже усилит зависимость от объектов, контролирующих их потребности и средства безопасности IT[1].

При планировании, разработке, установке и управлении инфраструктурами электросвязи, а также услугами и деятельностью, которые они делают возможными, необходимо помнить о безопасности. Безопасность является краеугольным камнем любой деятельности; ее следует рассматривать как услугу, делающую возможной создание других услуг и добавление стоимости (например, электронное правительство, электронное здравоохранение, электронное обучение). Безопасность является не только вопросом технологии[2]. Однако до настоящего момента основные доступные инструменты связи не имели ресурсов, необходимых и достаточных для обеспечения или гарантирования минимального уровня безопасности.

Доступ к IT системам, объединенным в сеть, может осуществляться на расстоянии; по существу они являются потенциальными объектами кибератаки. Системы подвергаются повышенному риску вторжения и возможности осуществления атак и совершения преступлений увеличиваются. Наряду с тем, что целью атак являются системы, действия преступников направлены на обрабатываемую информацию (рисунок I.2). Атаки могут повлиять на способности системы обрабатывать, хранить и совместно использовать информационный капитал, и они могут нанести ущерб нематериальным или символическим товарам, процессам производства и процессам принятия решений в организации. Компьютерные системы несут операционные риски при осуществлении деятельности организаций, которые ими обладают.

Таким образом, решение комплексных и многогранных проблем кибербезопасности, связанных с сетями электросвязи и открытыми системами может быть относительно сложным, а потенциальные последствия и влияние на деятельность организаций и стран может быть разрушительным. Факторы, являющиеся ключевыми для успеха экономик, могут зависеть от способности обеспечивать безопасность информации, процессов, систем и инфраструктуры.

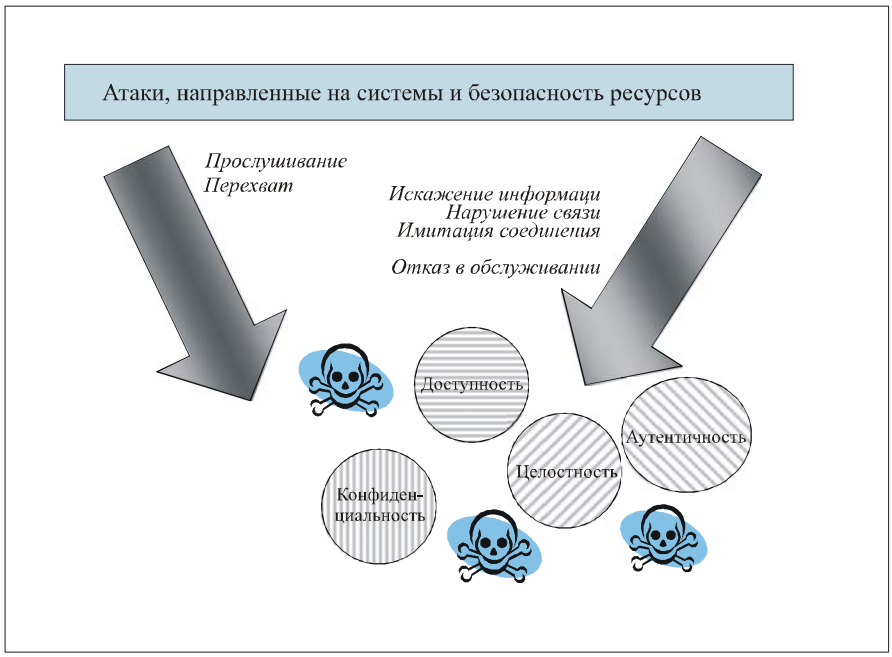
Широкое взаимодействие систем, увеличение связей между инфраструктурами, рост зависимости от цифровых технологий, а также увеличение опасностей и рисков вынуждает частных лиц, организации и страны принимать меры, вводить процедуры и приобретать инструменты для улучшения управления технологическими и компьютерными рисками. Задачи борьбы, содержащей технологические риски, – это задачи собственно 21 века. Они требуют всеобъемлющего подхода к безопасности, включающего в себя развивающиеся страны.

---

[1] С. Гернаоути-Хелие: "От "цифрового разрыва" к отсутствию цифровой безопасности: проблемы разработки и развертывания единой структуры электронной безопасности в многоаспектном контексте", в разделе *Международной сотрудничество и информационное общество* Справочника Швейцарии по политике развития, издательство IUED. Женева, ноябрь 2003 года.

[2] А. Нтоко: "Мандат и деятельность в области кибербезопасности – МСЭ-D". Тематическое заседание ВВУИО по вопросам кибербезопасности. МСЭ, Женева, 28 июня – 1 июля 2005 года.

Рисунок I.2 – Атаки, направленные на системы и безопасность ресурсов



Недостаточно просто установить точки доступа к сетям электросвязи. Необходимо развернуть надежные, восстановимые, устойчивые к ошибкам и безопасные инфраструктуры IT и киберуслуги при соблюдении основных прав человека и прав государств. Необходимость защиты систем и ценной информации должна сосуществовать и быть совместимой с параллельной защитой прав и приватности частных лиц.

Развивающимся странам необходимо входить в информационное общество, не подвергая себя чрезмерному риску, основываясь на опыте, приобретенном развитыми странами, и избегая опасности превращения кибербезопасности в новый фактор для их исключения.

I.2.2 Что кибербезопасность ставит на карту

Социальные вопросы, экономика, государственная политика, общественные проблемы: как на это ни посмотри, как ни назови (IT безопасность, безопасность электросвязи), кибербезопасность затрагивает безопасность цифрового и культурного благосостояния людей, организаций и стран (рисунок I.3). Возникающие проблемы сложны, и решение их требует политической воли для разработки и реализации стратегии по развитию цифровых инфраструктур и услуг, что включает в себя четкую, эффективную, поддающуюся контролю и управлению стратегию в области кибербезопасности. Стратегия кибербезопасности должна быть частью многодисциплинарного подхода, решения должны приниматься на образовательном, юридическом, управленческом и техническом уровне. Подход, учитывающий человеческую, юридическую, экономическую и технологическую стороны нужд безопасности цифровой инфраструктуры и пользователей, может помочь стимулировать доверие и вести к экономическому росту, в результате которого преуспеет все общество.

Овладение богатством цифровой информации, распределение нематериальных товаров, добавление стоимости к содержанию и устранение "цифрового разрыва" – проблемы экономической и социальной природы, которые требуют чего-то большего, чем односторонний, чисто технический подход к кибербезопасности.

Рисунок I.3 – Уровни кибербезопасности: частные лица, организации и страны

Если деятельность, основанная на обработке информации, будет развиваться и, таким образом, поможет сократить "цифровой разрыв", это потребует:

- надежных и защищенных информационных инфраструктур (с гарантированной доступностью, наличием, надежностью, и непрерывностью услуг);
- мер по созданию доверия;
- соответствующей юридической структуры;
- законодательных властей и органов безопасности, хорошо знакомых с новыми технологиями и способных сотрудничать с коллегами из других стран;
- инструментов управления безопасностью и информационными рисками;
- инструментов защиты, которые будут поощрять доверие в предлагаемых приложениях и услугах (коммерческие и финансовые операции, электронное здравоохранение, электронное правительство, электронное голосование и т. д.) и в процедурах, защищающих права человека, особенно приватность.

Целью кибербезопасности является помощь в защите имущества и ресурсов организаций в организационном, человеческом, финансовом, техническом и информационном аспектах, что позволит им выполнять свою задачу.

Конечной целью является гарантирование того, что им не будет нанесено никакого длительного вреда. Она состоит из снижения вероятности реализации угрозы; ограничения ущерба или неисправной работы и обеспечения того, что после инцидента, связанного с нарушением безопасности, можно будет восстановить нормальную работу за приемлемое время и с приемлемыми затратами.

Процесс кибербезопасности охватывает все общество, в котором реализация кибербезопасности касается каждого человека. Кибербезопасность можно сделать более важной путем разработки кодекса киберповедения для обеспечения соответствующего использования ИКТ и пропаганды подлинной политики безопасности, устанавливающей стандарты, соответствие которым, как ожидается, будут обеспечивать пользователи кибербезопасности, объекты, партнеры и поставщики.

I.2.3 Дефицит безопасности

Дефицит безопасности в информационно-коммуникационных технологиях является отражением природы информационных технологий и киберпространства. Тот факт, что пользователи передвигаются в виртуальном мире, действуя на расстоянии и относительно анонимно, создает трудности при разработке, реализации, управлении и контроле данной технологии; если добавить к этому аварии, сбои в работе, ошибки, неверные действия пользователя, несовместимость и даже стихийные бедствия, в результате мы получим, что не удивительно, атмосферу ненадежности, которая портит IT инфраструктуру (см. рисунок I.4).

Рисунок I.4 – Инфраструктура интернета и многочисленные причины проблем

В данном контексте существует много способов, при помощи которых преступники могут использовать слабые места в системе защиты[3].

Распространение таких атак – включая кражу идентификационной информации, получение доступа к системе обманным путем, вторжение, кража ресурсов, заражение вирусом, порча, разрушение, преступное использование, нарушение конфиденциальности, отказ в обслуживании, кража, вымогательство и т. д. – иллюстрирует ограниченность современных стратегий безопасности, но также, как это ни парадоксально, показывает, что инфраструктура обладает определенной надежностью.

Какими бы ни были мотивы отдельных компьютерных преступников, результаты атак всегда включают в себя далеко не простое влияние на экономику. Киберпреступность быстро превращается в международное чудовище с головами гидры.

Решения проблем безопасности существуют, однако они не являются абсолютными, обычно они представляют собой всего лишь ответ на определенную проблему в определенном контексте. В результате происходит замещение данной проблемы безопасности, и ответственность за безопасность перекладывается; более того, необходимо, в свою очередь, защищать и управлять решениями защищенным способом.

[3] Киберпреступность, компьютерные атаки и преступления подробно рассматриваются в Части II.

Они представляют, в лучшем случае, экспериментальную попытку бороться с динамической реальностью, с которой они сталкиваются: быстро меняющаяся технология, непостоянные цели, совершенствующиеся умения хакеров и видоизменяющиеся угрозы и риски. Таким образом, не может быть гарантии того, что определенный подход к безопасности обеспечит длительную защиту, так же как и то, что можно гарантировать прибыль от инвестиций, которые представляет данный подход.

Стратегия безопасности часто ограничивается установлением механизмов по сокращению рисков, которым подвергаются информационное имущество организации, обычно посредством чисто технологического подхода. Лучшей стратегией будет та, которая учитывает все стороны данной проблемы и удовлетворяет потребности частных лиц в безопасности, в особенности того, что касается защиты частной жизни и основных прав человека. Кибербезопасность должна охватывать всех, распространяя защиту на данные личного характера.

Решения безопасности уже доступны. Во многих случаях они являются чисто технологическими по характеру, решая определенную проблему в определенном контексте. Но, как и любая технология, все они подвержены ошибкам и их можно обойти. В большинстве случаев они только замещают проблему безопасности и перекладывают ответственность на другую часть системы, которую, как предполагается, они должны защищать. Более того, сами решения безопасности нуждаются в защите и безопасном управлении. Они не могут предоставить абсолютной или конечной защиты, из-за эволюционной природы контекста безопасности, который сам является результатом динамического окружения (меняющиеся потребности, риски, технологии, умения хакеров и т. д.). Таким образом, появляется проблема, поскольку существующие решения, в лучшем случае, действуют недолго. Другой проблемой является то, что быстрое увеличение разнородных решений может нанести вред общей согласованности стратегии безопасности. Очевидно, что одной технологии недостаточно; ее необходимо интегрировать в управленческий подход.

Достичь общей согласованности стратегии безопасности нелегко из-за наличия широкого диапазона различных объектов и частных лиц, участвующих в данном процессе (инженеров, разработчиков, системных инженеров, юристов, испытателей, клиентов, поставщиков, пользователей и т. д.), а также широкого круга интересов, взглядов, окружений и языков. Если мы хотим достичь такого уровня безопасности, который требуется для уверенного ведения деятельности при использовании информационных и коммуникационных технологий, и сделать вклад в создание доверия в цифровой экономике, необходим единый, системный взгляд на риски, связанные с безопасностью и предпринимаемые меры, а также понимание ответственности, лежащей на всех участниках.

I.2.4 Уроки, которые необходимо извлечь

I.2.4.1 Осуществляй контроль безопасности

В начале XXI века большинство крупных и множество небольших организаций осознали важность решения проблем безопасности IT. Стратегия безопасности больше не рассматривается только как набор разнородных инструментов безопасности. Наоборот, повсеместно ее стали правильно рассматривать как непрерывный процесс.

Целью управления безопасностью является гарантирование того, что в каждый определенный момент времени в каждом определенном месте используются наиболее подходящие меры безопасности. Данная концепция базируется на следующих простых вопросах:

- Кто, что, как и когда делает?
- Кто разрабатывает правила, определяет, утверждает и реализует их и осуществляет контроль над ними?

I.2.4.2 Определяй и управляй рисками

Стратегия безопасности для цифровых инфраструктур должна опираться на анализ рисков, связанных с обработкой информации, электросвязью и киберпространством, как часть процесса управления рисками. Необходимо определять риски безопасности IT (которые также называют компьютерными рисками, информационными рисками или технологическими рисками) наряду с другими рисками, с которыми сталкиваются организации (стратегические, социальные, экологические и т. д.)

Риски IT – это операционные риски, которые необходимо снижать. В основе управления рисками лежит анализ требований безопасности, который позволяет определить стратегию защиты и политику безопасности. На этом этапе необходимо ответить на несколько вопросов:

- Кто будет осуществлять анализ риска и управление рисками?
- Каким способом лучше осуществить такой анализ?
- Какие имеются инструменты и методы?
- Насколько они надежны?
- Насколько важны будут результаты? Каковы издержки?
- Не будет ли лучше привлечь соисполнителей для выполнения данной функции?
- И т. д.

Риск можно определить как опасность, которую можно в некоторой степени предвидеть. Величина риска оценивается по вероятности ущерба и получающемуся в результате урону. Риск выражает вероятность потери имущества или ценностей из-за уязвимости, связанной с некоторой угрозой или опасностью.

При принятии решения о необходимом уровне защиты и типах вводимых мер безопасности необходимо соотнести величину риска (в финансовом плане) и стоимости мер по снижению риска (см. рисунок I.5). Как минимум, необходимо определить имущество, которое нужно защитить, а также основную причину, по которой нужно защитить данное имущество в зависимости от реальных ограничений и имеющихся в наличии организационных, финансовых, человеческих и технических ресурсов. Принимаемые меры должны быть эффективными и должны отражать баланс между показателями работы и экономической целесообразностью.

Для организации преодоление рисков IT означает выработку стратегии, определение политики безопасности и ее тактической и оперативной реализации.

Рисунок I.5 – Компромиссы в управлении рисками: стратегическое решение

I.2.4.3 Определяй политику безопасности

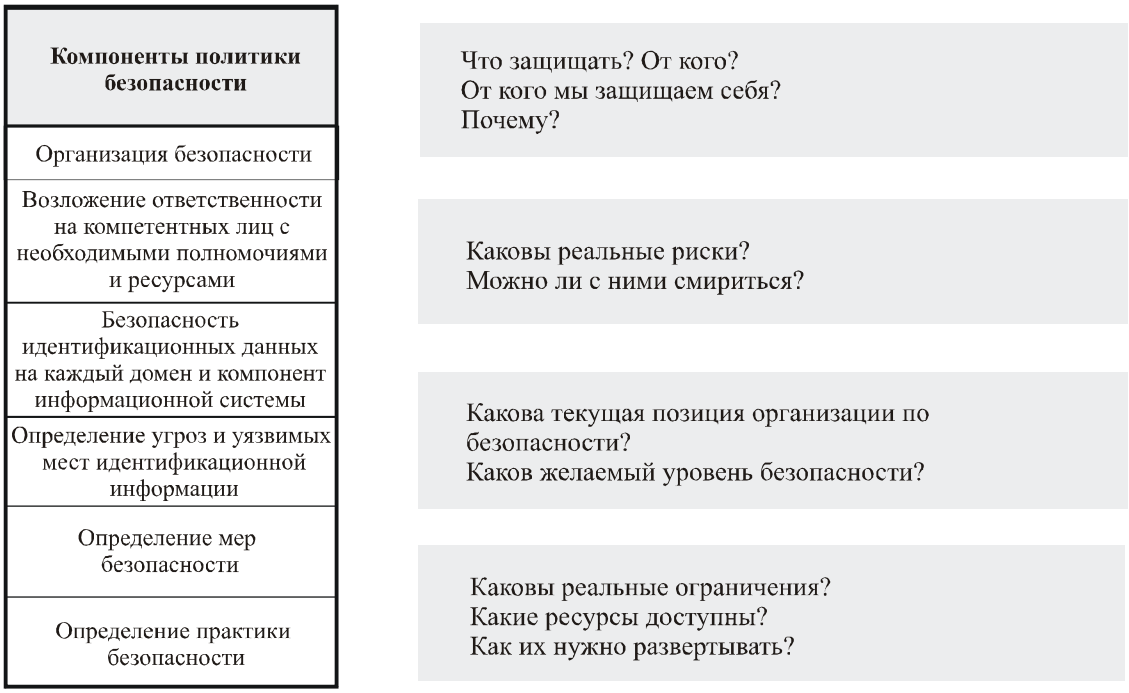
Политика безопасности переводит то, что понимается под рисками и их влиянием, в меры безопасности для реализации. Она облегчает как меры по предотвращению, так и меры по исправлению ситуации, необходимые в связи с проблемами безопасности, и помогает сократить риски и их влияние.

Поскольку полностью устранить риски невозможно, как и предвидеть все возникающие угрозы, важно уменьшить уязвимость среды и ресурсов, которые необходимо защищать, поскольку это лежит в основе многих проблем безопасности.

Политика безопасности должна устанавливать, помимо всего прочего, ресурсы, структуру, процедуры и планы защиты и подавления для гарантии того, что операционные, технологические и информационные риски можно контролировать.

В стандарте ИСО 17799 предлагаются нормы и правила для управления безопасностью. Данный стандарт можно рассматривать как справочник для определения политики безопасности; как перечень контрольных вопросов для анализа риска; как инструмент проверки безопасности, как для сертификации, так и для других целей; или как центр коммуникации для безопасности. Данный стандарт можно интерпретировать и реализовывать по-разному. Ценность данного стандарта основывается на том, что в нем учитываются организационные, человеческие, юридические и технические аспекты безопасности на всех стадиях разработки, реализации и поддержания безопасности. В версии данного стандарта (ИСО/МЭК 17799:2005)[4] 2005 года придается особое значение оценке и анализу риска, управлению имуществом и ресурсами, а также управлению в службе происшествий. Это указывает на важность управленческой стороны безопасности.

Рисунок I.6 – Для управления безопасностью, сначала необходимо определить политику безопасности



Эффективность политики безопасности не следует оценивать по размеру бюджета этой политики; скорее, эффективность зависит от политики управления рисками, и от качества анализа рисков (рисунок I.6). Среди факторов, определяющих риск, находятся сфера деятельности организации, ее размер, репутация, уязвимость системы, системное окружение и связанные с ним угрозы и степень, в которой данная организация зависит от своей информационной системы.

Качество безопасности IT зависит, главным образом, от определения и оценки информационных активов, оперативного развертывания соответствующих мер безопасности, основанных на хорошо продуманной политике безопасности, и эффективном управлении.

[4] Содержание данного стандарта приводится в Приложении B настоящего Руководства.

I.2.4.4 Развертывай решения

Для того чтобы сделать инфраструктуру IT и электросвязи более защищенной, необходимо ввести различные типы мер. Они включают в себя:

- улучшение осведомленности; обучение и профессиональная подготовка всех организаторов кибербезопасности;
- создание элементов, которые могут выступать в качестве национального центра раннего оповещения и кризисного центра, объединить в общий фонд ресурсы, необходимые для эффективного функционирования таких центров, и распределить их по нескольким странам или региону;
- введение наблюдения и проверки (аналогичные проверкам на дорогах);
- повышение компетентности команды компьютерной полиции, которая может способствовать совместному международному расследованию и судебному преследованию преступлений, связанных с компьютерами;
- разработка технологических решений для управления идентификационной информацией, контроля доступа, использования защищенных платформ аппаратного и программного обеспечения, поддержки инфраструктур, шифрования протоколов и оперативного управления.

I.2.5 Взгляд на управление

I.2.5.1 Динамическое управление[5]

Обеспечение безопасности при помощи процессов динамического и непрерывного управления означает, что организация имеет дело с динамической природой риска и возрастающими потребностями путем постоянной адаптации и улучшения своих решений. Уровень безопасности будет определяться качеством управления безопасностью. Политику кибербезопасности следует определять на уровне высшего руководства. Стратегий, мер, процедур и решений, касающихся безопасности, столько же, сколько организаций, имеющих потребности в безопасности, которые необходимо удовлетворять в любой момент времени.

В качестве примера динамического контекста, в котором должно осуществляться управление безопасностью, рассмотрим процесс обнаружения и ликвидации уязвимых мест безопасности. Данный процесс осуществляется при помощи периодического выпуска так называемых "заплат" (файлов с исправлениями) для устранения ошибок безопасности. Информационные бюллетени, более или менее заказные, информируют об уязвимых местах, которые были обнаружены, и о том, как их ликвидировать. Если необходимо поддерживать минимальный уровень безопасности, администратору по безопасности или системному администратору нужно будет устанавливать "заплаты" безопасности по мере их выпуска. Однако знание об опасных уязвимых местах системы полезно не только для администратора по безопасности, но также и для хакеров, которые могут попытаться воспользоваться данными недоработками до применения "заплат" безопасности. Поэтому необходимо выделять достаточное количество ресурсов для реализации динамического управления, в ходе которого решения по безопасности постоянно обновляются, и, таким образом, поддерживается соответствующий уровень безопасности.

Публикуемые предупреждения и "заплаты" позволяют администратору контролировать процесс обновления (решая, инсталлировать эти "заплаты" или нет); также возможно делать это в автоматическом режиме, эффективно делегируя ответственность за регулярную и систематическую установку "заплат" издателю программного обеспечения.

В связи с этим возникает вопрос об ответственности. Например, каковы юридические последствия отклонения обновленного программного обеспечения, когда из-за использования неисправленного уязвимого места системы возникают проблемы? Поскольку в ходе многочисленных атак происходит именно это, вопрос о том, кто решает, и об ответственности системного администратора является очень уместным.

---

[5] Следующие два раздела заимствованы из статьи "*Sécurité informatique, la piège de la dépendance*", А. Дюфур, С. Гернаоути-Хелие, *Revue Information et Système*, 2006 год.

Динамический аспект безопасности представляет важную задачу не только для поставщиков инструментов безопасности и издателей программного обеспечения, но также и для системных администраторов и администраторов по безопасности, у которых редко находится время для интегрирования всех имеющихся в наличии "заплат" и обновлений.

Поскольку компьютерные менеджеры, администраторы по безопасности и системные администраторы имеют полный доступ к IT ресурсам организации, необходимо не только применять строгие процедуры надзора и контроля их деятельности (пропорционально рискам, которым они потенциально подвергают подконтрольные им системы), но данные сотрудники должны также демонстрировать безукоризненную честность.

I.2.5.2 Привлечение соисполнителей и зависимость

Поставщики услуг, эффективно предлагающие антивирусные и антиспамные фильтры берут на себя часть управления безопасностью своих клиентов. Данная тенденция начинает менять распределение ролей и ответственности в вопросах безопасности. Безопасность будет все больше переходить в руки поставщика услуг или технического поставщика. Конечно, данный переход не решает проблему безопасности, он просто переводит эту проблему к поставщику услуг, который становится ответственным не только за доступность и качество услуги, но также и за управление и поддержку определенного уровня безопасности.

Издатели антивирусного программного обеспечения обычно предлагают услугу автоматического обновления. Добавление этого нового аспекта услуги делает аренду программного обеспечения все более привлекательной, поскольку ответственность за поддержание переходит к издателю на длительный период. Данный процесс также стимулирует более сильную тенденцию к привлечению соисполнителей приложений и сопутствующей модели предприятия.

Вопрос привлечения соисполнителей или делегирования всей или части задачи безопасности не является чисто техническим. Данный вопрос является стратегическим и юридическим, и он ставит фундаментальный вопрос о зависимости от поставщиков.

Стратегия привлечения соисполнителей в области безопасности может включать в себя определение политики безопасности, реализацию ее, управление доступом, администрирование защитной системы, удаленную поддержку систем и сетей, поддержку приложений третьей стороны, резервное управление и т. д. Выбор соисполнителя должен сопровождаться процессом контроля качества и может учитывать такие аспекты, как опыт соисполнителя, их компетенция, используемые технологии, время ответного действия, вспомогательные услуги, контрактные договоренности (например, гарантированные результаты) или распределение юридической ответственности.

I.2.5.3 Превентивные действия и реагирование[6]

Превентивные действия в вопросах безопасности по определению являются упреждающими. Они включают в себя человеческий, организационный, экономический (соотношение между стоимостью реализации/уровнем безопасности/предлагаемыми услугами) и технологический аспекты. До настоящего времени безопасность окружения IT по большей части касалась только технического аспекта. Такое понимание безопасности информационных систем, главным образом с технической точки зрения, без учета человеческого аспекта, представляет собой настоящую проблему контроля технического риска, связанного с преступлениями. Это происходит потому, что преступность является в первую очередь человеческим, а не техническим фактором. Поэтому чисто техническое реагирование не подходит для контроля того, что по существу является человеческим риском.

Обычный подход к IT преступности – это реагирование и судебное преследование. Оно, соответственно, происходит после совершения преступления, т. е. следует за инцидентом, который, по определению, выявил пробел в защитных мерах. Необходимо не только предотвращать кибератаки и противостоять им путем разработки следственных/уголовных механизмов, но и определять в политике безопасности меры, необходимые для борьбы с атаками и преследования нападающих. Для этого нужно разработать и реализовать запасные планы и планы бесперебойности, включающие в себя ограничения, относящиеся к расследованию и судебному преследованию киберпреступности в рамках различных рабочих процессов и целей, а также особые шкалы времени.

---

6 Данный раздел заимствован из книги *Sécurité informatique et réseaux* С. Гернаоути-Хелие, Дюно 2006 год.

I.2.6 Политический аспект

I.2.6.1 Ответственность государства

Государство несет значительную ответственность за реализацию цифровой безопасности. Это особенно касается определения надлежащей единой и практичной юридической структуры. Государство не должно только лишь содействовать исследованиям и развитию в области безопасности, оно также должно поощрять культуру безопасности и требовать соответствия минимальным стандартам безопасности (в продукты и услуги должна быть включена защита), при этом усиливая обеспечение правопорядка в отношении киберпреступности. Здесь встает вопрос о роли лежащей в основе финансовой модели и партнерства между государственным и частным сектором для планов действий на национальном и международном уровнях.

На стратегическом уровне необходимо гарантировать предотвращение, отчетность, обмен информацией и аварийное администрирование. Также необходимо повышать осведомленность о лучших способах управления рисками и безопасностью. Еще одним необходимым требованием является координация и гармонизация правовых систем. Нужно также содействовать обеспечению порядка и безопасности и выработать план совместных действий (формальные/неформальные, многосторонние/двусторонние, активные/пассивные, национальные/международные).

В то же время важно обеспечивать информацией и проводить обучение и профессиональную подготовку в области обработки информации и коммуникационных технологий, а не просто вводить меры защиты и сдерживания. Повышение осведомленности о вопросах безопасности не должно ограничиваться продвижением определенной культуры безопасности и кодекса киберповедения. Культура безопасности должна подкрепляться культурой IT.

Различным участникам нужно дать средство, для того чтобы научиться справляться с техническими, операционными и информационными рисками, угрожающими им при использовании новых технологий. В данной ситуации государство должно также способствовать предоставлению отчетности по случаям киберпреступности и обеспечивать доверие между различными участниками экономического мира и законодательными и правоохранительными органами.

Данные органы, а также органы гражданской обороны, вооруженные силы и органы безопасности играют тактическую и оперативную роль в борьбе против киберпреступности, для того чтобы защищать, преследовать и восстанавливать. Центры надзора, обнаружения, а также информационные центры для IT и криминальных рисков должны быть оперативными, для того чтобы обеспечивать предотвращение, необходимое для контроля этих рисков.

Каждое государство самостоятельно определяет политику развития информационного общества, отражающую его собственные ценности и обеспечивает необходимые ресурсы для реализации этой политики. Она включает в себя средства защиты и борьбу против киберпреступности.

Для глобального, централизованного и координированного сдерживания киберпреступности необходимо реагирование на политическом, экономическом, юридическом и техническом уровнях, единое реагирование, которое смогут осуществить все участники цифровой цепочки, являющиеся коллегами в области безопасности.

I.2.6.2 Суверенитет государства

Желаемая простота и эффективность в области безопасности не соответствует сложности потребностей и окружения, что делает привлечение соисполнителей для предоставления услуг и обеспечения безопасности систем и информации более привлекательным для специализированных поставщиков. Данная тенденция создает высокую или полную степень зависимости. Это является основным риском безопасности. Государства должны опасаться попадания в зависимость от внешних объектов, неконтролируемых ими, в области стратегического, тактического и оперативного управления.

Правительства играют важную роль в осуществлении следующего:

- встраивать возможности безопасности (безопасность по умолчанию) удобные для пользователя, наглядные, понятные и поддающиеся проверке;
- удерживать частные лица и организации от попадания в опасные ситуации (избегать ненадежных конфигураций, рискованного поведения, попадания в зависимость и т. д.);
- обеспечивать соответствие стандартам безопасности;
- уменьшение количества уязвимых мест в технологиях и решениях безопасности.

I.2.7 Экономический аспект

Суть безопасности состоит не в том, чтобы зарабатывать деньги, а в том, чтобы не терять их. Хотя, как может показаться, оценивать то, сколько стоит безопасность (связанные бюджеты, стоимость продуктов безопасности, обучение и т. д.) довольно легко, говорить о прибыльности безопасности довольно трудно. Исходя из субъективного подхода, можно предположить, что меры по обеспечению безопасности в действительности имеют "пассивную" форму эффективности, предотвращающую определенные возможные убытки.

Тем не менее, трудно оценить стоимость безопасности и издержки, связанные с убытками, возникшими из-за аварий, ошибок или действий злоумышленников. Стоимость безопасности является результатом потребностей организации и зависит от имущества, которое необходимо защищать, и стоимости ущерба нанесенного в результате недостаточного обеспечения безопасности. Таким образом, готовых ответов на следующие вопросы нет:

- Как можно оценить подверженность организации риску, особенно серийным рискам, возникающим из-за взаимодействия инфраструктур различных организаций?
- Как можно оценить непрямые издержки, возникающие из-за недостатка безопасности, связанные, например, с ущербом репутации компании или шпионажем?
- Что может безопасность дать организации, реализующей ее?
- Какова экономическая ценность безопасности?
- Какова прибыль от вложений в безопасность?

Экономическую ценность безопасности нужно рассматривать в самом широком социальном смысле, учитывая влияние новых технологий на частных лиц, организации и страны. Экономическую ценность нельзя сократить до издержек на установку и техническое обслуживание.

I.2.8 Социальный аспект

Важно, чтобы все участники интернета осознали важность получения права на безопасность, и то, каковы основные шаги, которые повысят уровень безопасности, при условии того, что они четко сформулированы, определены и разумно реализуются.

Для того чтобы все компьютерные пользователи вошли в процесс безопасности и образовалось ответственное информационное общество, необходимы информационные кампании и обучение гражданского населения.

Следует подчеркивать важность безопасности, ответственности каждого человека и мер по предотвращению, а также потенциальную причастность к преступлению за несоблюдение требований безопасности. В общем, также необходимо проводить обучение в области информационно-коммуникационных технологий, а не просто безопасности и мер предотвращения. Осведомленность в вопросах безопасности не должна ограничиваться продвижением определенной культуры безопасности. Культура безопасности должна входить в культуру IT, возможно в форме лицензии пользователя компьютера, рекомендуемой CIGREF (*Club Informatique des Grandes Entreprises Françaises*), ассоциации крупных корпораций Франции для решения вопросов IT[7].

[7] www.cigref.fr

Интернет следует превратить в общественное достояние, открытое для всех так, чтобы киберграждане могли потенциально получить выгоду от инфраструктур и услуг, имеющихся в их распоряжении, не беря на себя чрезмерных рисков безопасности. Кодекс этики безопасности необходимо разработать, принять и сделать так, чтобы все участники киберпространства уважали его.

I.2.9 Юридический аспект

I.2.9.1 Решающий фактор успеха

Некоторые национальные правовые нормы и международные конвенции юридически обязывают организации применять меры безопасности. В результате, менеджеры организаций и, на основании передачи прав и ответственности, их администраторы по безопасности несут обязательства, касающиеся мер безопасности (однако они не несут обязательств в отношении результатов). Юридическое лицо виновное в сбое безопасности может нести уголовную, гражданскую и административную ответственность. Существует ли такая ответственность или нет, конечно, не повлияет на уголовную ответственность частных лиц виновных в нарушении.

Соответствующее законодательство в области обработки данных дает возможность укрепить доверие между экономическими партнерами в инфраструктуре внутри страны, способствуя экономическому развитию страны. Таким образом, помогая создать благоприятное окружение для обмена данными на основе соблюдения закона, они являются движущей силой принятия услуг, основанных на информации и коммуникации, широкой общественностью. Законодательство и безопасность можно рассматривать как два уровня национальной экономики. Кибербезопасность, рассматриваемая в аспекте доверия и качества, закладывает основы развития здоровой системы услуг.

I.2.9.2 Укрепление законодательства и применения права

Как стало ясно из изучения статистических данных за год, предоставленных Институтом кибербезопасности (CSI)[8] или командой Скорой компьютерной помощи (CERT)[9], в настоящее время киберпреступность не контролируется должным образом. Таким образом, можно наблюдать как меры безопасности, реализуемые организациями, обеспечивают безопасность данного окружения в определенном контексте, но не могут предотвратить преступную деятельность через интернет. Причины такого положения дел связаны, в частности, с:

- природой киберпреступности (автоматизация, интеллектуальные злонамеренные программы, удаленное активирование);
- легкостью и безнаказанностью, с которой хакеры могут захватывать идентификационную информацию законных пользователей, таким образом, мешая юридической системе определить исполнителей преступного деяния;
- необходимостью решать вопросы компетенции до того, как проводить расследование;
- недостатком человеческих и материальных ресурсов для работы по борьбе с киберпреступностью;
- транснациональной природой киберпреступности, что делает необходимым частые призывы к международному содействию и судебному сотрудничеству, вызывая задержки, которые не соответствуют скорости преступников и потребностям атакованных IT систем в немедленном возобновлении работы;
- отсутствием соответствующих категорий в некоторых правоохранительных органах;
- неподходящим определением и временным характером большинства улик, связанных с IT.

[8] www.gocsi.com

[9] www.cert.org

По всем этим причинам законодательная система остается неэффективной в отношении интернета. Более того, также как есть налоговые укрытия, есть и законные убежища для компьютерных преступников. Распространение преступлений, связанных с компьютером не обязательно является признаком того, что законов недостаточно. Существующие законы уже охватывают многие виды деятельности преступников и хакеров IT.

Что является незаконным вне интернета, также незаконно и в интернете

Для дополнения многих существующих законов, которые, конечно, также применяются и в киберпространстве, необходимо новое законодательство, появление которого объясняется необходимостью определить подходящую законодательную структуру, адаптированную к использованию новых технологий.

Недостаточно укрепить законодательство, если нет средств его применения. Закон бесполезен, если правоохранительные органы не способны собрать и проанализировать улики, обнаружить и преследовать преступников. Если хакеры уверены, что они избегут наказания, это доказательство того, что закон неэффективен.

I.2.9.3 Борьба с киберпреступностью при уважении цифровой приватности: сложный компромисс

Средства, необходимые для борьбы с растущей международной киберпреступностью, требуют законодательной базы, согласованной на международном уровне, которую можно эффективно применять, а также средств для настоящего международного сотрудничества на уровне правоохранительных органов и органов правосудия.

Правительства стран несут большую ответственность за гарантирование кибербезопасности. Это особенно касается определения подходящей универсальной законодательной базы для развития культуры безопасности, которая будет уважать права частных лиц на цифровую приватность, при одновременном усилении борьбы с киберпреступностью.

Основной целью борьбы с киберпреступностью является защита частных лиц, организаций и стран при соблюдении основных принципов демократии.

Инструменты, используемые в борьбе против киберпреступности, потенциально враждебны по отношению к правам человека и могут разрушить тайну частной информации. Безопасность требует надзора, контроля и профилирования. Если необходимо предотвратить превышение служебных полномочий, противостоять соблазну применить тоталитарные методы и соблюсти гарантированные права, включая право на киберприватность и защиту конфиденциальной персональной информации, проверки и сопоставления очень важны.

В добавление к Европейской директиве 1995 года в течение нескольких лет в различных странах были приняты другие законы о защите личной информации:

Германия:	Закон от 21 января 1977 г.
Аргентина:	Закон о защите личной информации, 1996 г.
Австрия:	Закон от 18 октября 1978 г.
Австралия:	Закон о защите частной жизни, 1978 г.
Бельгия:	Закон от 8 декабря 1992 г.
Канада:	Закон о защите частной информации, 1982 г.
Дания:	Закон от 8 июня 1978 г.
Испания:	Закон от 29 октября 1992 г.
США:	Закон о защите индивидуальных свобод, 1974 г.; Закон о базах данных личной информации, 1988 г.
Финляндия:	Закон от 30 апреля 1987 г.
Франция:	Закон об информационной технологии и свободе от 6 января 1978 г., в 2004 году внесены поправки
Греция:	Закон от 26 марта 1997 г.
Венгрия:	Закон о защите личной информации и передаче общественной информации, 1992 г.

Ирландия:	Закон от 13 июля 1988 г.
Исландия:	Закон о записи личной информации, 1981 г.
Израиль:	Закон о защите частной жизни, 1981 г., 1985 г., 1996 г.; Закон о защите информации при администрировании, 1986 г.
Италия:	Закон от 31 декабря 1996 г.
Япония:	Закон о защите компьютеризированной личной информации, 1988 г.
Люксембург:	Закон от 31 марта 1979 г.
Норвегия:	Закон о личных записях данных, 1978 г.
Новая Зеландия:	Закон об официальной информации, 1982 г.
Нидерланды:	Закон от 28 декабря 1988 г.
Польша:	Закон о защите личной информации, 1997 г.
Португалия:	Закон от 29 апреля 1991 г.
Чехия:	Закон о защите личной информации в компьютеризированных системах, 1995 г.
Великобритания:	Закон от 12 июля 1988 г.
Россия:	Федеральный закон об информации, информатизации и защите информации
Словения:	Закон о защите информации, 1990 г.
Швеция:	11 мая 1973 г.
Швейцария:	Федеральный закон о защите информации, 1992 г.
Тайвань:	Закон о защите информации, 1995 г.

I.2.9.4 Международное законодательство по киберпреступности

Первым международным соглашением, рассматривающим международный характер киберпреступности, была "Конвенция о киберпреступности"[10] Совета Европы, принятая в Брюсселе 23 ноября 2001 года, вступившая в силу в июле 2004 года (после ратификации ее пятью из подписавших государств, не менее трех из которых должны были быть из Совета Европы). Данная конвенция содержит следующие пункты.

- Независимое уголовное право:
  - преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;
  - преступления с использованием компьютера;
  - преступления, связанные с нарушением авторского права и смежных прав.
- Процессуальное право:
  - быстрое сохранение компьютерных данных и данных трафика и быстрое раскрытие последних компетентным органам;
  - сохранение и поддержание целостности компьютерных данных на период времени, необходимый для того, чтобы дать возможность компетентным органам потребовать их раскрытия;
  - порядок представления;
  - поиск и захват хранимых компьютерных данных;
  - сбор компьютерных данных в режиме реального времени;
  - соответствующая защита прав и свобод человека.
- Каждое государство должно предпринимать необходимые юридические и другие меры для установления юрисдикций над следующими преступлениями, не ущемляя законов, действующих внутри страны:
  - намеренно выполненный доступ ко всей компьютерной системе или ее части лицом, не имеющим на то права;

[10] www.conventions.coe.int/Treaty/FR/Treaties/Html/185.htm

- намеренно совершенный перехват необщедоступной передачи данных из компьютерной системы или в нее лицом, не имеющим на то права;
- намеренно нанесенный ущерб, удаление, повреждение, изменение или утаивание компьютерных данных лицом, не имеющим на то права;
- намеренное серьезное нарушение работы системы лицом, не имеющим на то права;
- производство, продажа, приобретение для использования, импорт, распределение или другое распространение устройства, разработанного или приспособленного для совершения любого из данных преступлений;
- намеренный ввод, изменение, удаление или утаивание компьютерных данных приводящее к появлению неаутентичных данных с намерением использовать их для законных целей, как если бы они были аутентичными лицом, не имеющим на то права;
- намеренный ввод, изменение, удаление или утаивание компьютерных данных или любое вмешательство в работу компьютерной системы, вызывающее потерю собственности другого лица, с мошенническим или нечестным намерением получить экономическую прибыль для себя или другого лица лицом, не имеющим на то права;
- считать уголовным преступлением помощь или соучастие любому из данных преступлений, а также любую попытку совершить любое из данных преступлений.

– Каждая из стран, подписавших данную конвенцию, должна установить юрисдикцию над любым преступлением, совершенным:
  - на своей территории;
  - на борту корабля, несущего флаг данной страны;
  - одним из ее граждан, если преступление уголовно наказуемо там, где оно было совершено, или если преступление совершено вне территориальной юрисдикции любого государства.
– Правила международного сотрудничества, касающиеся:
  - экстрадиции;
  - взаимопомощи при расследовании;
  - процедур для преступлений, относящихся к компьютерным системам и данным;
  - сбора электронных улик преступления.
– Создание сети взаимопомощи:
  - доступной 24 часа в сутки, 7 дней в неделю;
  - с национальной точкой взаимодействия;
  - оказывающей немедленную помощь при расследовании преступлений.

На международном уровне существует политическая воля для борьбы с киберпреступностью. Проблема не всегда состоит в отсутствии законов или директив, таких, например, как директивы, опубликованные Организацией экономического сотрудничества и развития (OECD) в "Директивы OECD для безопасности информационных систем и сетей – К культуре безопасности – 2002[11]" (рисунок I.7). Скорее, проблема состоит в сложности и запутанности данной задачи и в ресурсах, необходимых для достижения целей в борьбе не только против киберпреступности, но и против организованной преступности, что приводит к тому, что интернет используют для целей злоумышленников.

[11] www.oecd.org/dataoecd/16/22/15582260.pdf – См. Приложение F данного Руководства.

Рисунок I.7 – Принципы информационной безопасности OECD (июль 2002 г.)

Осведомленность	Все участники несут ответственность за безопасность информационных систем и сетей
Ответственность	Все вовлеченные обладают частью безопасности систем и информационных сетей
Реакция	Участникам следует действовать своевременно и сообща для предотвращения, обнаружения и реагирования на случаи нарушения безопасности
Этика	Участникам следует уважать законные интересы других
Демократия	Безопасность информационных систем и сетей должна быть совместима с важными ценностями демократического общества
Оценка риска	Участникам следует проводить оценку риска
Разработка и реализация безопасности	Участникам следует считать безопасность важным элементом информационных систем и сетей
Управление безопасностью	Участникам следует придерживаться всеобъемлющего подхода к управлению безопасностью
Повторная оценка	Участникам следует пересматривать и повторно оценивать безопасность информационных систем и сетей и вносить соответствующие изменения в политику, практику, меры и процедуры безопасности

I.2.10 Основы кибербезопасности

Решения по безопасности должны способствовать удовлетворению основным критериям безопасности таким, как доступность, целостность и конфиденциальность (критерии AIC – availability, integrity и confidentiality). Другими критериями, на которые часто ссылаются в данном контексте являются аутентификация (которая дает возможность проверить идентификационную информацию объекта), неотказуемость и приписываемость (которые дают возможность проверить, что действия или события имели место) (см. рисунок I.8).

I.2.10.1 Готовность

Для гарантирования готовности услуг, систем и данных компоненты систем инфраструктур должны иметь подходящий размер и обладать необходимой избыточностью, кроме того, должны быть обеспечены ресурсы и услуги по оперативному управлению.

Готовность измеряется за период, в течение которого действует предоставляемая услуга. Потенциальный объем работы, который можно выполнить за период готовности услуги, определяет емкость ресурса (например, сети или сервера). Готовность ресурса тесно связана с его доступностью.

I.2.10.2 Целостность

Сохранение целостности данных, обработки или услуг подразумевает защиту их от случайного или намеренного изменения, порчи и уничтожения. Целостность необходима для гарантии того, что они остаются верными и надежными.

Для предотвращения преступного использования необходимо подтвердить, что они не были изменены во время хранения или передачи.

Целостность данных можно гарантировать, только если данные защищены от активных методов перехвата, которые могут быть использованы для изменения перехваченной информации. Данный тип защиты можно обеспечить при помощи таких механизмов безопасности, как:

– строгий контроль доступа;

– шифрование данных;

– защита от вирусов, "червей" и "Троянских коней".

Рисунок I.8 – Основы кибербезопасности

Система должна…	Цели безопасности	Инструменты безопасности
...иметь возможность для использования	• готовность • устойчивость • непрерывность • доверие	• определение характеристик • избыточность • операционные и резервные процедуры
...правильно работать	• безопасность работы • надежность • устойчивость • непрерывность • правильность	• разработка • производительность • эргономика • качество услуг • операционная поддержка
...предоставлять доступ авторизованным объектам (отклоняя попытки выполнения неавторизированного доступа)	• конфиденциальность (секретность) • целостность (без изменений)	• контроль доступа • аутентификация • контроль ошибок • проверка на непротиворечивость • шифрование
...проверять действия	• неотказуемость • аутентичность (без сомнений) • неоспоримость	• сертификация • регистрация, трассируемость • электронная подпись • механизмы доказательства

I.2.10.3 Конфиденциальность

Конфиденциальность – это охрана секретности информации, информационных потоков, транзакций, услуг или действий, осуществляемых в киберпространстве.

Конфиденциальность нужно реализовывать путем проверки доступа и шифрования.

Шифрование помогает защитить конфиденциальность информации во время передачи или хранения путем преобразования ее в форму, непонятную тому, кто не обладает средствами для ее расшифровки.

I.2.10.4 Идентификация и аутентификация

Цель аутентификации – устранить любую неясность в отношении подлинности ресурса. Аутентификация предполагает, что все объекты (аппаратное и программное обеспечение и люди) правильно идентифицированы и что определенные характеристики могут служить доказательством их идентификации. В частности, системы контроля доступа к ресурсам IT на основе логики требуют, чтобы проводилась идентификация и аутентификация объектов.

Процедуры идентификации и аутентификации реализуются для достижения следующего:

- конфиденциальность и целостность данных (доступ к ресурсам возможен только для идентифицированных аутентифицированных пользователей, и ресурсы защищены от изменений, которые не может вносить никто, кроме тех, кто имеет авторизацию);
- неотказуемость и вменение в вину (можно проследить действия идентифицированного и аутентифицированного объекта), трассируемость сообщений и транзакций (можно проследить передачу информации идентифицированного и аутентифицированного объекта), подтверждение адресата информации (можно доказать, что сообщение адресовано идентифицированному и аутентифицированному объекту).

I.2.10.5 Неотказуемость

В некоторых обстоятельствах необходимо выяснить, имело ли место событие или транзакция. Неотказуемость связана с понятиями отслеживаемости, вменения в вину, трассируемости и, в некоторых случаях, возможности проведения проверки (проверяемости).

Создание ответственности предполагает существование механизмов аутентификации частных лиц и приписывания им действий. Возможность записи информации, дающей возможность проследить выполнение действия, становится важной, когда нужно восстановить последовательность событий, особенно при компьютерном поиске адреса системы, использованной для передачи данных, например. Нужно сохранять информацию, необходимую для проведения последующего анализа, для проверки системы (регистрация информации). Это называется проверяемостью системы.

I.2.10.6 Физическая безопасность

Пространства, в которых расположены рабочие станции, серверы, участки IT и услуги (кондиционирование воздуха, щиты электропитания и т. д.), необходимо физически защищать от несанкционированного доступа и аварий (пожар, повреждение водой и т. д.). Физическая безопасность является самым основным типом управления системами IT.

I.2.10.7 Решения по вопросам безопасности

В контексте повседневной реальности проблем, связанных с безопасностью большинства инфраструктур, распространения предлагаемых решений и процветания рынка безопасности, возникает несколько вопросов:

- Соответствуют ли предлагаемые решения требованиям?
- Правильно ли их устанавливают и управляют ими?
- Можно ли их использовать или адаптировать к динамически меняющемуся окружению?
- Могут ли они уменьшить чрезмерную концентрацию власти в руках системного администратора?
- Как их можно использовать для решения проблем безопасности, возникающих из-за невнимательности, ошибки человека, конструктивной недоработки, проблем при установке или неправильного управления технологическими решениями и решениями безопасности?
- И т. д.

ЧАСТЬ II

Контроль киберпреступности

Раздел II.1 – Киберпреступность

II.1.1 Преступления с использованием компьютера и киберпреступность

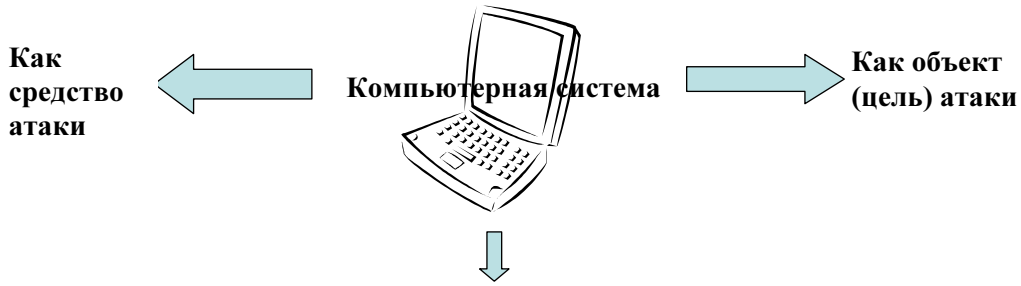
Комбинация уязвимых мест цифровых технологий и недостаточного их контроля создает небезопасное окружение. Преступники, естественно, пользуются данным положением дел. Преступники потенциально могут использовать для незаконных целей любую технологию; интернет не является исключением, что широко демонстрирует присутствие криминала в киберпространстве.

В 1983 году Организация экономического сотрудничества и развития определила преступление с использованием компьютера как любое незаконное, неэтичное или несанкционированное действие, включающее в себя передачу или автоматическую обработку данных.

Преступление с использованием компьютера – это такое преступление, в котором компьютерная система является объектом преступления, средством совершения преступления, или и тем и другим; это преступление, связанное с цифровой технологией, подмножество преступлений "белых воротничков". Киберпреступление – это форма преступлений с использованием компьютера, совершенных с использованием технологии интернет; киберпреступность охватывает все преступления, совершенные в киберпространстве.

В виртуальном мире преступление может быть автоматизировано, что создает потенциальную угрозу широкомасштабной компьютерной эпидемии, которую можно спровоцировать в удаленном режиме через сеть (что освобождает преступника от ограничений во времени и пространстве) с возможностью задержанного действия (рисунок II.1).

Рисунок II.1 – Природа преступлений с использованием компьютера



- Преступление "белых воротничков"
- Преступления, совершаемые в удаленном режиме через сеть, экранная анонимность Преступник свободен от ограничений во времени и пространстве
- Преступные "ноу-хау", внедренные в программное обеспечение
- Автоматизированные преступления в большом масштабе

Интернет технологии делают возможными большую часть нарушений: кража, информационный саботаж, нарушения авторского права, нарушение профессионального доверия, цифровой приватности, интеллектуальной собственности, распространение нелегального контента, атаки против конкурентов, промышленный шпионаж, посягательства на торговую марку, дезинформация, отказ в обслуживании, различные формы мошенничества и т. д.

Заметными событиями, повлиявшими на рост осведомленности об угрозе киберпреступности, – помимо проблемы двухтысячного года, которая привлекла внимание к уязвимости программного обеспечения и зависимости от компьютеров, – были атаки типа "отказ в обслуживании", как, например, предпринятые против Yahoo (10 февраля 2000 г.), и атака печально известного вируса "I love you" (4 мая 2000 г.). С тех пор освещение в СМИ атак вирусов (таких, как вирус "Code red" в июле 2001 г. или "Nimda" в сентябре 2001 г.) и атак типа "отказ в обслуживании" (такие, как атаки, предпринятые против сети DNS 21 октября 2002 г.), и многих других примеров усилило общую осведомленность общественности о реальности угроз, действующих через интернет. Новостные СМИ продолжают уделять большое внимание проблемам, относящимся к компьютерам.

II.1.2 Факторы, делающие интернет привлекательным для преступных элементов

II.1.2.1 Виртуализация и виртуальный мир

Отделение транзакций от физических носителей (виртуализация), инструменты связи, включающие в себя шифрование, стенографию и анонимность: вот факторы, которыми пользуются преступники в различных странах для сотрудничества без необходимости физических встреч, действуя гибким и защищенным образом совершенно безнаказанно. Они могут образовывать команды, планировать преступления и осуществлять их как традиционным образом, так и с использованием новых технологий. Глобальная доступность интернета позволяет преступникам действовать в глобальном масштабе очень быстро.

Эти значительные возможности, предоставляемые цифровым миром и электросвязью, являются одними из наиболее характерных проблем, связанных с разработкой, реализацией, управлением и контролем информационной технологии, с их аварийными отказами, неисправностями, ошибками и человеческими ошибками и даже стихийными бедствиями, а также взаимозависимостью инфраструктур, которые по определению подразумевают определенный уровень ненадежности в цифровых инфраструктурах.

Таким образом, потенциальные возможности для злонамеренного использования уязвимых мест очень велики, что на практике выливается в:

> кражу идентификационной информации, получение доступа обманным путем, несанкционированный доступ, мошенническое использование ресурсов, инфицирование, саботаж, разрушение, порчу, нарушение конфиденциальности, похищение данных, шантаж, вымогательство, рэкет, отказ в обслуживании и т. д.

Данное обстоятельство показывает неадекватность контроля рисков преступного происхождения, связанных с компьютером, которым подвергаются организации, и текущие стратегии безопасности.

Киберпространство, позволяющее пользователям работать в удаленном режиме через сеть, скрытую за экраном, создает идеальные условия для преступной деятельности. На самом деле, некоторые люди могут зайти за пределы дозволенного, не полностью осознавая криминальную природу своих действий.

II.1.2.2 Объединение ресурсов в сеть

Широкое взаимодействие компьютерных и информационных ресурсов через сеть делает их привлекательными объектами для экономической преступности, использующей новые технологии. Общей чертой различных форм компьютерных атак является относительно низкий риск для преступника по сравнению с потенциальной угрозой вреда и ущерба, значительно превышающего ресурсы, необходимые для осуществления атаки. Электронное похищение идентификационных данных, легко достижимая анонимность и возможности для осуществления контроля над компьютерами облегчает выполнение незаконных действий без какого-либо риска.

II.1.2.3 Распространение взломанных программ и информации об уязвимых местах

Широкая доступность так называемых "взломанных программ", использующих уязвимые места системы, а также библиотеки описаний атак и программное обеспечение, составляющие секреты преступников, облегчают выполнение компьютерной атаки. Это обстоятельство в комбинации с возможностью виртуальных действий поощряет компьютерных исследователей с преступными наклонностями и преступников с компьютерными знаниями использовать свой опыт со злым умыслом. В некоторых случаях, киберпространство способствует незаметному переходу к преступлению.

II.1.2.4 Ошибки и уязвимые места

Преступники используют организационные и технические ошибки и уязвимые места интернета, отсутствие согласованной законодательной структуры среди стран и недостаток эффективного координирования между правоохранительными органами стран. Это может включать в себя традиционные формы преступности (традиционные преступления, совершаемые при помощи новых технологий: отмывание денег, шантаж, вымогательство и т. д.) или новые типы преступности, основанные на цифровых технологиях: вторжение в систему, похищение времени процессора, похищение кодов источника, баз данных и т. д. Во всех этих случаях окружение чрезвычайно благоприятно: минимум рисков, широкий охват, большая прибыль.

На рисунке II.2 обобщаются источники уязвимых мест инфраструктуры интернет.

Рисунок II.2 – Основные характеристики интернета, используемого в преступных целях

II.1.2.5 Разоблачение киберпреступников

Преступление с использованием компьютера запутанно, оно обычно совершается по ту сторону границы страны, часто с задержкой времени. Следы, которые оно оставляет в системах, нематериальны, и их трудно собрать и сохранить. Они принимают вид цифровой информации, хранимой на всех видах средств информации: ОЗУ, периферия, жесткие диски, внешние диски, USB карты, электронные компоненты и т. д. Проблема состоит в том, как собрать разнообразные улики, найденные в ходе цифрового поиска. Следующие примеры иллюстрируют степень, в которой понятие цифровой улики остается неуловимым:

- Как идентифицировать текущие данные?
- Как отслеживать их?
- Как их хранить?
- Каковы юридические правила доказательств?
- Как восстановить факты, которые уже были расследованы?
- Как установить происхождение сообщения?
- Как установить личность человека на основании только цифровых признаков, учитывая трудность надежного сопоставления цифровой информации и ее физического автора (виртуализация) и распространение похищения идентификационной информации?
- Как установить неопровержимость цифровой улики при выяснении истины в суде (понятие цифровой улики), учитывая, что носители данных, с которых получены данные улики, не являются безошибочными (информация о дате и времени меняется от одной компьютерной системы к другой, и ее можно изменить)?
- И т. д.

Получить цифровые улики еще сложнее, если они разбросаны по системам, расположенным в разных странах. В таких случаях, успех полностью зависит от эффективности международного сотрудничества между законодательными органами и от скорости, с которой предпринимаются действия. Эффективность использования таких улик для идентификации частных лиц зависит от скорости, с которой обрабатываются запросы: если скорость обработки невелика, идентификация практически невозможна.

На рисунке II.3 показаны различные типы проблем, вызванных злонамеренными действиями такими, как физическое разрушение или кража оборудования, блокирование доступа к системам и данным, инфицирование ресурсов, принятие рискованных решений или процессы связи посредством атак типа "отказ в обслуживании" (или в результате шпионажа или вторжения в системы), похищение фальсификация информации (управление мнением, информационная война). На рисунке также в общих чертах намечаются основные характеристики киберпреступности, которые затрудняют установление личности преступников.

Кроме того, в большинстве стран существует значительный разрыв между умениями преступников, совершающих высокотехнологичные преступления, и ресурсами, имеющимися в распоряжении правоохранительных органов и органов правосудия, преследующих преступников. Использование компьютерных технологий этими органами, как на уровне страны, так и на международном уровне, остается слабым и значительно меняется от страны к стране.

В большинстве случаев при преследовании, обнаружении и аресте киберпреступников полиция и органы правосудия полагаются на традиционные методы расследования, используемые для обычных преступлений.

Рисунок II.3 – Трудности определения личности атакующего

II.1.2.6 Нетерриториальность, цифровые укрытия

Преступники пользуются нетерриториальным характером интернета и недостатком в некоторых странах законов, объявляющих преступления с использованием компьютера незаконными, а также множества юрисдикций, охватывающих интернет.

Подобно укрытиям от налогов, цифровые укрытия позволяют преступникам размещать сервера, распространять нелегальную информацию, осуществлять незаконную деятельность без страха быть наказанными. Установка таких серверов на территории слабых стран создает укрытие для осуществления трансграничных операций.

Недостаток международного регулирования и контроля и неэффективность международного сотрудничества в законных расследованиях и судебных преследованиях позволяют интернету выступать в качестве защитного буфера для преступников.

В настоящее время не существует эффективного законодательного или технического подхода к борьбе со всеми разнообразными типами преступлений, наблюдаемыми в интернете такими, как:

- хорошо организованное параллельное крупномасштабное производство программного обеспечения, контрафакция фильмов и музыки, принявшее в киберпространстве беспрецедентные масштабы;
- нарушения авторского права, злоупотребление профессиональным доверием, нарушение цифровой приватности и интеллектуальной собственности;
- имущественные преступления, кража, нанесение ущерба имуществу или разрушение его и вмешательство в чью-либо собственность (понятие электронного посягательства);
- распространение нелегальной информации;
- атаки против конкурентов, промышленный шпионаж, посягательства на торговую марку, дезинформация, атаки типа "отказ в обслуживании" направленные на конкурентов.

II.1.3 Традиционные преступления и киберпреступность

Киберпреступность является естественным продолжением обычной преступной деятельности. Сегодня преступления совершаются через киберпространство с использованием нетрадиционных средств так, что они дополняют обычное преступление.

Интернет создает не только идеальные условия для новой незаконной деятельности и проектов, но и различные варианты мошенничества и других преступлений, совершаемых при помощи компьютера.

Интернет облегчает поиск и использование новых способов получения денег. Это свойство, естественно, не проходит незамеченным мимо криминального мира. Используя IT, преступники надеются увеличить прибыль с минимальным риском.

II.1.4 Киберпреступность, экономическая преступность и отмывание денег

Экономическая преступность посредством интернета не ограничивается организованной преступностью. Современные информационно-коммуникационные технологии позволяют отдельным личностям совершать экономические преступления, работая либо поодиночке, либо в группах различной численности, создаваемых для конкретной цели.

Преступники могут организоваться на базе обмена информацией, благодаря использованию IT. Сети могут объединить людей и опыт для организации виртуальной преступной банды.

Учитывая, что экономическое преступление требует высокой квалификации и навыков в области экономики, очевидно, что это следующий кандидат на "совершенствование" средствами современных IT.

Интернет способствует получению информации и знаний о рынках, законах, технологии и т. д., необходимых для совершения экономических преступлений. Его также можно использовать для поиска жертв.

На экономические преступления оказывают влияние новые технологии, ставшие частью репертуара преступников и предоставляющие информацию для стратегий и процессов принятия решений.

Новые технологии могут облегчить кражу любого рода, фальсификацию, информационный саботаж и мошенничество. Шантаж, вымогательство, рэкет и требование выкупа перешли в интернет.

Информационные ресурсы, в сущности, стали потенциальными заложниками киберпреступников. Шантажисты перенесли свои действия в киберпространство, и теперь любой может вдруг оказаться жертвой попытки шантажа, дезинформации или пропаганды. Кроме того, резкое увеличение похищений идентификационной информации с 2003 года показывает, что преступники пользуются анонимностью, которую дает интернет. Преступники используют поддельную идентификационную информацию для ухода от судебного преследования, ответственности за преступления и террористические акты. Похищение идентификационной информации, легко осуществляемое через интернет, является одним из факторов противозаконной деятельности.

Как и все преступники, использующие существующие технические инфраструктуры, люди, занимающиеся отмыванием денег, используют интернет для придания деньгам, полученным от преступной деятельности такой, как контрабанда наркотиков и оружия, коррупция, проституция, жестокое обращение с детьми, уклонение от налогов и т. д., легального статуса.

Хотя отмывание денег через интернет часто незаметно и о нем скорее умалчивают, оно становится все более популярным. Благодаря своему виртуальному характеру (анонимность, киберпространство, скорость перевода) и свободе от территориальных ограничений (международный характер, противоречащие друг другу обеспечение и юрисдикции), интернет стал идеальным средством, которое научились использовать отмыватели денег. Интернет позволяет направлять денежные суммы криминального происхождения в законные экономические циклы, используя перевод денег, инвестиции и капитализацию.

Электронные инвестиции, азартные игры и торговля такая, как продажа воображаемых товаров и услуг за настоящие деньги, позволяют получать, казалось бы, законный доход, который трудно отследить и почти невозможно подвергнуть судебному преследованию. Банковские услуги, оказываемые через интернет, операции с недвижимостью, использование виртуальных подставных компаний и электронных денег могут использоваться для придания видимости легальности

преступной деятельности. Коммерческие организации могут быть невольно вовлечены со всеми – потенциально разрушительными – вытекающими отсюда последствиями юридического и коммерческого плана. Это основной источник рисков для компаний.

В настоящее время существует несколько эффективных способов управления явлением отмывания денег через интернет.

II.1.5 Киберпреступность – продолжение обычной преступности

Киберпреступность чаще всего принимает форму обычной преступности, по большей части невидимой, но, тем не менее, очень могущественной вследствие объединения ресурсов и людей в сеть. Не только компании, но и их IT и информационное имущество, могут привлечь преступные организации, ищущие прибыль. Это является стратегической угрозой, поскольку деньги находятся в информационных системах, корпорациях, пенсионных фондах и т. д., а не просто в банках.

При открытии общего выхода в интернет-серверы, порталы и адреса электронной почты, компании рискуют привлечь внимание преступников и дать им потенциальную точку опоры. Хотя интернет – это мощное средство связи, это также и хаотичная, сложная, динамически развивающаяся и враждебная среда, которую можно использовать для подрыва деятельности организации и совершения преступления. К интернету следует относиться с осторожностью, как к особо опасной зоне. При условии того, что организации придают большое значение своему присутствию в интернете, они, по всей вероятности, способствуют распространению преступности в интернете.

В наши дни национальная безопасность сталкивается с проблемами в виде угрозы преступлений, связанных с IT. Технологии интернета находятся в самом сердце понятия информационной войны, преследующей в основном экономические цели; эти технологии могут оказать огромное влияние на проведение деловых операций. Интернет не только позволяет манипулировать информацией, он также является идеальным средством распространения слухов, которое можно использовать для инициации кампаний по распространению дезинформации или неуверенности. Интернет также облегчает шпионаж и другие виды деятельности по сбору сведений, учитывая то, с какой легкостью может быть перехвачена информация, передаваемая через интернет.

II.1.6 Киберпреступность и терроризм

Киберпреступность может приобретать террористический характер, когда системы-жертвы являются частью важной инфраструктуры. Уязвимость важных инфраструктур страны (энергетика, водоснабжение, транспорт, снабжение продуктами питания, электросвязь, банковское дело и финансы, медицинские услуги, правительственные функции и т. д.) увеличивается по мере того, как увеличивается использование интернет-технологий.

Особое внимание следует уделять системам производства и распределения электроэнергии, которые необходимы для работы большинства инфраструктур. Одной из ключевых целей компьютерных террористов является контроль над элементами важных инфраструктур, на что указывает увеличение количества исследований (поиск уязвимых мест, которые можно использовать для проникновения в систему в будущем), целью которых были компьютеры операторов инфраструктур.

Согласованного определения того, что считать компьютерным терроризмом в настоящее время не существует. Согласно самому простому определению, это терроризм, применяемый в киберпространстве. В свою очередь, терроризм обычно понимают как систематическое проявление насилия для достижения политических целей.

Совершенно законно задаваться вопросом, не создаст ли выход из строя интернета или его части в результате злонамеренных действий страх в обществе пользователей интернета, некоторых групп участников экономики и широкой общественности.

Или, по большей части, мы можем сталкиваться с проявлениями экономического терроризма, направленного на нанесение ущерба организациям, использующим интернет в своей деятельности.

Термин "кибертерроризм", ставший популярным с памятного 11 сентября, следует использовать с осторожностью. Не следует забывать, что автором самой первой из широко обсуждавшихся в прессе атак типа "отказ в обслуживании" (DDOS) 10 мая 2000 года, был 15-летний подросток под псевдонимом "Mafia Boy". Юноша был обнаружен и арестован несколько месяцев спустя. Хотя причины данного поступка до сих пор не известны, мало вероятно, что они имели политический характер.

Если бы такая же атака произошла после событий 11 сентября, ее бы немедленно классифицировали как кибертерроризм.

При отсутствии конкретной информации, такой, как записка от атакующих или данные об их личности, очень трудно отнести какую-либо атаку к кибертерроризму.

Термин "кибертерроризм" охватывает довольно неопределенный список новых угроз, и сложно говорить о том, какова могла быть мотивация или цели неизвестного атакующего или группы атакующих. Когда известна только цель атаки, очень сомнительно предполагать мотивы хакера, террориста, наемника, активиста, обычного преступника или шутника.

Данный тип атаки с использование компьютера нельзя использовать для утверждения мотивации или целей атакующих с какой-либо степенью определенности. Это является одной из трудностей в борьбе против преступлений с использованием компьютера, поскольку для того, чтобы определить намерение преступника, требуется дополнительная информация.

Осуществляется ли кибертерроризм посредством процесса экономической дестабилизации или угрозы важным инфраструктурам, распространения идеологии или манипуляции информацией, он представляет собой новую угрозу, которую нужно воспринимать очень серьезно. Помимо угрозы информационным системам и кибермиру, символом которого является интернет, кибертерроризм может подвергнуть опасности жизнь людей путем создания прямой и непрямой угрозы жизни и здоровью.

II.1.7 Хакеры

Понимание мотивации хакера и уровня его подготовки может оказать помощь в оценке серьезности атаки и подготовке стратегии сопротивления. Для защиты информационных систем необходимо знать, против кого защищаться. В настоящее время существует две основные группы хакеров: профессионалы, зарабатывающие этим деньги, и любители, которые обычно являются людьми с ярко выраженной потребностью в признании (рисунок II.4).

Профессиональные хакеры обычно попадают в одну или более следующих категорий:

- непосредственные конкуренты организации-жертвы;
- государственные гражданские служащие;
- наемники (хакеры, которым платят организации в частном или государственном секторе);
- другие преступные элементы.

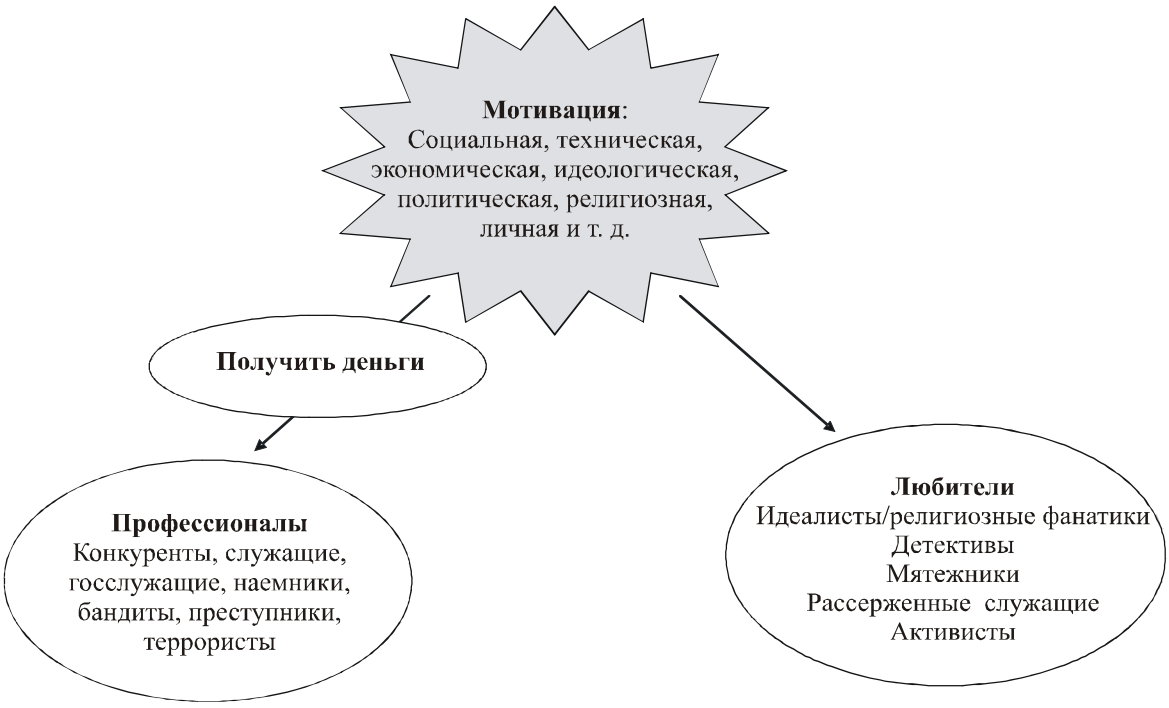
Хакеры-любители могут включать:

- специалистов, последователей первоначальных "хакеров", любителей компьютеров, основным желанием которых было продемонстрировать свое мастерство в области технологий;
- детективов;
- шутников, также называемых "скрипт-кидди" или "шутники-идиоты", которые часто получают большую известность, если их задерживают; не смотря на то, что их обнаруживают чаще всего, мы не должны думать, что они являются единственными представителями категории хакеров;

– людей с нарушенной психикой;

– активистов, работающих ради идеологической или религиозной цели (часто больше профессионалы, чем любители).

Рисунок II.4 – Две основные группы хакеров



Мотивация этих людей может быть связана с социальными, техническими, политическими, финансовыми факторами или с факторами, относящимися к правительству.

Социальным фактором обычно является потребность в одобрении другими людьми, часто это связано с членством в банде или группе. Эти хакеры хотят продемонстрировать свою значимость в группе, действуя согласно ее ценностям. Их преступления аналогичны действиям людей, рисующих граффити, и основываются на очень упрощенном видении социальной иерархии. Часто хакерством занимаются шутники, потому что это дает им чувство превосходства и контроля над учреждениями, которые доминируют над ними в обычной жизни.

Техническая мотивация встречается редко, основной целью ее является достижение пределов какой-либо технологии, демонстрация этих пределов и уязвимых мест и постижение сильных сторон.

Политическая мотивация концентрируется на событиях, которые вызовут интерес средств массовой информации и привлекут внимание к какой-либо серьезной проблеме. Если общественность будет осведомлена об этой проблеме, то данная проблема вскоре решится. Разграничение между хакерством по политическим мотивам и терроризмом может быть четким, по крайней мере, в теории. Социально-мотивированным людям не свойственно скрываться за политическими целями.

Финансовая мотивация может быть сильным фактором, она лежит в основе многих противоправных действий. Привлекательность легких денег заставляет преступников из "белых воротничков" (мошенников, растратчиков, недобросовестных конкурентов и т. д.) заниматься своей деятельностью в интернете.

И, наконец, последняя группа нашего списка включает в себя правительственные организации. Эта форма хакерства включает информационную войну и шпионаж, и осуществляется правительственными организациями, работающими на государство.

Преступники всех видов быстро адаптировались к веку компьютеров, добавив хакерство в свой актив. Они применяют пугающую находчивость, изобретая новые способы злонамеренного использования этой технологии.

II.1.8 Источники помех и злонамеренное программное обеспечение

II.1.8.1 Спам

Спам – это массовая рассылка незатребованных электронных сообщений в коммерческих или рекламных целях, для того чтобы убедить пользователей сети заказать тот или иной товар или услугу.

Спам остается значительной помехой, несмотря на огромные технические и финансовые ресурсы, которые поставщики услуг потратили на поиск способа его блокирования, несмотря на серьезное намерение органов государственной власти запретить спам, и несмотря на арест особенно злостных спаммеров в прошлом. В сентябре 2003 года спам составлял до 54 процентов от общего трафика электронных сообщений. В 2005 году число спам-сообщений в США превысило 12 миллиардов, т. е. 38,7 процентов всего трафика, согласно данным аналитической кампании IDC.

В худшем своем проявлении спам напоминает бомбардировку электронными сообщениями, что приводит к перегрузке почтовых серверов, переполнению почтовых ящиков пользователей и неудобству для обслуживающего персонала. Пользователи могут стать жертвой так называемой компоновки по списку, при которой их адрес добавляется в списки спаммеров без их согласия. Единственной альтернативой попытке извлечь свой адрес из таких списков, что может оказаться трудной задачей, является смена адреса электронной почты. Хотя эта мера является довольно эффективной, она также довольно разрушительна, поскольку от пользователя требуется уведомить лиц, с которыми ведется переписка, о смене адреса электронной почты.

Чрезмерное число незатребованных, неуместных и иногда шокирующих сообщений можно расценивать как вторжение в приватность пользователя, подобно "макулатурной" почте. Кроме того, спам все чаще стали использовать как средство передачи злонамеренных программ (злонамеренного программного обеспечения), что говорит о возрастании вредоносности спама.

II.1.8.2 Злонамеренное программное обеспечение

Основные организации, контролирующие безопасность IT (включая команду "скорой компьютерной помощи" (CERT)[12], Федеральное бюро расследований США (FBI) и французский *Clusif*), в своих ежегодных отчетах по киберпреступности отметили, что число злонамеренных или надоедающих программ, запускаемых на компьютерах без ведома их владельцев, возрастает.

Данные программы включают следующие виды программного обеспечения:

- программы загрузки, используемые для скачивания и установки данных и программ дистанционно;
- регистраторы ключей, контролирующие, какие ключи пользователь вводит в компьютер; существуют также аппаратные регистраторы ключей, невидимые на программном уровне, которые записывают такие данные;
- зомби, или "боты" (сокращение от "роботы"), программы, позволяющие дистанционно осуществлять контроль над системой для создания скрытой армии компьютеров. Каждый день обнаруживаются 25–50 новых ботов. Их используют для рассылки спама, мошеннических атак или для распространения бесплатных программных продуктов с размещенной в них рекламой. В октябре 2005 года полиция Нидерландов арестовала трех человек по подозрению в создании сети из 100 000 компьютеров-ботов для осуществления атак типа "отказ в обслуживании" и направленных на электронные счета PayPal и eBay своих жертв[13];

---

[12] www.cert.org – См. статистическую информацию за 1998–2005 годы на www.cert.org/stats/cert_stats.html.

[13] Источник: Отчет Clusif, *Panorama de la cybercriminalité, 2005*: www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k5-fr.pdf.

- бесплатные программные продукты с размещенной в них рекламой (рекламное программное обеспечение), используемое для специализации деловых операций;
- шпионящее программное обеспечение, которое, как ясно из названия, тайно записывает информацию. Согласно издателю программного обеспечения Webroot, в интернете существует более 100 000 различных типов шпионящего программного обеспечения и более 300 000 сайтов, на которых размещается такое программное обеспечение. На обычном персональном компьютере, имеющем выход в интернет, без ведома пользователя установлено в среднем 28 шпионских программ. На более 80 процентах компьютеров в компаниях установлена одна или несколько шпионских программ. Эти программы участвуют более чем в 70 процентах всех атак.

Кроме этих форм злонамеренного программного обеспечения, существуют вирусы и смежные продукты (черви, Троянские кони, логические бомбы).

Вирус состоит из злонамеренного кода, который устанавливается в систему без ведома пользователя и может копировать себя (в случае полиморфных вирусов, это скорее не копирование, а мутация). Вирус атакует среду-хозяина и заражает компьютеры, с которыми вступает в контакт. Вирусы можно классифицировать на основе их сигнатуры, характеристик, того, как они копируются и распространяются, типов злонамеренных функций, которые они запускают и т. д.

Целью компьютерного вируса, как и его биологического аналога, является воспроизводство и распространение. Вирус размножается, перемещается от компьютера к компьютеру, присоединяя свои копии к программам и, чаще всего, сообщениям электронной почты. Заражение вирусом обычно происходит при некотором действии со стороны пользователя. Ущерб, который вирус наносит целостности зараженных информационных ресурсов, может варьироваться от небольших неприятностей до большого разрушения, затрагивающего доступность и конфиденциальность системы.

Общий термин "вирус" используется для обозначения любой вредоносной программы (вызывающей инфицирование, разрушение, неправильное присвоение ресурсов и т. д.), обладающей способностью самовоспроизводиться и распространяться.

В 2005 году в ходу было около 50 000 новых вирусов[14]. Например, вирус HTML_NETSKY.P, согласно данным Всемирного центра отслеживания вирусов, с апреля 2004 года инфицировал 855 244 машин. Издержки инфицированных компаний составили порядка 42 миллионов долларов США, согласно данным Института кибербезопасности США. По данным сайта F-secure.com каждый день в мире появляется четыре тысячи новых вирусов.

Черви – это части компьютерного кода, также перемещающиеся через сеть, часто самостоятельно без всяких действий со стороны пользователя. Обычно черви создаются для ограничения ресурсов системы (памяти и пропускной способности), что подрывает доступность системы или делает возможным удаленный контроль над инфицированной системой.

Злонамеренные программы, известные как "Троянские кони", часто скрываются внутри обычных программ или справочных файлов, а затем просачиваются в системы, где они пытаются захватить контроль, для того чтобы красть время процессора, вмешиваться в данные или программы или разрушать их, вызывать аварии, выведывать информацию или проводить другие злоумышленные действия, или просто лежать, ожидая атаки в будущем.

Логические бомбы – это вирусы, активирующиеся при определенном событии (например, день рождения) и атакующие систему-хозяина.

Вирусы не следует путать с "ошибками" в компьютерных программах, которые являются ошибками программирования или, в целом, конструктивными недоработками, которые проявляются в виде функциональных проблем.

Обычно вирусы распространяются и начинают действовать, когда пользователь случайно активирует их, например, запустив инфицированную программу. В прошлом, большинство вирусов распространялось через приложения к сообщениям электронной почты и активировалось обычно при нажатии на пиктограмму файла.

---

[14] Источник: Отчет по компьютерным вирусам IPA/ISEC.

Многие злонамеренные программы маскируются под полезные дополнительные программы для навигации, соединения, настройки услуг и т. д., тогда как на самом деле они разработаны для осуществления надзора (похищение информации, пароля, контроль трафика), использования ресурсов компьютера или совершения атак. Они также используются для распространения и управления инструментами, используемыми для распределенных атак типа "отказ в обслуживании". Существуют тысячи таких программ, целью которых является финансовое обогащение.

Атаки типа "отказ в обслуживании" (DOS) и "распределенный отказ в обслуживании" (DDOS) направлены на выведение из строя ресурсов системы. Обычно они работают, перегружая сервер запросами обычных услуг, которые сервер должен обрабатывать автоматически, это мешает серверу предоставлять услуги обычным пользователям (отсюда термин "отказ в обслуживании"). Поскольку эти запросы напоминают обычные запросы, противостоять такой атаке очень тяжело (только объем запросов перегружает систему). Для большей эффективности, такую атаку могут начать одновременно с нескольких точек системы; это составляет распределенную атаку DOS.

Способы, при помощи которых распространяется злонамеренное программное обеспечение, включают в себя бесплатное или демонстрационное программное обеспечение и порнографические сайты или игры, электронную почту, а также спам и телеконференции.

Каковы бы ни были способы внедрения злонамеренного программного обеспечения – они могут даже включать, например, в случае бесплатных программных продуктов с размещенной в них рекламой (но никогда шпионского программного обеспечения), этап явного или подразумеваемого одобрения пользователем. Установленные однажды, они переходят в незаконное использование. Чаще всего они выполняются без согласия пользователя. Они тайно собирают и передают данные (например, предпочтения в интернете, представляющие интерес для последующей рекламы). Они могут выступать в качестве посредников для незаконной деятельности такой, как спам и мошеннические атаки, эффективно работая для получения лицом, их контролирующим, финансовой прибыли. Обнаружение и деинсталляция такого программного обеспечения не всегда является простым делом. Часто у пользователей не хватает умений и инструментов, необходимых для контроля этих рисков.

Термин фишинг (phishing) – это метафора для понятия "ловля рыбы", когда рыбак наматывает леску на катушку после того, как добыча привлечена наживкой и попалась на крючок – обозначает атаку, использующую почтовые программы, для того чтобы обманом или уговорами выманить у пользователей важную информацию, которую затем можно использовать в преступных целях (например, для мошенничества или хищения). В *Journal du net*[15] от 26 января 2005 года говорится о более 5 тысячах сайтов по мошенничеству такого рода, являвшихся активными в течение лишь одного месяца (сентябрь 2005 года), целью которых были 110 различных торговых марок.

В общем, фишинговые атаки осуществляются при помощи использования сообщений электронной почты, которые выглядят как сообщения, пришедшие от настоящих учреждений, с которыми у пользователя могут быть дела (например, почта, банк, торговец, сайт-аукцион в интернете), однако атакующие могут также использовать телефонный звонок, мгновенный обмен сообщениями (IM) или текстовые сообщения сотовых телефонов, или даже вступить в личный контакт с жертвой.

[15] www.journaldu net.com

II.1.8.3 Тенденции

В наши дни основной целью вирусов больше не является незаконное разрушение данных в больших масштабах. Теперь вирусы создаются для гораздо более сложной цели – зарабатывания денег. Из-за этого нового прагматического применения и внутренних характеристик вирусы могут использоваться для мошенничества. Таким образом, вирусы стали высокодоходными инструментами организованных преступников, участвующих в финансовых преступлениях.

Что касается спама и смежных источников помех, французский *Club de la sécurité des systèmes d'information français* (Clusif)[16] сообщил, что в 2003 году служба AOL отфильтровала 500 миллиардов спам-сообщений. А в декабре организация по борьбе со спамом Spamhaus[17] обнаружила, что самый активный спаммер рассылал 70 миллионов электронных сообщений в день!

Организация Clusif также сообщила, что в мае 2003 года США решением суда обязали так называемого спаммера Buffalo выплатить 16,4 миллиона долларов США поставщику услуг интернета Earthlink за рассылку 820 миллионов незатребованных сообщений. По данным Ferris Research в 2003 году спам стоил Европе 2,5 миллиарда долларов США, а США – 8,9 миллиардов. Если прибавить эти суммы к 500 миллионам долларов США, которые поставщики услуг вложили в блокирование спама, то станет ясна вся масштабность этой проблемы. Очевидно, что этот вопрос нельзя оставлять без внимания.

Кроме прямых издержек, возникающих в результате мошенничества, необходимо учитывать издержки, связанные с нарушением обслуживания и приводящие к нарушению операций, потере сбыта, сопутствующим убыткам, потере имиджа и репутации, и затраты по приведению систем в рабочее состояние. Все это создает значительные издержки для организаций, ставших жертвами компьютерных преступлений.

Наблюдения показывают, что число атак все время растет, и компьютерные вирусы стали настоящей эпидемией. Растет число операций по похищению идентификационной информации впечатляющих по уровню сложности, учащаются случаи мошенничества, различных форм обмана и шантажа, которые являются повседневной реальностью киберпространства. Они стали повсеместными и влияют на всех и на все виды деятельности, преодолевая препятствия во времени и пространстве.

Защищенной системы, аппаратной или программной платформы или операционной системы, включая мобильные системы (ноутбуки и мобильные телефоны), не существует.

II.1.9 Основные формы интернет-преступности

II.1.9.1 Мошенничество, шпионаж и разведывательные действия, рэкет и шантаж

Различные формы организованной преступности (рэкет, торговля людьми, получение денег обманным путем, кража и т. д.) могут извлекать пользу от использования информационных технологий, в особенности интернета. Облегчая связь, интернет помогает тем, кто замешан в любой форме контрабанды (будь то оружие или люди) и мошенничества (покушение на собственность, компьютерные системы и инфраструктуры, похищение данных, нарушение авторского права и т. д.).

Преступники используют интернет по-разному. Некоторые используют идентификационные данные других людей, для того чтобы делать покупки за счет жертвы. Часто такое происходит при подделке кредитной карты, например, путем создания действительных номеров карт, которые не совпадают ни с одним из реально существующих счетов. Эту информацию используют для покупки чего-либо в интернете, используя имеющийся в распоряжении адрес для разовой доставки. Затраты при этом будет нести банковская система или продавец. Пользователи кредитных карт также могут стать жертвами, например, когда вор-карманник или недобросовестный торговец разглашает номера их кредитных карт преступной группе.

---

16 www.clusif.asso.fr

17 www.spamhaus.org

Другим видом мошенничества является продажа несуществующих услуг (дипломов университетов, дипломатических паспортов для несуществующих стран, аукционы несуществующих товаров и т. д.).

Интернет также облегчает шпионаж и разведывательной работы, что позволяет легко перехватывать информацию, передаваемую через интернет.

Следует заметить, что систематическое использование террористами защищенных средств связи таких, как шифрование, может помочь им действовать с большей степенью безопасности, путем снижения количества информации, которую могут перехватить правоохранительные органы.

Интернет – это мощное средство, которое применяется для распространения способов совершения преступлений и незаконных действий, поощряя потенциальных преступников.

II.1.9.2 Преступления против личности

Интернет дает возможность тайным виртуальным сообществам формироваться на основе действий, подлежащих строгим правовым санкциям. Такие действия могут включать в себя порнографию, педофилию или так называемые игровые фильмы с намеренно произведенным реальным убийством (фильмы со сценами насилия и пыток над настоящими жертвами, которые иногда могут закончиться их смертью). Этот тип преступности часто бывает связан с торговлей людьми, чаще всего женщинами и детьми. Можно обмениваться фильмами и фотографиями с минимальным риском быть обнаруженными полицией. При том, что серверы часто расположены в странах, где правоохранительные органы отсутствуют или действуют неэффективно, и при использовании услуг частной системы диалогового общения по интернету (IRC) в течение очень ограниченного периода времени одноранговые (P2P) обмены значительно расширяют свободу действий преступников.

Среди преступлений против личности можно назвать нарушения, касающиеся приватности, репутации лица, профессиональной тайны и прав на тайну личных данных. Преступления против несовершеннолетних включают в себя распространение сообщений порнографического содержания, которые несовершеннолетние могут увидеть.

II.1.9.3 Нарушения авторского права

Легкость, с которой можно воспроизводить цифровую информацию, породила рынок нелегальных копий. Из-за этого издатели программного обеспечения, музыки и видеофильмов несут убытки, исчисляемые многими десятками миллиардов долларов США.

Также наблюдается увеличение количества плагиата в научных и учебных работах из-за простого копирования документов из сети.

Существует большое разнообразие возможных нарушений интеллектуальной собственности: подделка авторских работ (включая программное обеспечение), дизайна, модели, торговой марки и т. д.

II.1.9.4 Манипуляции с информацией

Манипуляция может принимать различные формы, например, разглашение внутренних документов, для того чтобы дестабилизировать компанию, отправка электронных запросов о благотворительных пожертвованиях через подставные сайты и т. д.

Интернет служит распространению слухов и дезинформации. Он также содействует нарушению закона о СМИ, подстрекательству к преступлениям, покровительству преступлений против человечества, покровительству терроризма и подстрекательству к нему, подстрекательству к расовой ненависти, историческому ревизионизму (нигилизму), злостной клевете, оскорблениям и т. д.

На рисунке II.5 приводится некоторые типы преступлений, которым содействует интернет.

Рисунок II.5 – Примеры преступлений, которым способствует интернет

Преступления против личности – Личный вред – Приватность – Репутация – Клевета – Профессиональная конфиденциальность – Цифровая приватность – Меньшинства
Преступления против собственности – Обман – Атаки на информационные системы – Нарушение закона о СМИ
Стимул к совершению преступлений – Покровительство преступлениям против человечества – Покровительство и подстрекательство к терроризму – Разжигание расовой ненависти – Отказ сознаться в геноциде – Клевета – Оскорбления
Нарушения закона об интеллектуальной собственности – Подделка работы автора (включая программное обеспечение) – Подделка чертежа или модели – Фальсификация торгового знака – Незаконная игра на бирже в интернете

II.1.9.5 Роль общественных организаций

Чаще чем обычно слышатся призывы к органам государственной власти о выполнении их традиционного предназначения по предотвращению и судебному преследованию мошенничества и преступлений. Они также должны проявить активность в подготовке и разъяснении среди широкой общественности. В частности, было бы полезно давать справочную информацию по защите людей и собственности при пользовании интернетом.

Было бы опасно позволять правоохранительным органам отставать в области технологий. Издержки на наверстывание упущенного за несколько лет времени превышают прямые финансовые расходы в виде приобретения новой инфраструктуры; существуют, прежде всего, общественные издержки, связанные с ростом влияния структур организованной преступности на общество, сопровождающиеся риском дестабилизации.

В то же время, чрезмерное присутствие полиции в интернете не всегда является желательным и может противоречить необходимости в защите конфиденциальности обмена информацией и уважении приватности.

II.1.10 Нарушения в области безопасности и незарегистрированные киберпреступления

Следует заметить, что по киберпреступности мало статистики. Это новый тип преступности, и о большинстве происшествий не сообщается в полицию. Также, если речь идет о нарушениях за пределами страны, уголовное право обычно зависит от конкретной страны, и поэтому трудно составить статистику по преступлениям, по-разному классифицируемым в разных странах. Например, в случае, если компьютерная система использовалась для выполнения мошеннической финансовой операции с использованием похищенных идентификационных данных пользователя, это преступление можно отнести к преступлениям с использованием компьютера или к финансовым преступлениям.

Тем не менее, некоторые организации в США, например, группы децентрализованного компьютерного расследования и определения угрозы инфраструктуре (CITA), координированные Национальным центром защиты инфраструктур (NIPC), дают некоторые указания на масштабы киберпреступности.

По данным CERT[18], число нарушений, связанных с безопасностью, с начала нашего века постоянно росло, также как и число атак, о которых было сообщено правоохранительным органам, что позволило лучше понять и оценить киберпреступность. В 2003 году произошло значительное увеличение количества спама, который кроме интернета распространился и на текстовые сообщения SMS. Было арестовано и осуждено множество спаммеров. Полномасштабные операции, проведенные в США (операции E-Con в мае 2003 года и Cyber-Sweep в октябре 2003 года) и Европе (Испания, Италия, Франция, Великобритания и т. д.), показали, что власти реагируют на новую криминальную ситуацию и адаптируются к ней. Арест и осуждение нескольких авторов вирусов и спаммеров подтвердило намерение бороться с этими новыми типами правонарушений. Однако число осужденных остается очень низким, если учитывать абсолютный объем спама и вирусов, появляющихся каждый день[19].

Оценить уровень киберпреступлений, которые не регистрируются, трудно. Возможно, правоохранительные органы, полиция и широкая общественность узнают не более чем о 12% киберпреступлений[20]. Получить подлинные данные о преступлениях с использованием компьютера трудно, и это серьезно затрудняет попытки анализировать это явление и определить его масштабы.

Отсутствие официальной статистики отчасти объясняется тем, что организации:

- желают избежать огласки атаки;
- могут не знать, что они стали жертвами киберпреступления, особенно в случае пассивной атаки (очевидное похищение данных, трафика, пассивный перехват, необнаруженное вторжение и т. д.); они также могут узнать об атаке слишком поздно, когда уже нет смысла как-либо реагировать;
- не знают, как справиться с кризисной ситуацией;
- недостаточно доверяют правоохранительным органам и полиции и их способности решать такие проблемы;
- предпочитают решать проблему самостоятельно.

Умения хакеров, сложность и мощь атак и инструментария атакующих совершенствуются с каждым днем, также растет и количество атак. Справиться с все время увеличивающейся сложностью, вытекающей из этой тенденции, сложно. Без большой политической воли и чувства ответственности всех участников на международном уровне, как и без эффективного партнерства частного и государственного секторов, любые меры по обеспечению безопасности, как технического, так и законодательного характера, будут неадекватными и несистематическими и, таким образом, будут неэффективны в борьбе с киберпреступлениями.

---

[18] Координационный центр CERT, Университет Карнеги-Меллон (www.cert.org).

[19] В Отчетах по компьютерным вирусам, 2004 г., Центра безопасности агентства продвижения информационных технологий (IPA/ISEC) в Японии говорится о 85 059 известных вирусов в ноябре 2003 года: www.ipa.go.jp/security/english/virus/press/200401/virus200401-e.html.

[20] Владимир Голубев, "Типология компьютерных преступлений", опубликованная 9 января 2004 года, Центром исследований компьютерных преступлений: www.crime-research.org/articles/Golubev1203/.

II.1.11 Подготовка к угрозе киберпреступности: обязанность обеспечить защиту

Необходимо приготовиться к угрозе киберпреступности, которая обязательно рано или поздно материализуется.

Необходимо организовать защиту имущества организации, учитывая риск преступления при определении стратегии безопасности. Хотя определить киберпреступников может быть сложно, и об их методах работы и мотивации известно недостаточно, было замечено, что преступные организации обычно действуют, приспосабливаясь, и атакуют наиболее незащищенных. Организации могут предпринять определенные шаги, чтобы не стать привлекательным объектом для киберпреступников, убедившись, что их компьютерная инфраструктура защищена лучше, чем окружающие инфраструктуры, а не довольствоваться тем же уровнем, что и их конкуренты, в смысле небезопасности. Киберпреступность, таким образом, становится средством воздействия для обеспечения высокого уровня безопасности.

Организация, рассматриваемая преступниками как привлекательная потенциальная жертва или важный объект для разрушения, неизбежно привлечет на себя направленную атаку. Во втором случае угроза настоящего разрушения в результате террористического акта становится реально возможной. В таких случаях необходимо реализовать соответствующую стратегию защиты. Однако эффективность традиционного страхования и инструментов управления рисками ограничена в вопросах взаимодействия с риском преступления, поскольку единственный способ избежать определенных рисков – это не подключаться к интернету.

Риск совершения преступления имеет глобальные масштабы и влияет на организации всех уровней (акционеры, органы исполнительной власти, служебный персонал, склады и т. д.). Поэтому они должны научиться сохранять свою целостность в условиях риска преступления, как они научились делать это в отношении риска коррупции, например. Они должны оставаться прибыльными, и компенсировать альтернативные издержки, вызванные рисками киберпреступления и издержки на меры, предпринимаемые для управления ими. С помощью тех, кто обладает частью благосостояния, создаваемого организацией, необходимо создать экономическую модель для нахождения лучшего способа компенсации стоимости защиты инфраструктуры и обеспечения безопасности для систем, сетей, данных и услуг, что несколько затрудняет экономический рост.

Осознание хрупкости цифрового мира и невозможности абсолютного контроля не только над IT и технологиями электросвязи, но и над коммерческими решениями по вопросам безопасности, должно неизбежно поставить фундаментальный вопрос о зависимости от технологий, которые мы не можем контролировать.

Насколько мы хотим зависеть от поставщика услуг, страны или администратора?

Первым шагом на пути контроля киберпреступности должны быть:

- пересмотр отношения к новым технологиям и поставщикам;
- осознание потребности в гарантии безопасности;
- установление ответственности всех участников.

До того как реализовывать традиционные меры безопасности, основанные на подходе "предотвращение – защита", мы должны сначала попытаться защитить важные ресурсы организации путем пересмотра отношения к новым технологиям.

Мы должны требовать:

- высококачественной продукции, гарантирующей управляемый и поддающийся проверке уровень безопасности;
- чтобы безопасность была явной, а не скрытой, как в прошлом;
- чтобы за безопасность несли ответственность не только пользователи, но и технические организаторы совместного дела (юридическая ответственность специалистов: разработчиков программного обеспечения, поставщиков доступа и т. д.);
- чтобы минимальный уровень безопасности был встроен в технические решения (безопасная продукция).

Принимая во внимание дела организации и сталкиваясь с совместной деятельностью и конвергенцией в области организованной преступности, экономической преступности, мы понимаем необходимость

всеобъемлющей, многосторонней и международной реакции для усиления уверенности участников экономики в области информационных технологий и уменьшения вероятности совершения преступления.

Эта реакция должна удовлетворять требованиям национальной безопасности и безопасности организаций и частных лиц. Она должна держать киберпреступность на приемлемом уровне, усиливать доверие в цифровом мире и минимизировать риск коррупции и угрозы правоохранительным органам.

Раздел II.2 – Кибератаки

II.2.1 Типы кибератак

Существуют различные способы использования возможностей, предоставляемых интернет-технологиями. Чаще всего эти способы основываются на присвоении параметров соединения или паролей законных пользователей и на обманном использовании недостатков и уязвимых мест технологий.

II.2.2 Похищение паролей пользователей для проникновения в систему

Основными методами, используемыми для получения параметров соединения законных пользователей, для получения доступа в системы являются:

- Угадывание: пароль настолько очевиден (имя пользователя, его супруга(и) или ребенка, дата рождения и т. д.), что учетная запись практически незащищена.
- Обман (бытовая махинация): атакующий представляется администратором и спрашивает пароль под каким либо предлогом технического характера. В удивительно большом числе случаев, пользователи раскрывают свои данные.
- Перехват трафика: атакующий перехватывает или прослушивает незашифрованные данные, передаваемые по сети через протоколы связи (пассивное прослушивание сети, слежение).
- Программное обеспечение: на рабочую станцию пользователя внедряется "Троянский конь", который тайно записывает параметры, используемые для соединения с удаленными системами.
- Получение доступа к файлу хранения паролей.
- Взлом паролей, пересылаемых в зашифрованной форме.
- Слежение за пользователями путем активации их мультимедийных периферийных устройств для записи параметров соединения.

Однажды получив код доступа, необходимый для входа в систему (комбинация имени пользователя и пароля), легко проникать в систему и выполнять все виды операций чтения и записи. Задача хакера – не быть обнаруженным и не оставить следов своего присутствия в системе, к которой был получен доступ.

II.2.3 Атаки типа "отказ в обслуживании"

Атаки типа "отказ в обслуживании" обычно выполняются путем перегрузки пропускной возможности системы. Системы-жертвы, загруженные гораздо большим числом запросов, чем они могут обработать, дают сбой и становятся недоступными. Эти атаки могут совершаться при использовании недостатков операционной системы и определенных свойств системы, например, управления буферным ЗУ (атака переполнения буфера), что вызывает серьезные сбои в работе, и даже может привести к выключению системы.

Электронное бомбардирование, включающее в себя наводнение почтового ящика пользователя сообщениями, является одной из форм атаки "отказ в обслуживании".

II.2.4 Атаки -искажения

Атака-искажение выполняется путем замены веб-страницы жертвы на другую, причем содержание новой страницы (например, порнографическое, политическое) будет зависеть от мотивов хакера. Один из вариантов такой атаки предполагает перенаправление пользователей на сайт-ловушку, который выглядит точно также как и тот сайт, на который они направлялись. Там пользователя просят ввести информацию о номере кредитной карты, например. Такие действия могут выполняться при мошеннических атаках.

Содержание веб-сайтов также может быть искажено для дезинформирования (для оказания влияния на события, распространения неуверенности, манипулирования общественным мнением и т. д.). Такие атаки являются семантическими, разрушающими смысл информационного содержания, и являются разновидностью информационной войны.

II.2.5 Атаки имитации соединения

Все протоколы TCP/IP (протокол управления передачей/протокол Интернет) можно повредить и использовать для нарушения безопасности системы. Такому же риску подвергаются протоколы и механизмы, осуществляющие передачу данных по сети. Таким образом, есть вероятность захвата сеанса TCP во время рабочего сеанса "клиент-сервер".

TCP функционирует путем установления логического соединения между двумя корреспондентами и поддержки обмена данными приложений между ними. Для соединения распределенных приложений TCP использует номера портов, логических идентификаторов приложений. Некоторые из них являются фиксированными, зарезервированными для определенных программ и хорошо известны пользователям; другие распределяются динамическим образом во время соединения, согласно определенному алгоритму. Атака на номер порта TCP включает оценку или предсказание следующих номеров портов, которые будут распределяться для обмена данными, и использование их вместо законного пользователя, эффективный захват этих номеров. Это позволяет пройти через защитные системы и установить "безопасное" соединение между двумя объектами (хакером и жертвой). Между тем, доступ законного удаленного пользователя к данному оборудованию, конечно, блокируется, но бывает достаточно просто отправить ему сообщение о том, что запрашиваемая система неактивна.

Протокол дейтаграмм пользователя (UDP) является протоколом 4-го уровня (транспортный), не ориентированным на установление соединений. Он является альтернативой использованию TCP для быстрой передачи небольших объемов данных. Соединения UDP не контролируются никакими механизмами, поэтому в них нет проверки на идентификацию, поток или ошибки. В результате любой человек может использовать IP адрес авторизованного пользователя системы, чтобы проникнуть в эту систему. Похищение сеанса UDP может произойти без сигнала тревоги со стороны серверов приложений.

Поскольку функционирование различных протоколов является общеизвестной информацией, злоупотреблять ими довольно легко, например, для генерирования ложных пакетов для перегрузки сети в атаке типа "отказ в обслуживании". Это показывает потребность в безопасности в отношении доступности сетей и служб.

Хакеры используют протоколы и их ограничения, для того чтобы:

- парализовать работу сетей;
- перенаправить IP пакеты не по назначению (например, к себе);
- перегружать системы, забрасывая их лишними сообщениями;
- помешать отправителю передать данные;
- взять контроль над передачей пакетов, задерживая движение сетевого трафика и ухудшая эффективность передачи (надежность и т. д.).

Обычно атаки маршрутизации включают подмену роутеров, шлюзов и адресатов путем предоставления им ложных адресов так, что данные передаются в неправильном направлении.

Атакующие могут легко перенаправить пакеты в нужном им направлении, используя необязательные IP характеристики, которые служат для определения маршрута, другими словами для указания адресов промежуточных систем, через которые должен пройти пакет, путем подделки этих адресов.

Атакующие знают, как можно использовать не только характеристики работы протоколов связи, но и характеристики различных оперативных систем и способов их работы. Так, при перегрузке некоторых буферов (атака по переполнению буфера) можно спровоцировать серьезные сбои в работе или аварию системы. Объектами таких атак являются, конечно, системы, предоставляющие важные услуги либо при передаче данных (например, маршрутизаторы) или при управлении именами и адресами, например, серверы преобразования имен. Целью большинства атак на веб-сайты является прекращение их работы при помощи использования недостатков оперативной системы.

II.2.6 Атаки против ключевой инфраструктуры

Уязвимость ключевых общественных инфраструктур (энергоснабжение, водоснабжение, транспорт, снабжение продуктами питания, электросвязь, банковские и финансовые учреждения, медицинские услуги, работа органов управления и т. д.) возрастает по мене того, как распространяется использование интернета и к этим инфраструктурам можно получить доступ через "сеть из сетей".

Особое внимание следует уделить уязвимости систем производства и распределения электроэнергии, которые важны для работы большей части инфраструктуры страны, и, таким образом, жизненно необходимы. Сложность и распределенный характер связей между различными ключевыми инфраструктурами является их сильной и одновременно с этим и слабой стороной.

Важно, чтобы шлюзы между сетями использовались для управления этими инфрастуктурами, обеспечивалась безопасность интернета и чтобы региональные и национальные организации могли следить за защитой важных инфраструктур. Первой задачей этих организаций должна стать координация и поддержка планов по защите каждой инфраструктуры. В случае возникновения чрезвычайных ситуаций в нескольких инфраструктурах одновременно, координированные и последовательные планы и решения по вопросам безопасности чрезвычайно важны.

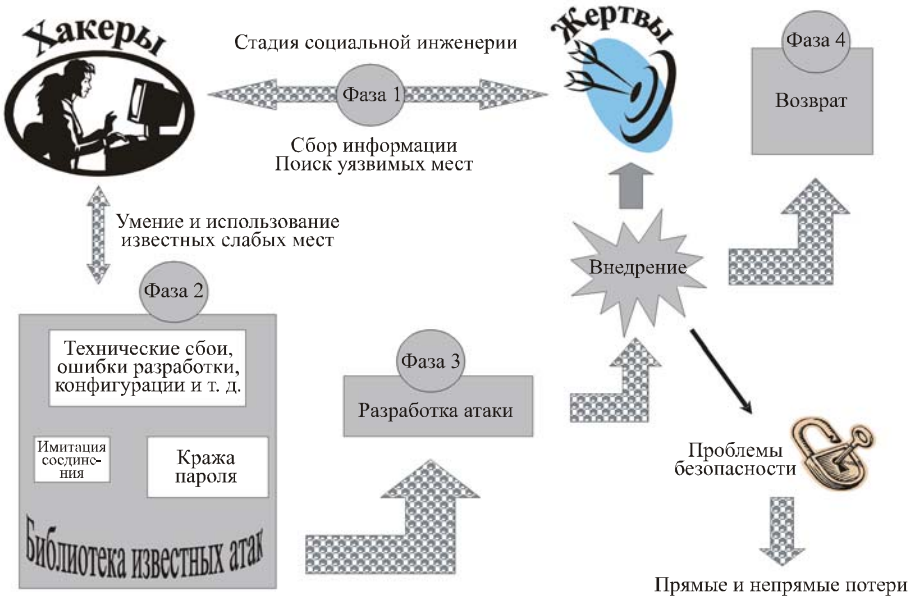
II.2.7 Стадии кибератаки

На рисунке II.6 показаны различные стадии кибератаки[21].

Целью первой стадии является сбор информации и обнаружение потенциальных уязвимых мест в системе-жертве для получения максимума информации для использования в будущем. На этой стадии происходит изучение механизмов и уровней безопасности, используемых для идентификации, аутентификации, управления доступом, шифрования и наблюдения, а также определение технических, организационных и человеческих слабостей в данной среде. Атакующий часто пытается обманом заставить наивных и доверчивых пользователей раскрыть информацию, которую можно использовать при нападении (это называется социальной инженерией).

[21] Иллюстрация взята из *Sécurité informatique et télécoms: cours et exercices corrigés* С. Гернаоути – Хелие (Дюно, 2006 г.).

Рисунок II.6 – Типичные стадии кибератаки



Для внедрения в систему хакеры также могут искать и использовать обнаруженные, но еще не ликвидированные уязвимые места, используя доступные средства (библиотеки атак, инструментарий атак). Целью стадии отступления является сокрытие следов атаки и, если эти следы скрыть невозможно, обеспечение того, что хакер не будет обнаружен. Хакеры повышают свою анонимность путем использования вымышленных имен, присвоения идентификационной информации законных пользователей или сокрытия следов при помощи использования многочисленных промежуточных систем (реле).

ЧАСТЬ III

Технический подход

Раздел III.1 – Инфраструктуры электросвязи

III.1.1 Характеристики

Благодаря охвату огромной территории, телефонная сеть стала основной сетью, обслуживающей большое число пользователей. Сегодня инфраструктуру телефонной сети можно использовать для передачи не только речи, но и данных. Так, при помощи необходимых интерфейсов можно соединять компьютеры через телефонную сеть. Кроме того, в последние годы распространились точки доступа к сети интернет, количество киберкафе все время увеличивается, и все больше и больше стран создают у себя доступную инфраструктуру передачи, предлагающую большие возможности. В некоторых местах, развертываются кабельные сети для поддержки передачи телевизионных каналов.

Кроме фиксированных инфрастуктур электросвязи, существуют также и так называемые "беспроводные" инфраструктуры, которые делают возможной мобильность пользователей. Поддержку беспроводных технологий осуществляют спутниковые и космические инфраструктуры и наземные системы радиосвязи. В последние годы средством предоставления услуг во многих развивающихся странах стала подвижная телефонная связь.

Для передачи речи и небольших объемов информации на нескольких континентах был принят стандарт GSM (Глобальная система подвижной связи). Однако более интенсивному использованию мобильных мультимедийных телефонов способствовало появление нового поколения сетей подвижной связи на основе стандарта UMTS (Универсальная система подвижной связи с глобальным роумингом), обладающего лучшими возможностями передачи. Сети GSM развиваются и теперь включают в себя GPRS (Пакетная передача данных по радиоканалам), что позволяет увеличить скорость передачи для удовлетворения потребностей применения данных к подвижным сетям.

Быстрое появление таких технологий, как GSM, отражает не только технические изменения, но и изменения в экономике и поведении людей. Подвижная связь является динамически развивающейся отраслью в условиях жесткой глобальной конкуренции. Подвижная связь также вывела на рынок электросвязи новую услугу, радиотелефонию, которая до этого относилась к сфере деятельности операторов. В то же время подвижная связь время создавала инфраструктуру, которую можно повторно использовать для всех видов передачи данных.

Вне зависимости от технологии, применяемой для развертывания электронных услуг, инфраструктуры электросвязи в развивающихся странах должны обеспечивать:

- стандартизованное межсетевое цифровое взаимодействие (голос, данные, изображения) определенного набора основных услуг, которые легко установить и поддерживать и которые предлагают необходимый географический охват (национальный и международный), в рамках структуры подхода абсолютного качества (устойчивый и постоянный спектр услуг, который можно изменить при минимальных технических и экономических затратах) и оптимальной безопасности;
- техническую и коммерческую координацию; защиту против возможной картелизации для гармоничного развития инфраструктур и услуг с гарантией активного контроля злоупотреблений и доминирующих позиций.

III.1.2 Основные принципы

Сеть электросвязи состоит из набора взаимодействующих информационных ресурсов и ресурсов передачи, предлагающих услуги связи. Эти услуги делают возможным удаленный доступ и обмен взаимосвязанными информационными ресурсами, взаимодействие приложений и людей, дистанционное выполнение программ и передачу информации.

Вся экономическая деятельность сейчас серьезно зависит от доступности эффективной инфраструктуры связи, соединяющей все виды оборудования, приложений и людей и позволяющая им работать вместе вне зависимости от расстояния, места и типа информационных потоков, предназначенных для передачи.

Сети классифицируются преимущественно на основе нескольких критериев таких, как географический охват, топология[22], используемая технология и поддерживаемые приложения, режим работы, тип среды передачи (проводная/беспроводная линия связи), их частный или общественный характер и т. д.

Исторически первыми сетями были территориально-распределенные сети (WAN)[23] (телефон, телекс, Transpac, интернет и т. д.). И только с появлением ПК (в начале 80-х) появились локальные сети[24].

Не так давно эти различия стали менее явными, поскольку сети, о которых идет речь, теперь взаимосвязаны. Например, локальная сеть может соединяться с другими локальными сетями (LAN) и таким образом стать большей по размеру сетью. Кроме того, сети больше не поддерживают только один тип приложений, теперь их можно использовать для передачи голоса, данных, видеоизображений (мультимедийная сеть).

Сеть может быть частной, принадлежать организации, имеющей исключительные права на использование, или быть сетью общего пользования. В сетях общего пользования услуги электросвязи предоставляются различным частным лицам или учреждениям на основе особых соглашений о подписке.

Основными технологиями передачи, используемых для создания глобальных сетей, являются TCP/IP, ретрансляция кадров и ATM (асинхронный режим передачи). На рынке коммерческих LAN основной технологией является сеть Ethernet и ее высокоскоростные варианты (быстрая сеть Ethernet, коммутируемая сеть Ethernet).

В области электросвязи основной шаг в эволюции инфраструктур и магистралей передачи и сделали оптическая передача и технология коммутирования ATM, что сделало возможной высокоскоростную и высококачественную передачу, динамическое распределение пропускной способности, различные битовые скорости передачи данных и системы со многими пользователями.

III.1.3 Компоненты сети

III.1.3.1 Среда межсетевого взаимодействия

Для того чтобы соединить компьютеры вместе и получить сеть, необходима среда передачи. Это могут быть физические среды (кабели витой пары, коаксиальные кабели, оптоволокно) или нематериальные среды (радио, инфракрасные волны). Все эти различные среды обладают особыми свойствами, которые определяют их надежность и пропускную способность при передаче различных объемов информации с различной скоростью.

Коэффициент пропускания или пропускная способность среды взаимодействия – это количество информации, передаваемой в течение определенного отрезка времени. Она измеряется в кило-, мега- или даже терабитах в секунду (например, 100 Мбит/с). Пропускная способность пропорциональна пропускной способности среды передачи, которая соответствует диапазону частот сигнала, который может проходить через данную среду без каких-либо изменений.

---

[22] Топология сети – это структура, состоящая из линий, соединяющих различные элементы или узлы сети.

[23] Территориально-распределенная сеть или WAN – это сеть, соединяющая компьютеры, разбросанные по относительно большой территории (> 100 км), или даже по всему миру.

[24] Сеть считается локальной или LAN, если она соединяет компьютеры в небольшой географической области размером в несколько километров (~10 км). Городская вычислительная сеть или MAN – это сеть, соединяющая локальные сети, которые могут принадлежать различным объектам, с охватом территории до 100 км. Для идентификации различных типов ресурсов, распределяемых через сеть, или для обозначения определенной области применения используются новые термины. Таким образом, например, в специализированных текстах встречаются следующие сокращения: HAN (домашняя сеть), сеть, соединяющая оборудование в доме, управляемое в удаленном режиме (духовку, видеомагнитофон, освещение и отопление и т. д.); CAN (автомобильная сеть); SAN (сеть склада) и т. д.

III.1.3.2 Компоненты соединения

Тип соединения или компонент соединения, который помещается между средой передачи и компьютером для связывания их воедино, зависит от типа среды и используемого режима передачи. Соединительная коробка, или сетевой интерфейс, решает проблемы соединения и адаптирует сигнал, передаваемый или получаемый компьютером, в сигнал, который можно передать по этой среде. Например, модем (модулятор/демодулятор) обеспечивает интерфейс между компьютером, который представляет собой цифровую машину, обрабатывающую цифровые сигналы, и средой передачи такой, как аналоговая телефонная линия, которая непрерывно передает сигнал[25]. Теоретически подсоединить к сети можно любой электронный компонент постольку, поскольку он имеет соответствующий интерфейс соединения аппаратного и программного обеспечения.

III.1.3.3 Специализированные машины и сервера данных

Кроме пользовательских систем, служащих для доступа к сети, и компьютеров, обрабатывающих приложения (узлы данных и сервера) и управляющих ими, транспортную инфраструктуру сети составляют процессоры передачи данных. Это компьютеры, выполняющие одну или более функций, необходимых для управления с установления электросвязи (оптимизация и обмен ресурсами, маршрутизация данных, управление адресами, именами, взаимодействие и т. д.). Они включают в себя, например, маршрутизаторы (роутеры), мультиплексоры, концентраторы, коммутаторы или шлюзы взаимосвязи.

Для обеспечения связи информацию необходимо надежно передавать в соответствии с договоренностями об обмене, подходящими корреспондентам. Проблема состоит в том, что системы, соединяемые посредством сетей электросвязи, априори различны. Для того чтобы установить диалог, им нужно использовать одну и ту же систему отсчета, другими словами, они должны говорить на одном языке и следовать общим правилам обмена.

Это напоминает двух людей, говорящих на разных языках, желающих обменяться информацией, которые договариваются, какой из двух языков использовать. Один из них может попытаться говорить на языке другого или они могут использовать третий общий язык.

Если к разговору присоединяется третий, четвертый, пятый и т. д. человек и эти люди начинают говорить на других языках, вероятно, им будет трудно обмениваться информацией, если для каждой пары разговаривающих необходимо переводить с какого-либо языка. В таком случае, предпочтительнее говорить на общем языке, который примут все участники дискуссии.

Подобным образом, компьютеры, соединенные в сеть, должны подчиняться одинаковым протоколам связи и следовать одним и тем же правилам диалога, для того чтобы взаимодействовать. Эти протоколы интегрированы в программное обеспечение связи. Они служат, помимо всего прочего, для обеспечения правильной маршрутизации данных и взаимодействия удаленных приложений и систем.

Международные стандарты или принятые де-факто стандарты связи определяются организациями, признаваемыми всем информационным сообществом. Международная организация по стандартизации (ИСО) и Международный союз электросвязи (МСЭ) являются международными органами стандартизации, которые рекомендуют международные стандарты (например, стандарты Серии X.400)

Принятый де-факто стандарт связи – это стандарт, хотя и не принимаемый такой организацией, широко используется на рынке. Затем он становится образцом, т. е. принятым де-факто стандартом электросвязи. Например, все протоколы, происходящие из интернета, являются принятыми де-факто стандартами.

---

[25] Для того чтобы информация на выходе компьютера передавалась по такой среде, ее необходимо смодулировать. Информацию, передаваемую в аналоговой форме, нужно демодулировать после получения и доставить компьютеру-адресату в цифровом виде. То же оборудование, модем, модулирует и демодулирует информацию, отправляемую и получаемую компьютером.

Стандарты определяют, среди всего прочего, тип услуг, предоставляемых протоколом связи, и то, как они должны предоставляться. Это дает возможность создавать методы решения проблем с данными, которые могут взаимодействовать друг с другом. Таким образом, различные (гетерогенные) машины могут взаимодействовать при использовании одних и тех же типов протоколов. Универсальный характер интернета опирается на интеграцию протоколов в семейство интернет на всех соединенных машинах.

III.1.4 Инфраструктура электросвязи и информационная супермагистраль

Под инфраструктурой электросвязи мы подразумеваем всю среду передачи, в которой могут быть созданы услуги связи. Следует различать каналы передачи и технологии маршрутизации с одной стороны, и решения электросвязи и услуги электросвязи, предлагаемые клиентам, с другой стороны. Таким образом, можно использовать существующую инфраструктуру, не приобретая ее, в качестве транспортного оборудования для обеспечения определенных приложений.

На основе доступности мультимедийного оборудования и хороших показателей работы инфраструктур электросвязи, а также конвергенции аудиовизуальной области, области информационных технологий и электросвязи, возникает понятие полной цифровой информационной цепочки: цифровая преемственность между всеми источниками и пользователями информации как внутри транспортной инфраструктуры, так и на уровне содержания.

Понятие информационной супермагистрали включает в себя широкий круг общественных или коммерческих услуг, предоставляемых при помощи высокоэффективных инфраструктур связи, целью которых является улучшение жизни людей, например, в области здравоохранения, образования, культуры, землепользования, администрирования или средств массовой информации. В силу характера некоторых услуг, предлагаемых в интернете, интернет можно рассматривать как информационную супермагистраль.

III.1.5 Интернет

III.1.5.1 Общие характеристики

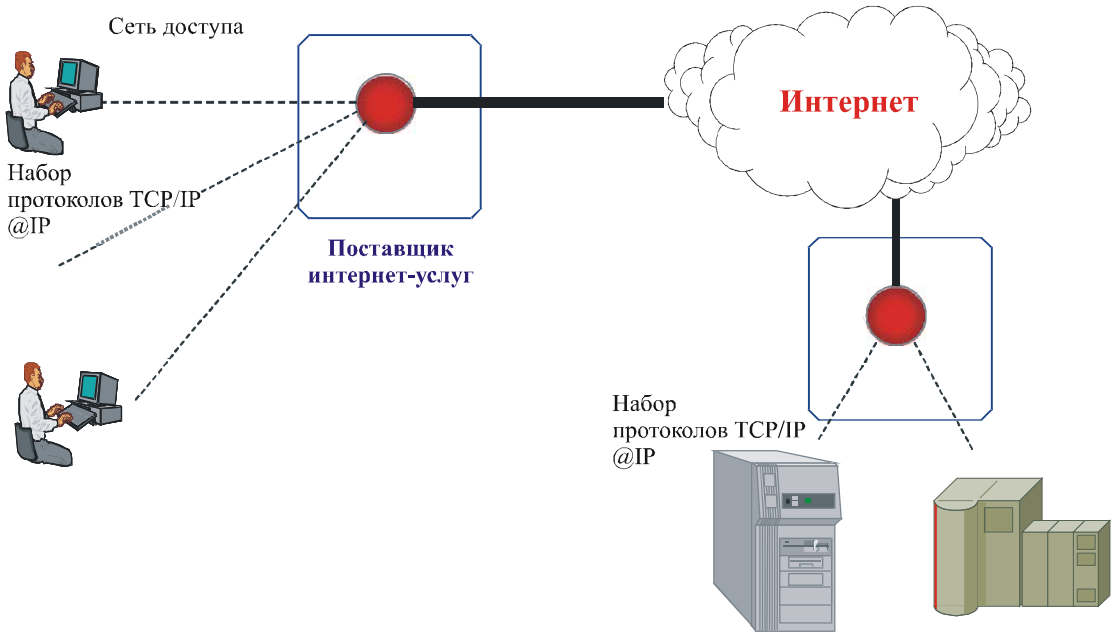
Интернет появился в США и широко распространился путем соединения соседствующих информационных систем и компьютерных сетей. Это сетевое развитие продолжается до сих пор. Оно определяет структуру сети, которая является сетью, состоящей из сетей. Полного контроля над всеми инфраструктурами быть не может, поскольку они независимы и принадлежат различным организациям.

Что касается аппаратного обеспечения, интернет, как и любая сеть электросвязи, включает в себя информационные системы, компоненты соединения и среду передачи. В информационные системы входят системы для получения доступа к сети и осуществления диалога с пользователем (ПК, мобильный телефон, пейджер, PDA и т. д.), системы для поддержки приложений (веб-серверов, серверов баз данных и т. д.) и системы для обработки внутри сети (маршрутизаторы, шлюзы взаимосвязи и т. д.).

Обмен данными между компьютерами осуществляется через среду передачи, при помощи которой они соединяются физически. Когда доступ в инфраструктуру интернет осуществляется через систему, делающую пользователя мобильным, например мобильный телефон, мы говорим о мобильном интернете.

Передача данных, маршрутизация и соединение между распределенными информационными процессами и пользователями осуществляется при помощи протоколов соединения семейства TCP/IP[26]. Эти программы для обмена, имеющие стандартную форму, составляют интерфейс связи, который обеспечивает взаимодействие различных типов систем. Для того чтобы соединяться с другими компьютерами в среде интернет, компьютер должен быть оснащен такими протоколами связи и иметь IP адрес, делающий его уникальным (рисунок III.1).

Рисунок III.1 – Доступ в интернет через ISP, комплект протоколов TCP/IP и IP адреса

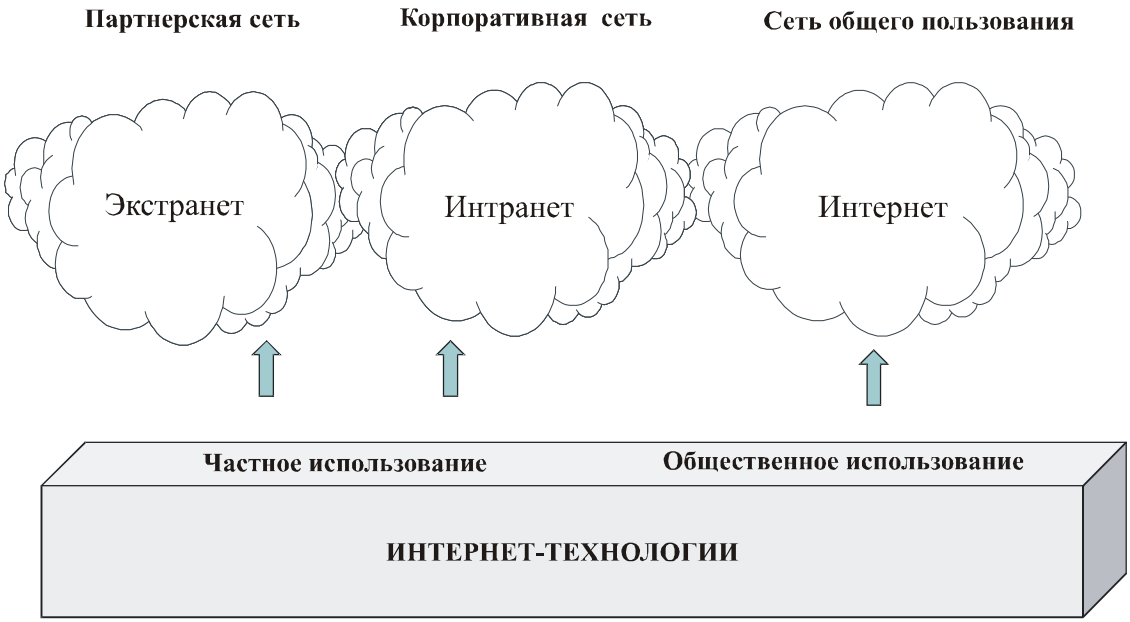


Интернет обозначает всю инфраструктуру связи, предоставляемую обществу для связи. Когда организация желает использовать эту инфраструктуру частным образом и в ограниченном объеме, она создает виртуальную частную сеть (VPN). Для внутренних нужд организация может также использовать интернет технологии для создания частной сети или интранета. Когда интранет открыт также и для нескольких партнеров (клиенты, поставщики и т. д.), такая сеть называется расширенной интрасетью или экстранетом (рисунок III.2).

Вместе с электронной почтой, "всемирная паутина" (или сокращенно "веб")) является самым важным приложением интернета. На основе веб-навигации было разработано множество услуг. Благодаря клиентскому программному обеспечению – браузеру, установленному на рабочей станции пользователя, предоставляющему удаленный доступ к веб-серверам, можно перемещаться по веб-сети. Браузер можно использовать для поиска, обсуждения или передачи информации или даже запуска программ. Понятие блуждания по интернету основывается на том, что документы, становящиеся доступными при помощи веб-приложений, являются гипердокументами. Это значит, что их создали, структурировали и отформатировали для непоследовательного чтения с использованием меток и ссылок, вставленных при создании документа. При активации ссылки пользователь перемещается в другую часть документа или в другой документ, возможно расположенный на удаленном компьютере. Таким образом, пользователь перемещается от одного сайта к другому при помощи активации таких гиперссылок.

[26] TCP/IP: Протокол управления передачей/протокол Интернет.

Рисунок III.2 – Интернет – интранет – экстранет



III.1.5.2 IP адрес и имена доменов

Доступ в сеть интернет с точек доступа управляется и контролируется специальными учреждениями, называемыми поставщиками услуг интернет (ISP). Каждый ISP сам по себе подсоединен к интернету постоянными линиями электросвязи, которые он делит между своими клиентами. Кроме этой основной услуги, поставщики обычно предлагают службу управления электронной почтой, а также могут размещать сайты клиентов.

Для того чтобы подсоединиться к интернету, нужен интернет-адрес (IP адрес). Это 32-битная двоичная последовательность, однозначно определяющая каждую машину, подсоединяющуюся к интернету[27].

IP адрес выражается в десятичной форме и состоит из четырех десятичных чисел, отделяемых друг от друга точками. Например, адрес 128.10.2.30 соответствует двоичному значению 10000000.00001010.00000010.00011110. Поскольку запоминать такие последовательности, даже десятичные, невозможно, для идентификации ресурсов в среде интернет используются имена (часто мнемонические) или логические адреса. Эти IP адреса и соответствующие имена хранятся в электронных справочниках, которые называются серверами имен, более широко известными в виде сокращения DNS (domain name server – сервер доменных имен).

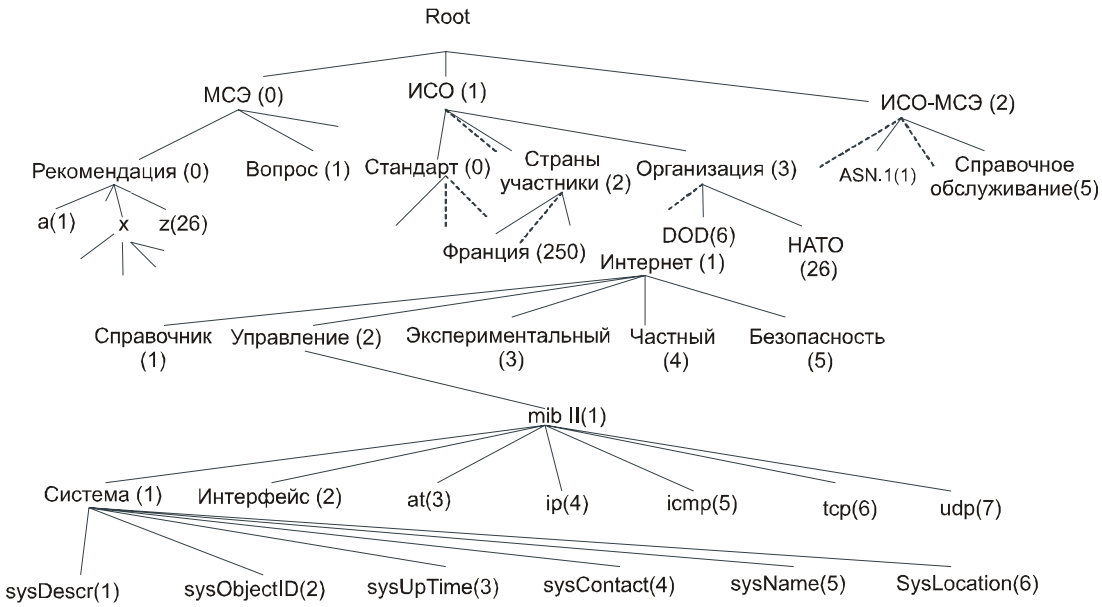
Для осуществления связи в открытой среде необходимо обладать способностью распределять уникальный идентификатор в данном домене имен. Участники процесса связи должны быть идентифицируемыми (адреса, системы, процессы приложений, объекты, объекты управления и т. д.) также как и инструменты реализации для установления соединения (протоколы). Для того чтобы гарантировать уникальность имен по всему миру, существуют процедуры регистрирования имен в компетентных органах, задачей которых является назначение однозначных и уникальных идентификаторов для каждого идентифицируемого объекта.

[27] IP адрес уникален. Он может быть присвоен на постоянной основе (статичный IP адрес) или на непостоянной (динамический IP адрес).

В стандарте 9834 ИСО определяются органы регистрации, которые выстраиваются в иерархическую древовидную структуру. От основания этого дерева отходит три ветви, ведущие к узлам первого уровня, представляющим домены имен МСЭ, Международной организации по стандартизации и объединенного комитета ИСО-МСЭ. Это – международные органы регистрации. Уровень, непосредственно ниже ИСО авторизует регистрацию, помимо всего прочего:

- различных стандартов ИСО (стандарт 0);
- членов ИСО (организация-член 2), под которым находятся AFNOR (208) и ANSI (310);
- организации (организация (3)), под которыми расположены, например, Министерство обороны США (DOD) (6) (рисунок III.3).

Рисунок III.3 – Органы регистрации и дерево



Общие доменные имена интернет регистрируются в этой логической структуре регистрации. Значимой частью дерева регистрации в данном случае является корневой узел доменных имен высшего уровня, которые называются "домены верхнего уровня" (TLD). Эти домены, в основном, идентифицируют страны, обозначаемые двумя буквами (fr, it, uk, ch, nl, de и т. д.), и функциональны домены такие, как:

- .com коммерческие организации;
- .edu учебные заведения в Северной Америке;
- .org организации, учреждения и др.;
- .gov правительство Америки;
- .mil военные организации Америки;
- .net операторы сетей;
- .int международные объекты;
- .biz для деловой сферы;
- .info для всех пользователей;
- .name для частных лиц;

- .museum для учреждений, в которых коллекции объектов находятся для хранения и демонстрации общественности;
- .aero для авиатранспортной промышленности;
- .coop для кооперативных обществ;
- .pro для профессий.

Внутри этих широких обозначений доменов существуют субдомены, соответствующие крупным корпорациям или важным учреждениям.

Центр по присвоению номеров интернет (IANA)[28] совместно с интернет корпорацией по присвоению имен и адресов (ICANN)[29] отвечают за присвоение имен и адресов и должны гарантировать их уникальность. Ответственность за управление именами можно переложить на субдомен, который в иерархии находится ниже этой организации.

Регистрирование доменного имени состоит в занесении этого имени в справочник имен. Это равноценно созданию нового ответвления в дереве регистрации, управляемом авторизованной организацией. В мире существует несколько таких ответвлений, в частности для доменов .biz, .com, .info, name, .net, .org.

Во Франции, например, органом регистрации (аккредитованным регистрационным бюро), аккредитованным ICANN, является AFNIC[30].

Полномочия распределять адреса и управлять ими отданы американской ассоциации – на американской территории, действующей по американским законам[31]. Таким образом, эта ассоциация контролирует доступ в интернет. Это поднимает важнейшую проблему зависимости организаций и государств от иностранной структуры, открытой всему миру, в которой, однако, неамериканское представительство слабо.

Организации не могут контролировать или управлять критерием безопасности в области доступности (инфраструктур, услуг, данных), зависящим от доступности сети интернет. Организации зависят, при доступе в интернет, от распределения IP адресов и доменных имен, то есть от внешних объектов.

Справочники доменных имен можно рассматривать как базы данных, которыми управляют DNS сервера. Около пятнадцати корневых DNS серверов координируются ICANN, в Северной Америке расположено большинство корневых серверов. Они управляют доменными именами верхнего уровня и IP адресами. Доменные имена верхнего уровня включают все ранее упомянутые доменные имена (.org, .com, etc.), а также 244 доменных имени для различных стран (.cn – Китай, .ga – Габон, .lk – Шри-Ланка, .pf – Французская Полинезия и т. д.). На локальных DNS серверах, называемых преобразователями IP адресов, хранятся копии информации, содержащейся на корневых серверах. Эти преобразователи, часто связанные со стратегическими точками доступа к сети или подсоединенные к поставщикам услуг интернет, служат для ответа на запросы пользователей, касающихся перевода доменного имени в IP адрес (рисунок III.4)[32].

---

[28] www.iana.org/

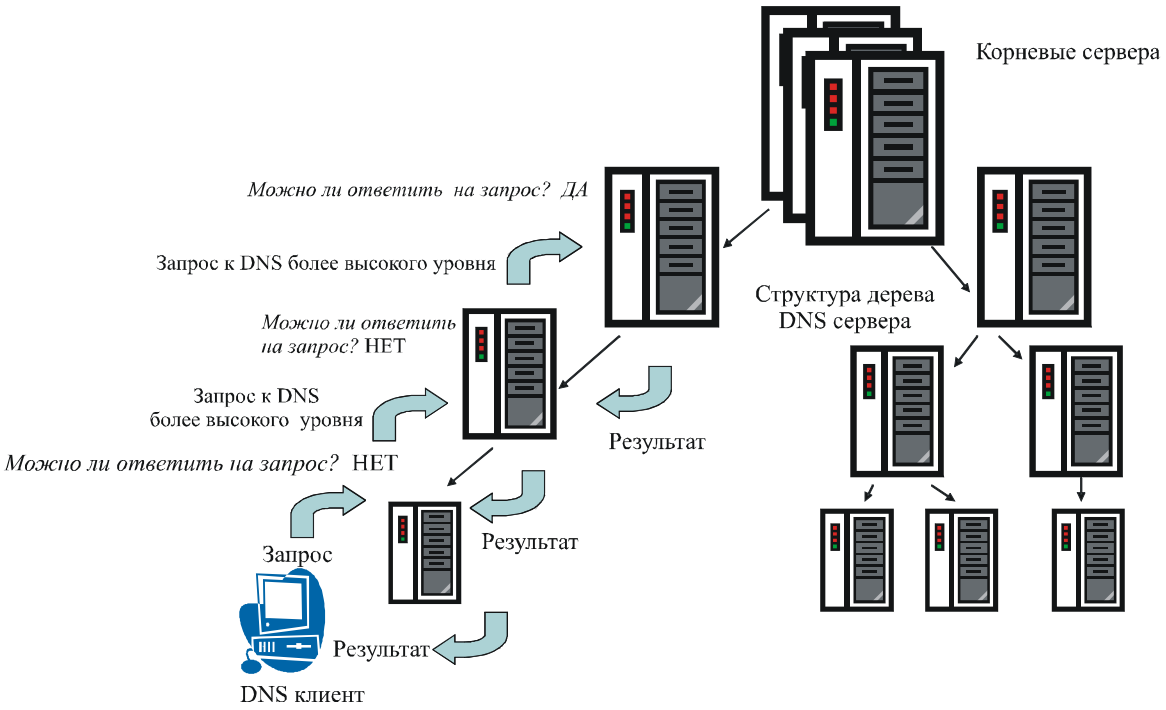
[29] www.icann.org/index.html

[30] www.afnic.fr

[31] Согласно ICANN: "Интернет – корпорация по присвоению имен и номеров (ICANN) – это международная некоммерческая корпорация, несущая ответственность за пространственное распределение адресов протокола Интернет (IP), присвоение идентификатора протокола, функции управления системой доменов верхнего уровня общих (gTLD) кодов и кодов стран (ccTLD). Эти услуги первоначально оказывались в рамках контракта Правительства США с Центром по присвоению имен интернет (IANA) и другими организациями. Сейчас функции IANA выполняет ICANN."

[32] Рисунок взят из: "*Sécurité informatique et télécoms: cours et exercices corrigés*"; С. Гернаоути-Хелие; Дюно 2006 г.

Рисунок III.4 – Структура дерева DNS серверов



Чрезвычайно важно, чтобы адреса, процессы и системы, участвующие в управлении именами и адресами и маршрутизации данных, характеризовались доступностью, целостностью, надежностью и защищенностью. Защита и эффективное управление средой связи – задача объектов, отвечающих за транспортные инфраструктуры.

III.1.5.3 Протокол IPv4

Версия 4 протокола Интернет (IPv4)[33], существовавшая с начала сети интернет, все еще широко используется. Этот протокол инкапсулирует передаваемые данные и составляет IP пакеты, которые будут направляться по сети интернет к месту назначения. Каждый пакет содержит, среди всего прочего, источник IP адреса системы – отправителя и IP адрес системы назначения.

Маршрутизация данных осуществляется путем их передачи каждой встречающейся промежуточной системе (маршрутизатору) после интерпретации адреса пакета и выполнения маршрутизатором алгоритма маршрутизации.

Протокол IPv4 не включает в себя никакой функции или алгоритма, обеспечивающего безопасное обслуживание. Действительно, в IPv4 нет способа аутентификации источника или места назначения пакета, как и нет гарантии конфиденциальности передаваемых данных или IP адресов, участвующих в передаче информации между двумя объектами. Кроме того, поскольку данный протокол работает в режиме, не ориентированном на установление соединений, нет гарантии:

- доставки данных (возможные потери данных);
- доставки данных правильному адресату;
- правильной последовательности данных.

[33] IPv4: RFC 0791 –www.ietf.org/rfc/rfc0791.txt IPv4 и основные протоколы TCP/IP:
TCP: RFC 0793 – www.ietf.org/rfc/rfc0793.txt – UDP: RFC 0768 – www.ietf.org/rfc/rfc0768.txt – FTP: RFC 0959 – www.ietf.org/rfc/rfc0959.txt – HTTP версия 1.1: RFC 2616 – www.ietf.org/rfc/rfc2616.txt – Telnet: RFC 0854 – www.ietf.org/rfc/rfc0854.txt

Протокол IP (уровень 3 архитектуры OSI) не обеспечивает надежной службы доставки IP пакетов. Он работает в так называемом режиме "максимальные усилия", другими словами он делает все возможное в данных обстоятельствах, и доставка пакетов не гарантируется. В действительности, не гарантируется никакого качества услуг и нет восстановления при ошибках. Таким образом, пакет может быть потерян, изменен, копирован, фальсифицирован или доставлен с нарушением последовательности без ведома отправителя или получателя. Поскольку между отправителем и получателем не устанавливается никакой логической взаимосвязи, это означает, что отправитель посылает свой пакет, не уведомляя об этом получателя, и пакеты могут потеряться, изменить маршрут или прибыть в неверном порядке.

Для компенсации этого недостатка качества обслуживания, на конечные системы устанавливается протокол управления передачей (TCP). TCP предоставляет надежные транспортные услуги в режиме, ориентированном на установление соединения (уровень 4 архитектуры OSI). Однако протокол TCP не предлагает никакой службы безопасности в полном смысле этого слова.

Раздел III.2 – Инструменты безопасности

Обеспечение безопасности информации, услуг, систем и сетей включает в себя гарантирование доступности, целостности и конфиденциальности ресурсов, а также неотказуемость определенных действий и аутентичность событий и ресурсов.

Безопасность данных имеет значение только, если она применяется к данным и процессам, которые определенно являются точными (понятие качества данных и процессов) так, чтобы они были стабильны в течение определенного времени (понятие стабильности данных и продолжительности услуг).

Основные решения безопасности базируются на использовании шифрования и методов изоляции окружения, на излишках ресурсов и на процедурах надзора, контроля и управления нарушениями безопасности и поддержания систем, контроля доступа или управления.

Безопасность данных в электросвязи достигается при помощи последовательности барьеров (мер защиты), повышающих уровень трудностей, которые должны преодолеть потенциальные нападающие, для того чтобы получить доступ к ресурсам. Эти барьеры не решают проблему безопасности, а просто изменяют ее и складывают ответственность за безопасность на другие объекты. Сами решения безопасности нуждаются в защите, если они должны обеспечивать определенный уровень безопасности (рекурсивный характер безопасности).

III.2.1 Шифрование данных

Методы шифрования дают возможность сохранять конфиденциальность данных, проверять целостность данных и аутентифицировать объекты.

Существует два основных типа систем шифрования данных: шифрование симметричным ключом (секретный ключ) и ассиметричное шифрование открытым ключом.

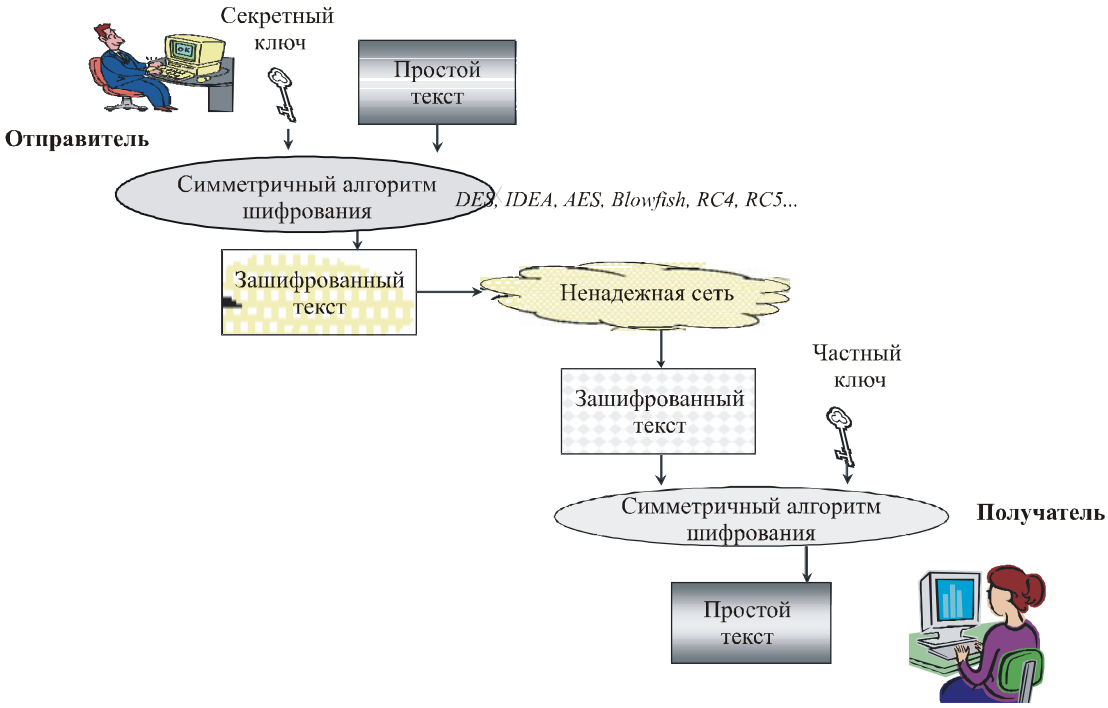
Существуют различные алгоритмы шифрования. Вне зависимости от того, работают ли они в симметричном или асимметричном режиме, они основываются на использовании ключей. В общем, то, насколько они хорошо работают, зависит от способности безопасно управлять ключами шифрования, от длины ключа (минимальная длина ключа определяется типом алгоритма), от безопасности физической и программной платформ, на которые устанавливаются и на которых запускаются алгоритмы шифрования.

III.2.1.1 Симметричное шифрование

Для того чтобы зашифровать или расшифровать текст, нужен ключ и алгоритм шифрования. Если для обеих операций (шифрования и расшифровки) используется один и тот же ключ, такое шифрование называется "симметричным". Отправитель и получатель должны пользоваться одним секретным ключом, для того чтобы сделать данные конфиденциальными и для того чтобы их понимать. Это создает проблему управления и распределения секретных ключей (рисунок III.5).

Основными алгоритмами симметричного шифрования являются: DES, RC2, RC4, RC5, IDEA и AES.

Рисунок III.5 – Симметричное шифрование



III.2.1.2 Асимметричное шифрование или шифрование открытым ключом

Система асимметричного шифрования основана на использовании уникальной пары соответствующих друг другу ключей. Этот двойной ключ состоит из открытого ключа и секретого ключа. Всем может быть известен только открытый ключ, в то время как секретный ключ должен оставаться конфиденциальным и держаться в секрете.

Отправитель зашифровывает сообщение при помощи открытого ключа получателя, а получатель расшифровывает сообщение при помощи своего секретного ключа (рисунок III.6).

Основные алгоритмы шифрования при помощи открытых ключей, названные в честь их создателей, обычно используют ключи длиной от 512 до 1024 битов, или иногда 2048 битов. Ими являются алгоритмы: RSA[34] (сокращение от R. Rivest, A. Shamir, L. Adelman), алгоритм Диффи-Хэллмана[35], алгоритм Эль Гамаля[36].

III.2.1.3 Ключи шифрования

Ключ шифрования должен быть вдвойне секретным. Секретными ключами для систем шифрования нужно управлять конфиденциально.

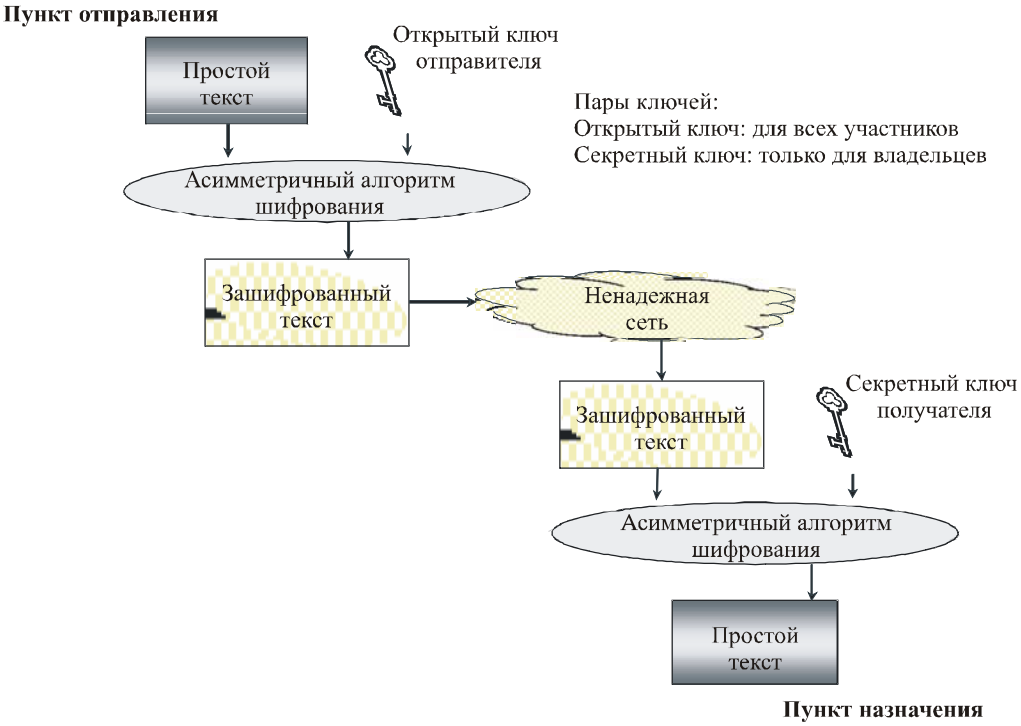
[34] RSA: Б. Шнайер, "Прикладная криптография" 1996, 2-е издание 1996 г.

[35] Диффи – Хэллман: www.ietf.org/rfc/rfc2631.txt.

[36] Ель Гамаль: Б. Шнайер, "Прикладная криптография" 1996, 2-е издание 1996 г.

Как уже было сказано, безопасность процесса шифрования в очень большой степени зависит от конфиденциальности и длины используемых ключей, от того, насколько хорошо работают алгоритмы, а также от безопасности лежащих в основе платформ аппаратного и программного обеспечения.

Рисунок III.6 – Асимметричное шифрование



III.2.1.4 Система управления ключами

Инфраструктура открытых ключей (PKI) используется для реализации систем шифрования. Основными поддерживаемыми функциями являются:

- генерирование уникальной пары ключей (секретный ключ + открытый ключ), распределение пары по объектам и хранение необходимой информации для управления этой парой, архивация ключей и процедур для поиска на случай, если пользователь потеряет ключ или правоохранительные органы потребуют выдачи сведений;
- управление цифровыми сертификатами, а также создание, подписание, выпуск, подтверждение, аннулирование и обновление сертификатов;
- распространение открытых ключей надежным ресурсам запросов;
- сертификация открытых ключей (подписание цифровых сертификатов).

III.2.1.5 Цифровые сертификаты

Цифровой сертификат – это цифровая идентификационная карта объекта (юридического или физического лица) или информационного ресурса, предмета сертификации. Он содержит, среди всего прочего, идентификационную информацию субъекта (держателя), открытый ключ, назначенный этому субъекту и идентификационную информацию организации, выпустившей этот цифровой сертификат.

В стандарте X.509 (структурная аутентификация Справочника) предлагается архитектура структуры для создания службы аутентификации на основе использования цифровых сертификатов, и определяется структура и формат цифрового сертификата. Эта стандартизованная структура присутствует во многих решениях на рынке (рисунок III.7).

Рисунок III.7 – Основные элементы цифрового сертификата X.509v3

Версия
Серийный номер
Алгоритм подписи
Название выпускающей организации Пара серийный номер/выпускающий должна быть уникальной
Достоверность
Имя субъекта
Открытый ключ субъекта
Дополнительная информация, касающаяся субъекта или механизмов шифрования
Подпись сертификата Алгоритм и параметры подписи, а также действительная подпись

Для подтверждения полученного сертификата клиент должен получить открытый ключ объекта, выпустившего данный сертификат в отношении алгоритма подписи, и расшифровать подпись. Используя данную информацию, клиент вычисляет значение хэш-функции и сравнивает его со значением в последнем поле данного сертификата. Если два значения совпадают, происходит аутентификация сертификата. Затем клиент удостоверяется, что период действия данного сертификата является верным.

При управлении доступом, основанном на цифровых сертификатах, к данному серверу может подключиться большое количество пользователей. Управление осуществляется на основе информации, содержащейся в цифровом сертификате клиента. Таким образом, сервер принимает на веру данные о достоверности сертификатов и способах их создания, что создает лазейку к системе безопасности, поскольку есть вероятность повреждения сервера сертификатов или даже создания поддельного цифрового сертификата. Более того, проверить достоверность сертификата нелегко. Аннулирование сертификата – чрезвычайно трудоемкая задача, поскольку информацию нужно передавать всем участникам и регистрировать списке аннулированных сертификатов (CRL). Сертификат должен быть аннулирован при любом изменении его содержания (например, когда информация в сертификате устаревает, произошло повреждение секретного ключа пользователя, пользователь покидает компанию и т. д.). Систематическое обращение к соответствующей базе данных замедляет процесс управления доступом и уменьшает доступность серверов, включая доступность для авторизованных пользователей.

III.2.1.6 Доверенная третья сторона

Как бы ни называлась такая организация – доверенная третья сторона (trusted third party (TTP)), орган регистрации, орган сертификации или орган безопасности – основной функцией организации, создающей инфраструктуру открытых ключей, является выпуск сертификатов, подтверждающих открытый ключ, назначенный объекту (идентифицировать сертификат).

Клиент заполняет запрос на регистрацию (запрос сертификации) в сертификационной организации (служба регистрации в интернете). Сервер регистрации может запросить подтверждение идентификационной информации клиента согласно процедурам идентификации и аутентификации, осуществляемым данной организацией. После подтверждения данной информации сертификационный сервер генерирует ключи шифрования и создает цифровой сертификат на имя клиента, подписывает сертификат своим секретным ключом (сертификация цифрового сертификата) и отправляет данный сертификат клиенту. Клиент будет использовать открытый ключ данной организации для подтверждения того, что данный сертификат на самом деле был выпущен данной организацией.

Орган сертификации – это доверенная третья сторона, выпускающая цифровые сертификаты и служащая для подтверждения достоверности определенной информации.

III.2.1.7 Недостатки и ограничения инфраструктур открытого ключа

Наличие нескольких органов сертификации создает проблемы в отношении взаимного распознавания сертификатов из взаимодействия, совместимости и пределов достоверности сертификатов. Тем не менее, нежелательно, чтобы был только один глобальный орган сертификации ввиду чрезмерных полномочий, которые будут фактически возложены на эту организацию, а также величины инфраструктуры, которую необходимо будет создать. Существует настоящая нехватка доверия со стороны пользователей в отношении таких органов сертификации, которые обычно находятся за рубежом (Достоверность сертификатов? Гарантии безопасности? Защита личных данных? И т. д.)

Ограничения, свойственные инфраструктурам открытых ключей (PKI), основаны на:

- сложности инфраструктуры и стоимости развертывания и управления ею;
- высоком уровне безопасности, который требуется для установки службы PKI;
- достоверности, сроке действия сертификатов.

Потенциальные проблемные участки в реализации услуг PKI включают в себя:

- Политические проблемы: Большинство инфраструктур PKI – органов сертификации – принадлежат американским объектам (США). Это ставит вопрос о характеристиках работы и вопрос о доверии этим объектам в отношении предоставляемых услуг (создание, хранение и распространение открытых и секретных ключей, идентификационной информации, подтверждение подлинности ключей), недостатке гарантий в отношении возможного неправильного использования данных, нейтралитете при обмене информацией и возможности обращения за помощью в случае спора с органом сертификации.
- Технические проблемы: Традиционные системы шифрования могут быть взломаны, некоторые цифровые сертификаты не дают гарантий безопасности, возможна подделка сертификатов, безопасность инфраструктуры обеспечивается при помощи традиционных средств безопасности, которые можно легко обойти. Кроме того, использование инфраструктуры ключей отодвигает проблему безопасности обменов, на самом деле, не решая ее.
- Организационные проблемы: Взаимодействие инфраструктур, развертывание, управление, поддержка, безопасность, сложность и т. д.

III.2.1.8 Подпись и аутентификация

Отправитель зашифровывает сообщение при помощи своего секретного ключа. Любой объект, знающий открытый ключ отправителя сможет расшифровать данное сообщение, тем самым подтверждая факт того, что оно на самом деле было создано при помощи соответствующего секретного ключа.

Документ может быть подписан (цифровая подпись) в электронном виде при помощи использования алгоритма шифрования открытым ключом, следующим образом:

- создание сообщения, заявляющего об идентичности отправителя – подпись (например, "Меня зовут Альфа Танго Чарли") – которое зашифровывается при помощи секретного ключа отправителя и присоединятся к передаваемому сообщению;
- сообщение и его подпись зашифровываются при помощи открытого ключа получателя, и передается;
- получатель расшифровывает сообщение при помощи своего секретного ключа и отделяет подпись, которую он расшифровывает при помощи открытого ключа отправителя.

Однако мы должны быть осторожны, так как нет препятствий, для того чтобы кто-либо мог повторно использовать цифровую подпись сообщения вместо настоящего отправителя. Также можно создать цифровую подпись в месте нахождения партнера, украв его секретный ключ. Для того чтобы повысить уровень безопасности цифровой подписи, подпись формируется из содержания сообщения, что гарантирует целостность сообщения и аутентификацию отправителя.

III.2.1.9 Целостность данных

Проверить, не вносились ли в данные изменения во время передачи, можно путем присоединения к сообщению профиля сообщения, который передается одновременно с данными. Профиль формируется в результате применения к данным хэш-функции. Получатель высчитывает значение хэш-функции полученных данных, используя ту же функцию. Если есть какое-либо расхождение в полученных значениях, можно предположить, что данные были изменены. Можно зашифровать сам профиль до пересылки или хранения данных.

Как симметричная, так и асимметричная системы шифрования могут определить, вносились ли изменения в передаваемые данные, потому что в таком случае, данные невозможно расшифровать. Это помогает проверять целостность, но не может помочь подтвердить, что данные не были полностью уничтожены.

Для более эффективного контроля целостности к первоначальному сообщению применяется функция, которая преобразует его в короткую случайную последовательность битов, составляющую разновидность цифровой контрольной суммы файла (профиль).

Так называемая односторонняя хэш-функция генерирует профиль сообщения, т. е. его контрольную сумму, которая короче, чем первоначальное сообщение, и необъяснима. Затем она зашифровывается при помощи секретного ключа отправителя и присоединяется к передаваемому сообщению. После получения этого сообщения и контрольной суммы получатель расшифровывает контрольную сумму при помощи открытого ключа отправителя, пересчитывает контрольную сумму полученного сообщения, используя ту же самую хэш-функцию, и сравнивает ее с полученной контрольной суммой. Если результат такой же, это значит, что получатель подтвердил подлинность отправителя и убедился в целостности сообщения, поскольку, если в сообщение были внесены изменения, даже незначительные, его контрольная сумма значительно изменится.

Используя комбинацию методов шифрования, цифровой подписи и контрольной суммы, можно гарантировать целостность данных. Эти процедуры требуют значительного времени на обработку и замедляют работу операционной среды.

III.2.1.10 Неотказуемость

Служба неотказуемости была создана для предотвращения отказа или отрицания того, что сообщение было отправлено или получено или что транзакция имела место. Неотказуемость дает возможность доказать, например, что объект связан с данным действием или событием.

Неотказуемость основывается на простой подписи или идентификации, подтверждающей, кто создал данное сообщение. Эта услуга может предоставляться посредством алгоритма шифрования открытым ключом. В качестве кибернотариуса может быть также привлечена доверенная третья сторона.

III.2.1.11 Ограничения решений безопасности, основанных на шифровании

Доверие при решениях шифрования на рынке может быть только относительным, поскольку гарантий или средств проверки не существует (Существование лазеек в программном обеспечении? Дублирование, разглашение секретных ключей? И т. д.). Также нет доказательства того, что алгоритмы, в настоящее время считающиеся надежными, останутся такими же и в будущем.

III.2.2 Защищенный IP протокол

Необходимость удовлетворения требованиям безопасности свидетельствовала в пользу пересмотра 4 версии протокола Интернет. Кроме того, также появилась необходимость обеспечивать более широкий круг адресов и увеличить число доступных интернет-адресов, а также обеспечить динамическое распределение пропускной способности для поддержки мультимедийных приложений. В результате была создана переработанная версия IP протокола, названная "протоколом Интернет следующего поколения" (IPnG), или IP версии 6 (Pv6)[37].

III.2.2.1 Протокол IPv6

В 1994 году[38], Совет по архитектуре интернета (IAB)[39] рассмотрел требования безопасности IP протокола. Версия 6 IP протокола (IPv6) включает в себя возможности аутентификации и обеспечения конфиденциальности.

Основные усовершенствования в IPv6 по сравнению с IPv4 относятся к следующим пунктам [RFC 2460]:

- расширенное адресное пространство и иерархия адресов: размер адреса увеличен с 32 битов (4 байтов) до 128 битов (16 байтов); адреса представлены в шестнадцатеричной системе счисления[40], каждые два байта отделяются двоеточием (например, 0123:4567:89ab:cdef:0123:4567:89ab:cdef), вместо десятеричной системы счисления – отделение точками;
- возможность динамического распределения пропускной способности для поддержки мультимедийных приложений;
- возможность создания виртуальных IP сетей;
- поддержка процедур аутентификации и шифрования с использованием заголовков опций;
- упрощение заголовков пакетов для облегчения и ускорения маршрутизации.

Принятие IPv6 предусматривает, среди всего прочего, изменение адресации и механизма управления адресами[41], установки во всей интернет среде систем, поддерживающих IPv6, систем, работающих с обеими версиями, полномасштабной синхронизации изменения версии и т. д.

По этим причинам версия 6, созданная еще в 1995 году, пока в значительной степени не распространена, и, кажется, ни один правительственный стимул или международная рекомендация не могут обеспечить принятие версии 6 данного протокола по всей сети. IPv6 установили только несколько частных инфраструктур.

Реализация нового протокола Интернет (IPv6) со встроенными функциями безопасности, редка. Поэтому, чтобы удовлетворить требованиям безопасности сети, интернет сообществом было разработано и принято промежуточное решение, называемое IPSec[42], совместимое как с IPv6, так и с IPv4. В 1995 году Комитет по инженерным проблемам интернета (IETF)[43] издал несколько документов (RFC с 1825 по 1829), где определяются пути обеспечения безопасности инфраструктуры интернета.

---

[37] IPv6: RFC 1883 1995 года, заменен RFC 2460 в декабре 1998 года – www.ietf.org/rfc/rfc2460.txt.

[38] RFC 1636: Отчет Семинара IAB по безопасности архитектуры интернета, 8–10 февраля 1994 г.

[39] www.iab.org/

[40] Алфавит шестнадцатеричной системы счисления (основа 16): 0 1 2 3 4 5 6 7 8 9 A B C D E F

[41] В RFC 1886, определенном в 1995 году, необходимо сделать изменения в DNS для поддержки IPv6.

[42] RFC 2401 – www.ietf.org/rfc/rfc2401.txt.

[43] www.ietf.org.

III.2.2.2 Протокол IPSec

При помощи IPSec можно сделать конфиденциальным содержание пакетов, передаваемых протоколом. IPSec предлагает конфиденциальность данных и услуги аутентификации на уровне передачи IP протоколом, посредством вставки заголовка аутентификации (AH) или заголовка безопасного закрытия содержания (ESP).

Каждое приложение вне зависимости от того, какой тип трафика оно генерирует, может использовать данные услуги безопасности без какой-либо адаптации. IPSec работает в режиме "точка-точка" (безопасность данных между отправителем и получателем обеспечивается за счет безопасного соединения между ними).

Заголовок аутентификации обеспечивает услуги по аутентификации и целостности IP пакета, таким образом, гарантируя, что данные не были изменены во время передачи и что адрес источника на самом деле такой же, как и указано в данном пакете.

Заголовок безопасного закрытия содержания делает возможной реализацию механизмов шифрования (симметричное шифрование такое, как DES, Тройной DES, RC5 или IDEA) и предлагает услуги аутентификации, аналогичные тем, что предоставляет заголовок аутентификации.

Алгоритмы шифрования используют ключи, которые нужно генерировать и распространять. Таким образом, управление ключами шифрования является важной задачей, которую необходимо выполнять при реализации решений на основе IPSec. Например, протоколы обмена ключами включают в себя: протокол определения ключей Окли (Oakley key determination protocol)[44], основанный на алгоритме обмена ключами Диффи-Хэллмана [RFC 2412]; протокола установления безопасных интернет-соединений и управления ключами (ISAKMP) [RFC 2408]; протокол обмена ключами через интернет (Протокол IKE) [RFC 2409].

III.2.2.3 Виртуальные частные сети

При установке протокола IPSec в точках доступа к сети интернет между этими точками можно установить канал связи с аутентифицированными конечными точками (рисунок III.8).

Эти конечные точки расположены в системах организации и, таким образом, защищены физически. Согласно выбранному варианту, данные, передаваемые по соединению, могут быть зашифрованы. Другими словами, между двумя точками ненадежной инфраструктуры можно создать безопасный маршрут (это концепция виртуальной частной сети). Следует заметить, что слово "сеть" в выражении "виртуальная частная сеть" употреблено не совсем правильно, поскольку создается только (виртуальное) логическое соединение.

III.2.3 Безопасность приложений

Большинство приложений имеют защищенную версию, что обычно допускает аутентификацию корреспондентов и шифрование передаваемых данных.

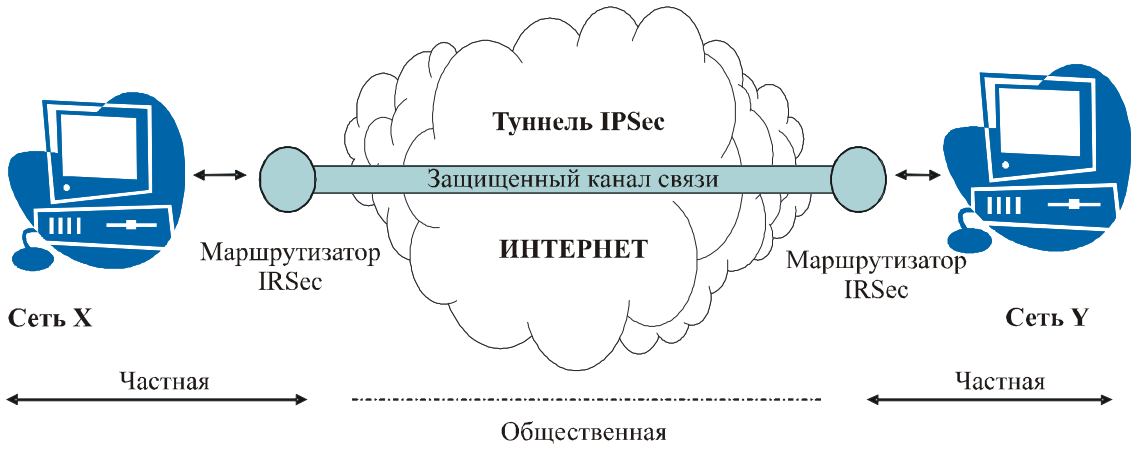
Альтернативой установке новых защищенных версий протоколов приложений является установление общего механизма безопасности, предлагающего общие услуги безопасности для всех приложений. Сейчас широко используется программное обеспечение протокола безопасных соединений (SSL), в особенности для коммерческих транзакций через интернет.

Интенсивное использование гипертекстовых документов, а также загрузки содержания, как активного, так и пассивного, создает многочисленные проблемы безопасности, относящиеся, помимо всего прочего, к источнику, автору, подлинности, вредоносности и т. д. Начинает появляться некоторая реакция на этот новый аспект безопасности информационных систем: техники цифровой подписи XML документов, "водяные знаки", управление электронными правами так, чтобы обеспечить некоторую стабильность в отношении безопасности. Нужно поддерживать заданный уровень безопасности, даже если защищаемый объект выпадает из физических границ среды, в которой обычно происходит управление его безопасностью.

---

[44] Протокол определения ключей Окли: RFC 2412 – www.ietf.org/rfc/rfc2412.txt.

Рисунок III.8 – Создание VPN с использованием канала связи IPSec



III.2.4 Протокол-слой безопасных соединений (SSL) и защищенный протокол передачи гипертекста (HTTP) (S-HTTP)

Протокол-слой безопасных соединений (SSL) – это программное обеспечение, гарантирующее безопасность обменов приложениями. Этот протокол поддерживается большинством веб-браузеров на рынке.

Аутентификация двух связывающихся объектов в соединении SSL происходит посредством процедуры сертификации и доверенной третьей стороны. Затем они согласуют уровень безопасности, который будет применяться к данной передаче данных. Передаваемые данные зашифровываются для соединения SSL (рисунок III.8).

Установка SSL оказывает большое влияние с точки зрения сервера на учетные записи требуемой сертификации, что делает необходимым диалог с общепринятым органом сертификации и также требует, чтобы переключатели защитной системы поддерживали работу SSL. Сертификация иногда рассматривается как помеха, затрудняющая развертывание данного решения.

Расширения к протоколу HTTP (защищенный HTTP, или S-HTTP) являются альтернативным решением, разработанным ассоциацией CommerceNet. S-HTTP дает те же возможности безопасности, что и SSL, с теми же ограничениями по сертификации, но поддерживает только потоки данных HTTP. Это решение распространено повсеместно.

III.2.5 Электронная почта и безопасность сервера имен

Риски безопасности, возникающие при использовании электронной почты, относятся к:

- потере, перехвату, изменению или уничтожению сообщения;
- инфицированию системы при помощи сообщений, содержащих вирусы, червей или "Троянских коней";
- причинению беспокойства: бомбардирование сообщениями, почтовый "мусор", спам, затрагивающий людей, чей адрес электронной почты используется без их предварительного согласия и с которыми отправитель (спаммер) никогда не входил в контакт. Спам, вызывающий массовое распространение инфицированных сообщений, может способствовать быстрому распространению вирусов (спам + вирус), причем механизмы взаимодействия с электронной почтой уже включены в код вируса, поэтому они распространяются самостоятельно;

– краже идентификационной информации (нападающий притворяется кем-то другим, системный компонент передает, прослушивает или перехватывает сообщения, не адресованные ему, и т. д.);

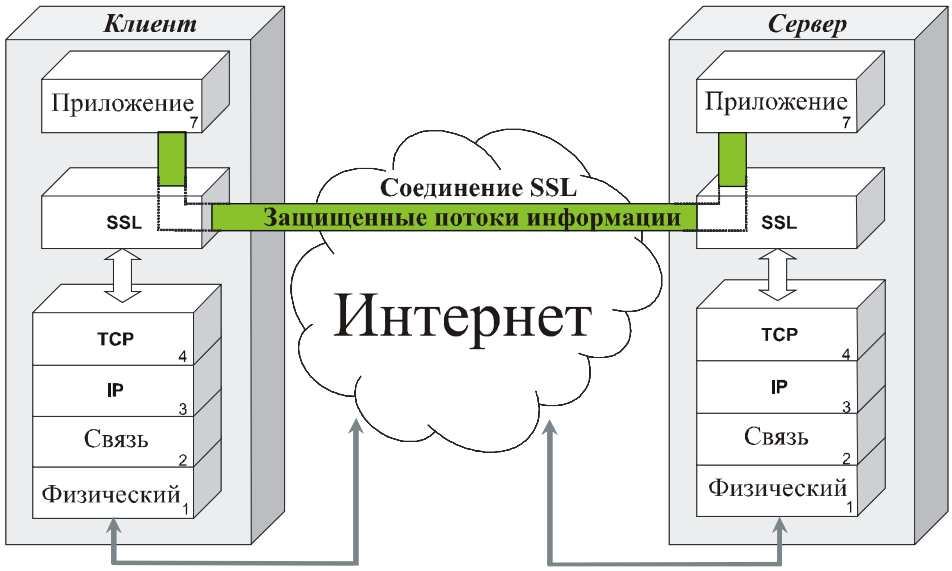
– вставке, смешению, удалению или задержке сообщений;

– отказу в предоставлении услуги на основании неисправного компонента в цепочке системы сообщений;

– обнародованию конфиденциальной информации;

– отказу (часть системы отрицает факт отправки или получения сообщения).

Рисунок III.8 – Архитектура SSL (протокол-слой безопасных соединений*)*



К этому еще нужно добавить все угрозы, связанные с сетями и работой в них (атаки на уровне маршрутирования, серверов имен и т. д.).

Для того чтобы преодолеть эти ограничения безопасности, свойственные функциям электронной почты, в новые версии программного обеспечения включены возможности шифрования для обеспечения конфиденциальности, целостности и аутентичности передаваемой информации и корреспондентов.

Требования безопасности для систем электронной почты относятся к:

– конфиденциальности и целостности (сообщения, последовательности сообщений);

– неотказуемости (подтверждение отправки, подтверждение получения, подпись, сертификация сообщения);

– аутентификации подлинности всех участников системы электронной почты (пользователей, промежуточных элементов, памяти сообщений, агентов пересылки сообщений и т. д.).

Самым большим риском, возможно, является заражение вирусом, червем или "Троянским конем" через сообщение. Одним из методов предотвращения этого является установка анти-вирусного программного обеспечения на каждую систему для обнаружения вирусов и, если возможно, их лечения. Антивирусное программное обеспечение будет обнаруживать только те вирусы, для которых оно разработано, но не обеспечит защиты от новых форм заражения. Кроме того, постоянная необходимость в обновлении баз вирусов представляет серьезную проблему управления.

Другим вариантом является создание карантинного сервера, который будет тщательно сканировать все получаемые сообщения вместе с приложениями. Если использовать несколько антивирусных программ, работающих параллельно, шансы обнаружения инфицированного сообщения значительно увеличатся.

Первоначальный протокол, использовавшийся для пересылки электронной почты в интернете, называемый "простым протоколом пересылки электронной почты" (SMTP), с течением времени был переработан так, чтобы поддерживать мультимедийное содержание сообщений, а также механизмы безопасности. Примерами таких протоколов являются S/MIME (защищенные/многоцелевые расширения электронной почты в интернете), PEM (электронная почта повышенной секретности) и PGP (очень хорошая конфиденциальность).

Интернет приложения опираются, прямо или косвенно, на работу системы серверов доменных имен (DNS), в которой DNS сервера соотносят логические имена с соответствующими IP адресами. DNS играют ключевую роль в гарантировании того, что информация направляется по верному маршруту. По этой причине они являются достаточно чувствительными компонентами архитектуры связи и требуют дополнительной защиты. Для предотвращения фальсификации информации, хранящейся на серверах, созданы механизмы безопасности (контроль доступа, аутентификация, регистрация данных, дублирование, согласованность, шифрование запроса и ответа и т. д.). Информацию могут фальсифицировать с целью перенаправления информации непредусмотренным получателям, атак типа "отказ в облуживании", вызывающих перегрузку сервера или фатальные сбои в сети из-за потока поддельных запросов, и создания фиктивных серверов имен, что ведет к получению неверных ответов, ошибкам передачи или вторжению.

III.2.6 Обнаружение вторжения

Вторжения, инциденты и аномалии нужно обнаруживать и идентифицировать как можно скорее и тщательно с ними бороться, чтобы гарантировать, что данные системы продолжают нормально функционировать и остаются защищенными.

Инцидент – это событие, которое происходит неожиданно. Хотя инциденты сами по себе по большей части не очень серьезны, тем не менее, они имеют тяжелые последствия. Аномалия – это исключительное происшествие, которое может привести к ненормальному функционированию информационной системы и нарушение действующей политики безопасности. Причины аномалии могут быть случайными (например, ошибка конфигурации) или предумышленными (направленная атака на информационную систему). Вторжение является характерной чертой атаки или может расцениваться как инцидент или аномалия.

Обнаружение вторжения относится к набору действий и механизмов, используемых для обнаружения ошибок, которые могут привести к нарушениям политики безопасности, а также для диагностирования вторжений и атак (оно включает обнаружение аномалий и неправильного использования)[45].

Система обнаружения вторжений (IDS) включает в себя три основных функциональных, а именно: сбор данных, анализ данных, а также обнаружение вторжения и реакцию.

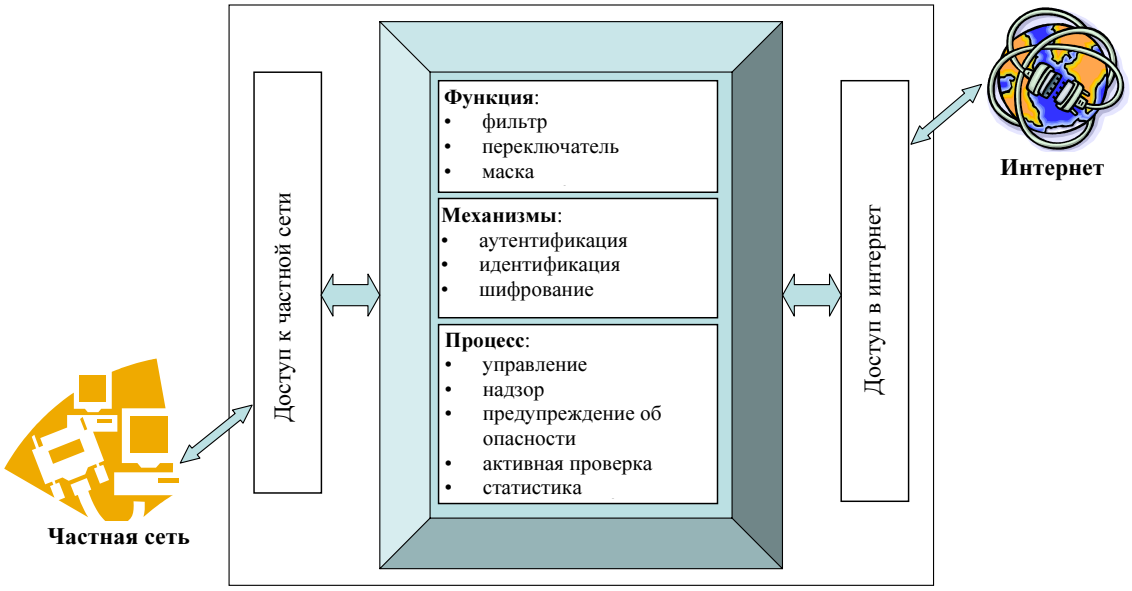
III.2.7 Разделение среды

Отделение и экранирование частной среды от общего интернета достигается путем установки одной или более защитных систем (firewall).

[45] Д. Алессандри и др. "К таксономии систем обнаружении вторжения и атак": www.domino.watson.ibm.com/library/cyberdig.nsf/papers/5FA980EB952E09D085256AC600535997/$File/rz3366.pdf

Защитная система – это система для фильтрации и, в некоторых случаях, блокирования потоков данных. Система анализирует поток, авторизует его, если он удовлетворяет определенным условиям, или, в противном случае, отклоняет его. При помощи разделения окружения можно создать отдельные IP окружения, если сделать точки доступа к сети, которую нужно разделить, физически независимыми друг от друга. Это позволяет взаимодействовать двум сетям, имеющим разные уровни безопасности (рисунок III.9)[46].

Рисунок III.9 – Функциональная структура защитной системы



В зависимости от характера анализа и выполняемой обработки существуют различные типы защитных систем. Защитные системы обычно делятся в зависимости от обеспечиваемого уровня фильтрации данных: уровень 3 (IP), уровень 4 (TCP, UDP) или уровень 7 (FTP, HTTP и т. д.) модели OSI.

Защитная система приложений, также известная как прокси (прокси-сервер, защитная система-прокси), выступает в качестве переключателя приложений. Действуя со стороны пользователя, она создает требуемую услугу. Целью соответствующей системы-рокси является предоставление маски подсети при помощи переключателя приложений, а также обеспечение прозрачности внутреннего окружения организации. Система–прокси – это обязательная точка пересечения для всех приложений, требующих доступа в интернет. Данная система требует установки приложения переключения на рабочую станцию пользователя и на защитную систему.

Установка и конфигурирование защитной системы основываются на архитектуре сети, выбранной так, чтобы она удовлетворяла требованиям безопасности и управления при соединении с различными системами.

Защитная система – это один из инструментов, используемых для реализации политики безопасности, и всего лишь компонент аппаратного и программного обеспечения, используемого для этой цели, поскольку защитная система сама по себе не обеспечивает адекватной защиты сетей и систем организации. Защитная система должна использоваться совместно с инструментами, мерами и процедурами, сопутствующими целям безопасности, определенным в соответствии с политикой

[46] Рисунок взят из "*Sécurité informatique et télécoms: cours et exercices corrigés*"; С. Гернаоути-Хелие, Дюно, 2006 год.

безопасности. Эффективность защитной системы будет во многом зависеть от ее позиции относительно защищаемых систем, а также от ее конфигурации и управления.

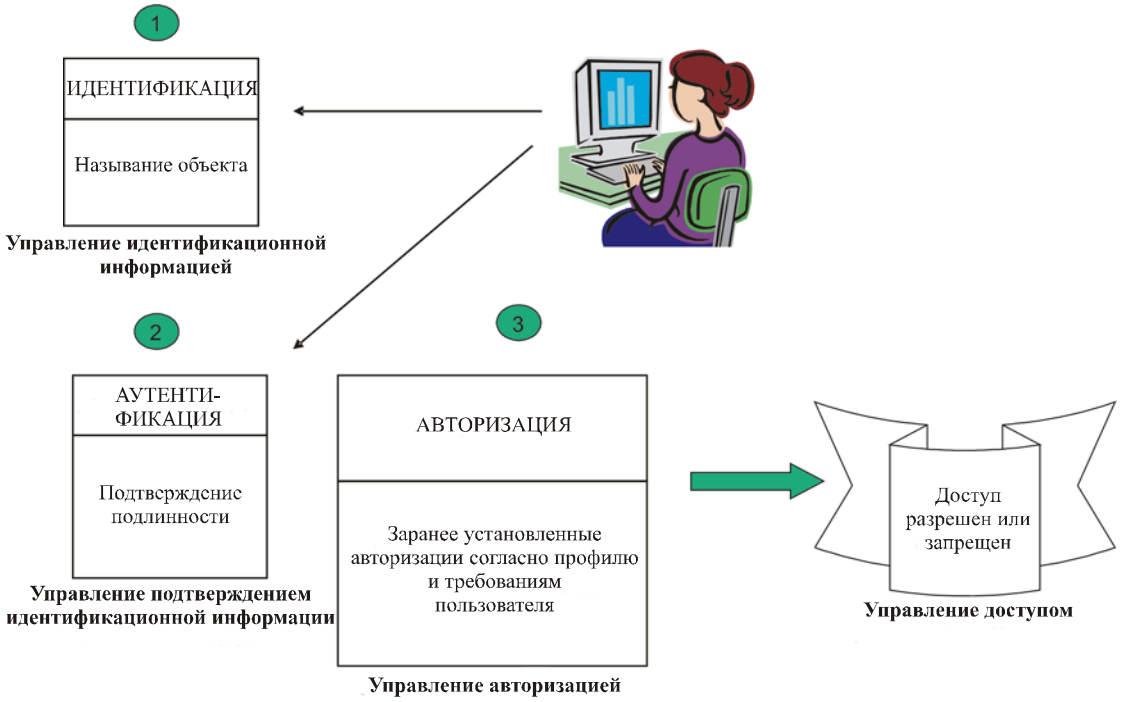
Хотя защитная система и системы обнаружения вторжения могут предоставлять определенные услуги безопасности, их одних недостаточно для обеспечения полной защиты информационных ресурсов.

III.2.8 Управление доступом

III.2.8.1 Общие принципы

Механизм логического управления доступом, основанный на идентификации и аутентификации частных лиц, а также на разрешениях или правах доступа, предоставляемых им, служит для ограничения доступа к информационным ресурсам (рисунок III.10).

Рисунок III.10 – Основные компоненты логического управления доступом



На основе аутентифицированной идентификации, механизм управления доступом дает доступ к запрашиваемым ресурсам согласно параметрам (профилю) пользователя. Это предполагает, что управление идентификационной информацией, управление подтверждением идентификационной информации и управление авторизацией эффективно выполняются по отношению к пользователю.

Профиль (параметры) пользователя содержат все данные, на которых основываются решения об авторизации доступа. Профиль должен быть определен в соответствии с политикой управления доступом.

Целью аутентификации является соединение понятия об идентификационных данных с данным частным лицом. Авторизация доступа вызывает выборочную фильтрацию запросов доступа к ресурсам и услугам, предоставляемым сетью, для того чтобы разрешать доступ только правильно авторизованным объектам.

Целью службы аутентификации является проверка того, что указанные идентификационные данные являются подлинными (подтверждение подлинности). Это, как правило, будет зависеть от одного или более следующих факторов:

– секрет, известный данному объекту, т. е. пароль или личный номер (PIN);
– элемент в собственности объекта (карта, маркер и т. д.);

– свойство, присущее только данному объекту (отпечаток пальца, отпечаток голоса, отпечаток сетчатки и т. д.).

Проверка подлинности соответствует сценарию, в котором объект, запрашивающий доступ, заявляет о своей подлинности и предоставляет элемент доказательства, которым, как предполагается, обладает только он один (например, пароль, конфиденциальный ключ, отпечаток пальца). Затем служба аутентификации сравнивает эту информацию с данными, хранящимися на ее сервере аутентификации.

Сервер аутентификации должен быть чрезвычайно хорошо защищен при помощи специальных механизмов, обеспечивающих управление доступом и управление защищенными системами и при помощи шифрования находящихся на нем данных. Сервер аутентификации не должен быть подвержен ошибкам, поскольку общая безопасность информационной и телекоммуникационной инфраструктуры зависит от качества ее работы.

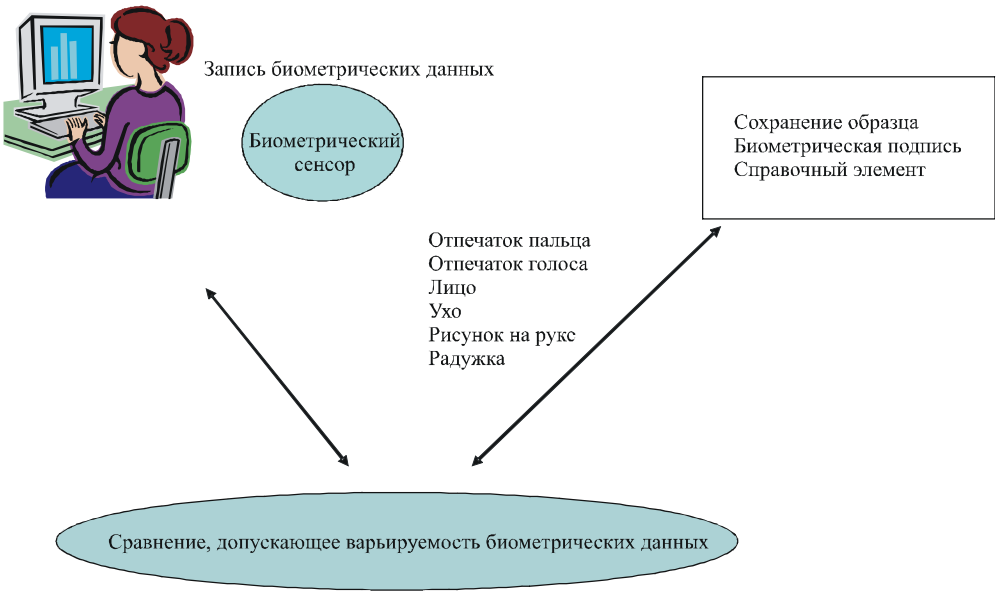
III.2.8.2 Положительные стороны и ограничения биометрии

Биометрическая индивидуализация состоит в использовании биометрических данных для проверки подлинности частных лиц в точке доступа к оборудованию или в рамках судебного контроля (полицией и т. д.).

Используя биометрию для управления доступом к информационным ресурсам можно отказаться от пароля, заменив его физической характеристикой, из которой можно легко извлечь значение двоичных данных.

Для того чтобы использовать физические характеристики частных лиц с целью идентификации их и подтверждать их идентификацию, сначала необходимо извлечь и записать их биометрические характеристики в форме "биометрического образца". Такие записи должны быть высоко надежными и защищенными (рисунок III.11).

Рисунок III.11 – Биометрическое управление доступом



Продолжительность процесса аутентификации может быть большой, поскольку фаза сравнения должна учитывать вариации, свойственные живой природе сравниваемых данных. Например, образец голоса никогда не будет полностью идентичным. Сравнение основывается на статистической и вероятностной обработке биометрических данных. Неопределенность, включаемая в систему аутентификации, означает, что никогда нельзя быть полностью уверенным в результате аутентификации, т. е. система не может со 100-процентной вероятностью определить, что персона "x" – это тот или та, за кого себя выдает. Уровень ошибок таких систем все еще высок, что делает невозможным высокий уровень безопасности. В комбинации с "традиционными" механизмами

аутентификации, основанными на паролях (двойное подтверждение), биометрическая сторона служит для повышения предоставляемого уровня безопасности.

Все большее использование биометрических технологий вызывает многочисленные вопросы этического и эргономического характера, не говоря уже об экономическом, юридическом и техническом аспектах. Такие вопросы включают в себя:

- конфиденциальность биометрических данных, которые могут считаться секретными;
- случаи, когда биометрические данные могут не быть уникальными (идентичные близнецы);
- факт того, что большинство пользователей считают сенсоры биометрических данных навязчивыми и отказывается от них в случаях, когда есть выбор. Также сенсоры создают угрозу свободе частного лица, например, большое количество сенсоров, таких как видеокамеры, установленные в общественных местах и работающие без ведома людей;
- случаи кражи идентификационной информации или незаконного или мошеннического использования биометрических данных.

Из-за недостатка точности и продолжительных высоких издержек на покупку, развертывание и работу решения управления доступом, основанные на использовании биометрических данных, не находят сейчас широкого использования.

Резюме ограничений, возникающих при использовании биометрических данных для управления доступом:

1 Биометрические данные, используемые при идентификации частного лица, изменятся со временем.

2 Биометрические данные нужно собирать и преобразовывать в контрольный образец для хранения в базе данных. Поскольку данные преобразуются в цифровой формат, они становятся уязвимыми (и, следовательно, поддаются изменению), поэтому им нужно обеспечить наилучшую защиту. Для каждого запроса доступа, необходимо записывать биометрические данные пользователя; это создает проблему принятия метода записи и связанного с ним ощущения вмешательства, которое во многих случаях нежелательно

3 Управление доступом, основанное на биометрических данных, не является отказоустойчивым на 100% из-за изменчивости анализируемого человеческого образца во время процесса аутентификации. Согласно используемой системе вероятность неверной положительной или неверной отрицательной идентификации может быть относительно высокой и будет зависеть от технологии, используемой для записи биометрических данных, и качества работы.

III.2.9 Защита инфраструктур связи и управление ими

III.2.9.1 Защита

Физический уровень (уровень 1) может способствовать безопасности передач при помощи линейного кодирования, т. е. передачи неважной информации, для того чтобы замаскировать поток важных данных внутри непрерывного потока неважных данных. Однако если возникнет необходимость защитить передачи от пассивного прослушивания путем фиксации электромагнитного излучения, вызываемого сигналом, передаваемым по среде передачи, последнюю нужно будет полностью изолировать в клетках Фарадея. Очевидно, что такую меру защиты нужно вводить только при особой необходимости.

Физическую защиту среды передачи, распределительные щиты и оборудование соединения нужно правильно устанавливать и обслуживать.

Инфраструктуру передачи нужно защищать от любой формы излучения, которая может подвергнуть процесс передачи данных опасности, а также от пассивных (отслеживание данных) или активных (модификация, разрушение или создание данных) атак.

Знания о том, как защитить соединения пользователя представляют особую важность. С этой целью их нужно идентифицировать (кто является пользователями?), установить их местоположение (где они находятся?) и идентифицировать их требования (каковы передаваемые потоки приложений?). Ответив на основной вопрос "кто, что и где делает?", можно идентифицировать различные требования безопасности, относящиеся к транспортной сети.

Обеспечение безопасности передачи данных состоит в интегрировании процесса безопасности в инфраструктуру связи, которая должна быть способна принять этот процесс во всей его полноте. Чаще всего это требует обновления всех маршрутизаторов – ситуация, которая в некоторых случаях может привести к проблемам взаимодействия маршрутизаторов и управления изменениями.

Кроме того, в результате шифрования данных на уровне "сети" получаются пакеты данных, больше незашифрованных пакетов по размеру. В результате передача таких пакетов занимает большую часть пропускной способности и ресурсов связи. Если учесть то, что процесс шифрования увеличивает время обработки пакета, реализация безопасности на этом уровне может заметно повлиять на показатели работы сети.

Основным преимуществом шифрования на уровне инфраструктуры сети является независимости приложений и механизмов шифрования, связанных с передачей, которые таким образом полностью прозрачны для пользователя.

Безопасность передачи на уровне приложений (шифрование данных как можно ближе к приложению, обрабатывающему данные), напротив, модифицирует само приложение. При этом данные зашифровываются в восходящем направлении при их доставке к протоколу сети, который направит их к месту назначения, где они будут расшифрованы принимающим сервером приложений. Именно во время фазы установления диалога между объектами приложений (например, клиент и сервер) происходит аутентификация и согласование ключа сеанса связи. Сложность этой фазы может меняться, также как и время установления связи. Однако после завершения установления связи шифрование происходит довольно быстро. Шифрование не зависит от исполнительной платформы и инфраструктуры связи.

Защита на уровне рабочей сферы пользователя, реализующего распределенное приложение, больше зависит не от носителя данных или сети, а от текущего окружения пользователя. Трудность защиты приложений состоит в том, что предоставляемая защита должна включать в себя все окружение приложения, рабочую станцию пользователя (а не только само приложение) и, в качестве расширения, физическое окружение пользователя (доступ к оборудованию и т. д.).

Защита приложений сводится к вопросу о правах отдельного пользователя в отношении рабочих станций, приложений и физической области, в которой они работают.

Основные функции операционной системы, установленной на рабочей станции пользователя, играют важную роль в этой защите (другие участники не могут взять на себя управление во время сеанса, автоматический разрыв соединения после определенного периода времени и т. д.). Защита также включает в себя защиту сетевой карты, поддержку протоколов приложения в защищенном режиме (передача защищенных файлов, безопасная отправка сообщений и т. д.) и зеркальное отображение и дублирование операций (защита данных путем их копирования на диск, операции записи и избыточность оборудования).

Обеспечение безопасности транспортной инфраструктуры или приложения состоит в решении одной и той же проблемы на различных уровнях:

- нужно аутентифицировать процессы и пользователей;
- отправитель и получатель используют одинаковый алгоритм шифрования/расшифровки;
- каждый объект, участвующий в соединении, должен обладать данным алгоритмом и ключами шифрования/расшифровки;
- нужно осуществлять управление ключами шифрования/расшифровки;
- данные нужно форматировать до передачи.

III.2.9.2 Управление

При правильной реализации деятельность по управлению системой и сетью может обеспечивать доступность и показатели работы, необходимые для достижения безопасности. Эта деятельность включает в себя надзор за сетью и обнаружение аномалий или инцидентов (например, вторжений) – задачи, составляющие основную часть общей безопасности сети и информационной системы.

Хорошее управление сетью помогает обеспечивать доступность инфраструктур, услуг и данных с высокой степенью эффективности. При помощи управления сетью, в особенности управления

конфигурацией, показателями работы и управления инцидентами, можно достичь обеспечить доступность и целостность как целей безопасности.

Кроме того, такой аспект управления сетью, как управление учетом сетевых ресурсов, делает доступными все данные, необходимые не только для выставления счета пользователям, но и для выполнения надзора и проверки, которые играют ключевую роль в вопросах безопасности. Оно может использоваться для контроля действий в контексте подтверждения или неотказуемости.

Управление сетью также способствует достижению конфиденциальности, поскольку оно гарантирует отсутствие отслеживания и незаконного доступа к данным. Функция управления доступом, являющаяся компонентом управления сетью, необходима для практической реализации безопасности.

Показатели работы, качество обслуживания, доступность и надежность сети в большой степени зависят от качества управления маршрутизаторами и оборудованием, обеспечивающим изменение маршрута в соответствии со статусом сети и запросами маршрутизации трафика. Обновление таблиц маршрутизации большинства сетей – настоящая головная боль администраторов сетей, поскольку необходимо синхронизировать любые изменения значений в таких таблицах, чтобы избежать сбоев в работе и потерь данных при передаче. Протоколы управления сетью созданы таким образом, чтобы, среди всего прочего, обновлять таблицы маршрутизации. Управление сетью может способствовать безопасности маршрутизатора путем создания защищенных точек доступа во время их конфигурирования, генерирования сигнализации об опасности в случае попыток вторжения и обеспечения безопасности управления маршрутизатором и центрами мониторинга.

Таким образом, для того чтобы предотвратить незаконное введение изменений пользователями, очень важно обеспечить необходимую защиту путем блокирования или обнаружения следующих действий:

- изменение адресов, содержащихся в таблицах маршрутизации, IP пакетах и т. д.;
- изменение маршрутов и незаконное копирование передаваемых данных;
- мониторинг потока;
- изменение маршрута пакетов, изменение самих пакетов или их разрушение;
- отказ в обслуживании, атака на маршрутизатор, перегрузка сети и т. д.

Очень важно обеспечить безопасности процессов, при которых данные направляются через сети электросвязи. Поставщики "сетевых" услуг должны защищать все объекты, участвующие в этом процессе, в особенности маршрутизаторы и сервера имен таким образом, чтобы качество услуг по маршрутизации удовлетворяло таким требованиям безопасности, как доступность (услуга работает), конфиденциальность (данные доставляются по назначению) и целостность (данные не изменяются во время передачи).

Службы сети не гарантируют доставку данных авторизованным участникам, поскольку служба доставки не проверяет, чтобы данные, доставленные по верному адресу, на самом деле доставлялись участникам, имеющим право на получение этих данных. Для этого необходимо проводить дополнительную проверку типа "управления доступом". Более того, если данные пересылаются в незашифрованном виде и прослушиваются при передаче, они могут стать доступными неавторизованной третьей стороне. В случаях, когда данные являются уязвимыми, их необходимо шифровать.

Управление информационной сетью предполагает постоянное наблюдение за ее работой. Целью такого наблюдения является не только обеспечение того, чтобы качество услуг в данной сети было приемлемым, но и обнаружение проблем, инцидентов, ошибок и аномалий, снижающих качество работы сети и подвергающих опасности ресурсы сети, что позволит быстро и соответствующим образом реагировать на них. Управление сетью допускает отслеживание действий и событий так, чтобы их можно было записывать для последующего анализа (это обычно называется проверкой). Управление сетью также помогает обеспечивать доступность ресурсов путем подтверждения того, что сеть работает правильно. Это является важнейшей функцией при управлении сетью, поскольку оно играет роль в управлении работой, инцидентами, конфигурацией, а также управлении пользователями и безопасностью.

ЧАСТЬ IV

Всесторонний подход

Раздел IV.1 – Различные аспекты законодательства, регулирующего новые технологии

IV.1.1 Защита личных данных и электронная коммерция[47]

В этом разделе обсуждается защита личных данных в той степени, в какой она имеет отношение к электронной коммерции, а также на основе ситуации во Франции и Швейцарии определяются основные тексты законов, которые должны знать системные администраторы и менеджеры по безопасности организаций, занимающихся электронной коммерцией. Таким образом, можно выделить основные принципы, на которых основывается ведение бизнеса в киберпространстве, и применить их к развивающимся странам.

IV.1.1.1 Электронная коммерция: то, что незаконно вне интернета, также незаконно и в интернете

Электронную коммерцию можно обсуждать с точки зрения электронного бизнеса, который ведется либо с потребителями (бизнес–потребитель (B2C)) либо между компаниями (бизнес–бизнес (B2B)). Например, электронное администрирование можно разделить таким же образом, т. е. электронный бизнес с другими гражданами или с частными или общественными организациями. Это разделение является важным с юридической точки зрения, поскольку торговое право различает транзакции, производимые между компаниями, и транзакции, производимые с потребителями.

В обеих ситуациях безопасность вместе с соответствующим интернет-маркетингом и стратегией продаж, реализуемая в соответствующих правовых рамках, является краеугольным камнем электронной коммерции. Прививая доверие, основанное на инструментах безопасности, и уважение к закону, создавая тем самым контекст, благоприятный для обмена данными, страны могут побудить широкую общественность принять информационные технологии и услуги электросвязи и в то же время развить настоящую постиндустриальную экономику.

Необходимость определить соответствующие правовые рамки для использования новых технологий привела к появлению новых законов, дополняющих существующее законодательство, большая часть которого может также применяться для киберпространства. Однако, что бы то ни было, то, что является незаконным вне интернета, незаконно и в интернете! Киберпространство является международным и не имеет территориальных границ. Поэтому очень сложно определить, под чью юрисдикцию подпадают юридические вопросы, касающиеся электронной коммерции. Вот почему при интернет-транзакциях нужно указывать границу предложения и предоставлять точную информацию, в чьей юрисдикции находятся спорные случаи.

IV.1.1.2 Обязанность защищать

Защита личных данных является ключевым аспектом электронной коммерции. Потребители должны знать о характере данных, собираемых, используемых и передаваемых интернет-рекламодателями или компаниями. Они должны знать заранее, как будут использоваться и передаваться касающиеся их данные и кто еще будет иметь к ним доступ. Потребителей также нужно проинформировать о мерах, предпринимаемых для защиты этих данных. Когда происходит транзакция, эффективная политика безопасности должна быть явно изложена, информацию о ней нужно легко находить, учитывать, обозревать и понимать. Информацию о политике безопасности необходимо опубликовать на веб-сайте компании.

Компания должна также предпринимать соответствующие меры безопасности для защиты данных клиентов при сборе и обработке. Она также должна удостовериться, что третьи стороны, участвующие в транзакциях, также удовлетворяют требованиям безопасности.

---

[47] Этот раздел был написан в сотрудничестве с Игли Таши, аспирантом-ассистентом в Университете Лозанны.

IV.1.1.3 Уважение основных прав

Конфиденциальность личных данных и цифровой приватности являются основными правами человека.

Пример Европейской директивы

Европейская директива по данному вопросу существовала с 1995 года, а в 1970-х годах несколько стран приняли национальное законодательство, касающееся защиты личных данных и контроля использования государственных архивов, содержащих информацию личного характера, для того чтобы избежать риска ненадлежащего или ненужного хранения личных данных.

Ситуация во Франции

Одним из примеров является французский *Loi informatique et libertés* [Акт об информационных технологиях и гражданских свободах], опубликованный в 1978 году и переработанный в августе 2004 года. В переработанной версии вводились юридические понятия, применимые к новым формам обработки, появившимся в информационном обществе и цифровой экономике. Эта директива замещает Директиву 95/46/ЕС от октября 1995 года. Целью данной Директивы является укрепление прав и защиты, предоставляемых физическим лицам, а также усиление обязательств, возложенных на тех, кто обрабатывает данные.

Законодательство такого рода обычно содержит положения, относящиеся к определению именных или личных данных; возражение на доступ, возражение и исправление; цели обработки; сбору, хранению и обновлению данных; безопасности именных данных; продаже данных; мониторингу трансграничных потоков данных.

Такое законодательство часто дополняется другими юридическими документами такими, как, в случае Франции, *Loi sur la sécurité quotidienne* [Акт о повседневной безопасности] от 15 ноября 2001 года, в котором указывается, что данные, относящиеся к электронной связи, кроме информации о платежах, необходимо удалять или предоставлять анонимно. Нужно также удалять то, что называется "косвенными" данными (сведения о посещенных URL, IP адреса, к которым обращался сервер, строки темы сообщения).

Ситуация в Швейцарии

Швейцария приняла Федеральный акт о защите данных 19 июня 1992 года (Германия: Акт от 21 января 1977; Бельгия: Акт от 8 декабря 1992; Канада: Акт о защите личной информации и электронных документов 1982 года; США: Акт о приватности 1974 года; Статут о базах данных и приватности 1988 года.

В Швейцарии защита данных гарантируется в первую очередь пересмотренной Федеральной Конституцией, вступившей в силу 1 января 2000 года, статья 13/2 которой гласит: "*Все люди имеют право на защиту от злоупотребления их личными данными*"[48].

Самыми важными федеральными законами являются Акт о защите данных 1992 года и исполнительные распоряжения от 14 июня 1993 года. Акт о защите данных применяется вне зависимости от среды и технологии, используемой для сбора и обработки данных. Он применяется как к отдельным лицам, так и федеральным органам власти, к физическим лицам и к компаниям, вне зависимости от того, как происходила обработка данных. В статье 3 личные данные определяются как "*вся информация, относящаяся к определенному или определяемому лицу*". В данном Акте также определяются правила, относящиеся непосредственно к уязвимым личным данным и личным параметрам пользователя.

Обработка определена достаточно широко и включает в себя "*любые операции, относящиеся к личным данным, вне зависимости от используемого оборудования и процедур, а в особенности сбор, хранение, использование, изменение, передача, архивирование или уничтожение данных*". Тем не менее, в статье 2/2 перечисляются несколько областей, в которых данный Акт не применяется, таких, как судопроизводство, находящееся на рассмотрении, и "*личные данные, обрабатываемые физическим лицом исключительно для личных целей, и не передаваемые третьей стороне*"

[48] Кроме специально оговоренных случаев, цитаты из французских или швейцарских юридических документов переведены с французского Службами переводов МСЭ.

(подпункт a). Решением Федерального суда от 5 апреля 2000 года, понятие тайны электросвязи распространилось на электронные сообщения. В статье 43 Федерального акта об электросвязи Швейцарии также содержится обязательство по секретности: "*Любому человеку, предоставлявшему или предоставляющему услуги электросвязи, запрещено предоставлять третьей стороне информацию о трафике пользователя; таким людям также запрещено давать возможность кому-либо еще передавать такую информацию третьим сторонам*". В статье 44 данного Акта, который дополняется статьями 6 и 11 Распоряжения Федерального совета о почтовой связи и надзору за электросвязью от 1 декабря 1997 года, устанавливается процедура и условия для контроля.

Швейцарские правила, регулирующие защиту личных данных в интернете, во многом похожи на правила Европейской директивы по тому же вопросу.

IV.1.1.4 Экономическое значение законодательства

Законодательство по вопросам обработки личных данных и защиты приватности в секторе электронной связи побуждает организации хорошо управлять безопасностью информационных технологий и сети (данные пользователей, контроль связи и работников, безопасное управление, автоматизированная обработка личных данных и т. д.). Организации должны обеспечить себя соответствующими средствами безопасности и контроля.

Экономическое значение инвестиций, необходимых для гарантирования минимального уровня безопасности (физическая и юридическая защита), меняется в зависимости от потенциальных материальных потерь организации и угрозы ее репутации и имиджу. Таким образом, законодательство является внутренней движущей силой безопасности.

IV.1.2 Электронная коммерция и заключение контрактов в киберпространстве[49]

В данном разделе обсуждаются различные аспекты контрактов в той степени, в которой они относятся к деловым операциям, производимым в киберпространстве, а также определяются основные европейские и швейцарские законодательные акты, регулирующие такие операции. Цитируемое законодательство Швейцарии и основные европейские директивы, содержат несколько основных принципов, которые можно применить к другим странам и внутригосударственному праву.

IV.1.2.1 Вопрос выбора правовых норм

Первой юридической проблемой электронной коммерции является определение географической области, внутри которой происходит электронная транзакция. Характеристики интернета (международный охват, цифровая технология, режим работы) несовместимы с понятием географических границ государства, а потоки информации не останавливаются на государственных границах.

Данные и услуги являются общедоступными и могут предоставляться дистанционно, вне зависимости от того, где находятся интернет-пользователи и сервера. Продавец и покупатели часто взаимодействуют, находясь в разных странах. Поэтому знание того, закон какой страны применяется в случае возникновения спора, является чрезвычайно важным и составляет ключевой момент каждого предложения. В этом отношении, в транзакциях, выполняемых посредством интернета, должны указываться ограничения предложения и определенная информация о том, суды какой страны обладают юрисдикцией в случае спора[50].

Стороны, заключающие контракт, могут договориться о выборе законодательства и суда юрисдикции. При отсутствии пункта выбора правовых норм необходимо определить, подпадает ли контракт под область действия международного соглашения такого, как Принципы международных торговых отношений UNIDROIT (1994), форма сетевого этикета; или Гаагская конвенция от 15 июня 1955 года. Однако международные соглашения не являются принудительными, если только они в явном виде не включены в контракт. Если ни одно из данных решений невозможно, применяются правила договорного права.

---

[49] Этот раздел был написан в сотрудничестве с Игли Таши, помощником аспиранта в Университете Лозанны.

[50] Закон места рассмотрения дела – это доктрина международного частного права, относящаяся к законодательству страны, в которой должны проводиться судебные слушания.

В законодательстве Швейцарии, например, эти правила устанавливаются в Федеральном акте о международном частном праве 1987 года, статья 1 которого гласит[51]:

"[1] Данный Акт регулирует в международном контексте:

a. юрисдикцию швейцарских судов или административных органов;

b. основное законодательство;

c. предпосылки для признания и применения в жизнь зарубежных решений;

d. банкротство и компромиссные соглашения должника с кредиторами;

e. арбитраж.

[2] Международные соглашения остаются в силе."

Основными принципами являются следующие: контракт регулируется законом того государства, с которым он связан теснее всего (ст. 117/1 Акта). Обычно это относится к поставщику товаров и услуг, если это в явном виде включено в общие условия, за одним исключением: статья 120 данного Акта, которая регулирует *Контракты с потребителями*, гласит, что:

"Контракты для исполнения, относящегося к обычному потреблению, предназначенного для личного использования потребителем или его семьей и не связанного с его профессиональной или коммерческой активностью, должны регулироваться законом того государства, в котором обычно проживает потребитель, если:

a. продавец получил заказ в данном государстве;

b. в данном государстве заключению контракта предшествовало предложение или реклама, и потребитель выполнил все необходимые юридические действия для заключения контракта, или

c. продавец побудил потребителя поехать за границу и поставил его заказ туда.

[2] Выбор закона исключается."

Содержание сайта, например, используемый язык или список валют, может говорить о целевом рынке продавца и, таким образом, о применяющемся законодательстве.

В случаях, когда выбор закона не был определен соглашением между сторонами, можно подать ходатайство по месту жительства обвиняемого или в месте расположения его штаб-квартиры.

IV.1.2.2 Контракты, заключаемые в электронном виде

Правила, применимые к контрактам, заключаемым в электронном виде, в целом такие же, как и правила, применимые к так называемым традиционным контрактам. Контракт считается заключенным, если одна из сторон делает предложение (оферту), а другая сторона принимает это предложение (оферту).

Европейская директива

Директива 97/7/ЕС Европейского парламента и Совета Европы от 20 мая 1997 года, касается вопросов дистанционных продаж и электронной торговли. В этой Директиве указывается, что перед заключением любого дистанционного контракта потребителю нужно предоставить следующую информацию:

- личность продавца и, в случае, если контракт требует предоплаты, его адрес;
- основные характеристики товаров и услуг;
- цена товаров и услуг, включая все налоги;
- стоимость доставки, где необходимо;
- соглашение об оплате, доставке или исполнении;
- существование права на возврат, кроме случаев, описанных в Статье 6 (3) данной Директивы;

---

[51] Источник англоязычной версии Федерального акта о международном частном праве: Джером Г. Фарнум, бакалавр гуманитарных наук, доктор права, *Федеральный акт Швейцарии о международном частном праве, английский перевод официального текста*, Швейцарско-американская торговая палата/Schulthess, Цюрих, 2004 г. (исправленная версия).

- стоимость использования средств удаленной связи, если она исчисляется не на основе тарифной ставки;
- период времени, в течение которого действует данное предложение цены;
- где необходимо, минимальная продолжительность контракта в случае контрактов по поставке товаров или услуг, осуществляемой постоянно или с определенной периодичностью.

Наиболее важный момент, касающийся заключения контракта, относится к определению того, что составляет "оферту" и "акцептование оферты". Товары, "выставленные" на интернет-сайтах с указанием цены, рекламная информация о них, составляют не оферту, а скорее приглашение делать заявки в контексте статьи 7 Кодекса Швейцарии об обязательствах: "[2] *Отправка тарифов, прейскурантов и т. п. сама по себе не составляет оферты […]".*[52]

Отправка электронного сообщения или бланка заказа также считается приглашением к заявке.

Твердая оферта считается сделанной, а контракт подписанным, когда покупатель принимает или щелкает на кнопке "Купить". Он не выражает большего намерения купить, просто посещая сайт, чем просто входя в магазин. С другой стороны, выставление товаров на веб-сайте составляет оферту, только если продавец указывает количество товара, имеющегося в наличии, и если это количество уменьшается после заказа, или если характер товара таков, что продавец всегда может выполнить заказ.

Контракт считается заключенным, как только получатель услуги, т. е. потребитель, желающий купить выставленные товары, получает электронное подтверждение от продавца, но только, если оба документа отправлены в течение короткого промежутка времени. Существует разграничение между контрактами, о которых обе стороны узнали одновременно, и контрактах, о которых обе стороны узнали не одновременно.

Контракт между отсутствующими? *Да, но…*

Контракт, заключенный через интернет, считается контрактом между отсутствующими, что предполагает, что оферта должна быть акцептована в течение приемлемого времени, как указано в статье 5 Кодекса Швейцарии об обязательствах:

"Ст. 5:

b. Между отсутствующими людьми

[1] Если оферта отправляется отсутствующему человеку без установления лимита времени, продавец должен оставаться связанным обязательством до тех пор, пока он будет ожидать получения ответа, отправленного должным образом вовремя.

[2] Таким образом, продавец может предположить, что его оферта прибыла вовремя.

[3] Если объявление о получении было отправлено вовремя, но прибыло к продавцу только после истечения времени, продавец считается связанным обязательством, если он не предупредит без промедления о своем намерении не быть связанным обязательством."

Однако если обмен данными контракта происходил посредством дискуссионного форума, дискуссионной группы, мгновенного обмена сообщениями или интернет-телефонии, считается, что контракт стал известен обеим сторонам одновременно, и подтверждение должно быть незамедлительным. В статье 4/1 Кодекса Швейцарии об обязательствах говорится: "*Если оферта делается присутствующему человеку без установления временного предела, продавец не должен считаться связанным обязательством, если оферта не акцептуется незамедлительно.*"

IV.1.2.3 Электронная подпись

Читатель может проверить целостность сообщения и, таким образом, убедиться, что оно не было изменено во время передачи, а также, благодаря системе асимметричного шифрования, удостовериться, кто является отправителем; следовательно, отправитель не может отрицать, что он

---

[52] Источник англоязычной версии Кодекса об обязательствах: Ребекка Брюннер-Петерс, доктор права, и др. *Кодекс Швейцарии об обязательствах,* Часть I, Договорное право, Статьи 1–551, английский перевод официального текста, Швейцарско-американская торговая палата/Schulthess, Цюрих, 2005 г. (исправленная версия).

отправил данное сообщение (понятие неотказуемости). Эти услуги информационной безопасности выполняются при использовании цифрового сертификата для "подписи" цифрового документа. По аналогии с рукописной подписью электронная подпись является цифровой подписью данных. Смежными понятиями являются (секретный и открытый) ключи шифрования и орган сертификации (также называемый третьей доверенной стороной или TTP).

Для того чтобы электронная подпись считалась заменителем рукописной подписи на бумажном документе в цифровом мире, она должна быть уникальным образом связана с подписавшей стороной, она должна обладать способностью идентифицировать подписавшую сторону, и должна быть создана при помощи средств, которые подписавшая сторона может держать под своим единоличным контролем.

Закон Швейцарии считает, электронные подписи имеют такую же силу, как и рукописные. Согласно статье 14 Кодекса об обязательствах:

"[1] Подпись должна быть выполнена собственноручно.

[…]

[2bis] Соответствующая электронная подпись, основанная на соответствующем сертификате, созданная поставщиком услуг по сертификации, официально признанным в рамках Федерального акта об электронных подписях от 19 декабря 2003 года, должна быть эквивалентна рукописной подписи. Отклоняющиеся правовые нормы и положения договора сохраняются."

Электронные подписи регламентируются Федеральным актом об электронных подписях от 19 декабря 2003 года, где определяется понятие электронной подписи, описываются различные формы, которые она может принимать, и перечисляются те формы, которые участвуют в реализации механизма подписи и выдаче цифровых сертификатов.

"Ст. 2 Определения

Дл целей данного Акта:

a. электронная подпись обозначает данные в электронной форме, которые присоединяются или логически связываются с другими электронными данными, и которые служат в качестве средства аутентификации;

b. усовершенствованная электронная подпись обозначает электронную подпись, которая удовлетворяет следующим требованиям:

1. она уникальным образом связана с подписавшейся стороной,

2. она обладает способностью идентифицировать подписавшуюся сторону,

3. создается при помощи средств, которые подписавшаяся сторона может держать под своим единоличным контролем,

4. связана с данными, к которым она относится, таким образом, что любое последующее изменение данных можно обнаружить;

c. соответствующая электронная подпись обозначает усовершенствованную электронную подпись на основе безопасного соглашения для создания подписи в рамках значений ст. 6/1 и 6/2, а также на основе соответствующего сертификата, который был действителен во время ее создания;

d. ключ подписи обозначает уникальные данные такие, как коды или частные ключи шифрования, которые используются подписывающейся стороной для создания электронной подписи;

e. ключ подтверждения подписи обозначает данные такие, как коды или открытые ключи шифрования, используемые для подтверждения подлинности электронной подписи;

f. соответствующий сертификат обозначает сертификат, который удовлетворяет требованиям, изложенным в ст. 7;

g. поставщик услуг сертификации (поставщик) означает объект, сертифицирующий данные в электронном окружении и выдающий электронные сертификаты для этой цели;

h. орган распознавания обозначает объект, который, согласно правилам аккредитации, уполномочен распознавать поставщиков и наблюдать за ними;

[…]".

Электронная подпись и Европейская директива

В Директиве 1999/93/ЕС от 13 декабря 1999 года о Европейской структуре для электронных подписей выделяется три типа электронной подписи в зависимости от степени интеграции механизмов шифрования и предоставляемого уровня безопасности.

Существуют различные типы электронных подписей. Во-первых, сообщение может быть просто "подписано", при этом подпись не будет связана с содержанием сообщения (основное понятие электронной подписи). В таком случае, кто угодно может "отделить" подпись от сообщения и использовать ее вместо подписи законного владельца. Для преодоления этого недостатка, для того чтобы связать подпись с содержанием сообщения и подтвердить подлинность отправителя и целостность сообщения при получении, можно использовать функцию шифрования (понятие усовершенствованной электронной подписи).

И, наконец, в Директиве описываются защищенные электронные подписи, основывающиеся на положениях о безопасности Приложения II, касающихся требований для поставщиков услуг по сертификации, выпускающих соответствующие сертификаты[53].

IV.1.2.4 Право на отказ

Легкость, с которой можно купить товары в интернете, может побудить некоторых потребителей действовать поспешно. В такой ситуации, право на отказ приобретает особую важность.

В Швейцарии право на отказ регламентируется статьей 9 Кодекса об обязательствах, в параграфе 1 которого устанавливается следующий принцип: "*Если продавец отзывает свою оферту и такой отзыв достигает другой стороны раньше[…] оферты, […] следует считать, что эта оферта не была сделана*". Тот же принцип применяется и к отзыву акцепта.

Право на отказ и Европейская директива

В Европейском союзе право на отказ регламентируется Директивой 1997/7/ЕС от 20 мая 1997 года, где указано, что для любого контракта на расстоянии, у потребителя есть период, продолжительностью по крайней мере в семь рабочих дней, в которые он может отказаться от контракта без штрафных санкций и без объяснения причины. Если поставщик не смог выполнить обязательства, изложенные в статье 5, в особенности, касающиеся условий и процедур для соблюдения права на отказ от контракта, продолжительность периода устанавливается равной трем месяцам.

IV.1.2.5 Разрешение споров

Участники спора, возникшего в связи с правильно заключенным контрактом, должны предоставить свидетельства того, был ли контракт заключен в электронном виде или нет. Следовательно, рекомендуется всегда вести записи транзакций такие, как копии электронного сообщения или распечатки с экрана.

Ситуация во Франции

Во Франции в статье 109 Кодекса потребителя не указывается, в какой форме должны предоставляться свидетельства в случае сделок между компаниями. Поэтому допускаются сообщения электронной почты, как и бумажные документы. Однако для сделок между бизнесом и потребителем для транзакций, превышающих определенную сумму, требуется письменное подтверждение. Цель – защитить среднего потребителя, у которого нет ни возможности, ни правовых ресурсов выиграть дело в случае спора с коммерческой фирмой.

Однако сообщения электронной почты могут приниматься в качестве доказательства для нормативных актов, касающихся электронной подписи. Это означает, что сообщение электронной почты будет считаться действительным доказательством, если соблюдаются вышеупомянутые требования, предъявляемые к электронным подписям.

---

[53] europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

Общие условия

Часто контракты на расстоянии включают в себя общие условия, которые являются составной частью контракта. Для того чтобы эти общие условия были действительными в случае спора, к ним должен быть обеспечен легкий доступ в интернете, а покупателю необходимо сообщить, что они являются частью контракта.

Разрешение споров в интернете

Принимая во внимание международный характер электронной коммерции, были разработаны способы разрешения споров, не включающие в себя традиционный зал суда. Понятие разрешения спора в интернете (online dispute resolution (ODR)) появилось благодаря желанию найти немедленное решение по вопросу невыполнения контрактов, заключенных в интернете. Этот тип разрешения конфликтов основывается на согласительных процедурах, которые включают в себя переговоры, посредничество и арбитраж[54]. Это быстрее, дешевле и удобнее для пользователей. Недостатком является то, что разрешение спора в интернете основывается на кодексах поведения и рекомендациях, также известных как законодательство в области программного обеспечения (таких как Политика разрешения споров по унифицированным доменным именам ICANN), что затрудняет исполнение решений.

IV.1.3 Киберпространство и интеллектуальная собственность[55]

IV.1.3.1 Области права, защищающие интеллектуальную собственность

Права интеллектуальной собственности защищаются в нескольких областях права, а именно:

- закон о товарных знаках;
- закон об авторских правах;
- патентное право;
- закон о промышленных образцах и моделях;
- закон, защищающий сорта растений;
- закон о полупроводниковых топологиях;
- закон о государственном гербе и других государственных символах.

Закон о недобросовестной конкуренции также защищает права интеллектуальной собственности.

IV.1.3.2 Авторские и смежные права

Это область права, защищающая:

- авторов литературных и художественных работ;
- исполнителей, продюсеров звукозаписей и видеозаписей, а также аудиовизуальные предприятия связи.

Работа – это произведение литературного или художественного характера; оно индивидуально по своей природе, вне зависимости от ценности и предполагаемой цели создания. Произведения такого характера включают в себя:

- работы, использующие язык, будь то научные, литературные или другие работы;
- музыкальные и другие акустические произведения;
- произведения изобразительного искусства, в особенности скульптуры и графику;
- работы научного или технического содержания такие, как чертежи, планы, карты, скульптуры или модели;
- архитектурные произведения;
- произведения прикладного искусства;

---

[54] Данный механизм разрешения споров является предметом типового закона, принятого Комиссией ООН по международному торговому законодательству (UNCITRAL).

[55] Данный раздел был написан в сотрудничестве с профессором Саррой Бен Лага из Политехнического института Туниса, лектора в Университете Лозанны.

- фотографии, кинематографические и другие визуальные и аудиовизуальные произведения;
- хореография и пантомима;
- компьютерные программы (программное обеспечение);
- проекты, названия и части произведений, которые являются индивидуальными по характеру.

Авторское право наделяет автора (физическое лицо, создавшее произведение) или предполагаемого автора (человека, который показывает данное произведение, до тех пор, пока не будет определен автор) моральным правом и правом собственности.

Нет необходимости отдавать произведение на хранение в офис или регистрировать права, хотя в некоторых странах действительно есть хранилища авторского права. Идеи не могут защищаться авторским правом, поскольку защите подлежат только материальные произведения.

Термин "моральные права" относится, главным образом, к подтверждению авторства и права решать будет ли публиковаться данная работа, и, если да, то когда, каким образом и под каким названием она будет опубликована. "Права собственности" относятся к использованию работы (производству и продаже копий, презентации, распределению, вещанию и т. д.).

Передача собственности произведения, будь то копия или оригинал, не предполагает передачи авторского права. Право собственности может быть приписано и наследоваться.

Термин "смежные права" относится к правам исполнителей (физических лиц, исполняющих произведение или участвующих в представлении с художественной точки зрения) или продюсерам звукозаписей и видеозаписей, а также аудиовизуальных предприятий связи.

IV.1.3.3 Закон о товарных знаках

Цель товарного знака – отличать продукцию и/или услуги владельца товарного знака от продуктов и/или услуг других компаний. Товарный знак идентифицирует объект (а не субъект права, который обычно идентифицируется при помощи имени или названия компании).

Нельзя получить защиту для:

- знаков, являющихся всеобщим достоянием;
- форм, которые соответствуют природе продукции или свойственны ее использованию;
- знаков, вводящих в заблуждение;
- знаков, противоречащих действующему законодательству или принципам морали.

Товарный знак должен быть зарегистрирован, для того чтобы пользоваться защитой.

В регистрации торгового знака может быть отказано, если:

- он идентичен знаку, ранее зарегистрированному для идентичного продукта;
- он идентичен какому-либо знаку или похож на какой-либо товарный знак, ранее зарегистрированный для аналогичных товаров и/или услуг, и есть риск, что товары/услуги могут перепутать.

IV.1.3.4 Патентное право

Патенты выдаются на промышленные изобретения. Они не могут выдаваться на очевидные побочные продукты технического развития, на сорта растений или породы животных или на чисто биологические процессы, используемые для производства растений или животных. Патенты могут выдаваться на микробиологические процессы и продукты, полученные в результате таких процессов.

Патент выдается (при определенных условиях) лицу, которое подало на него заявку (изобретателю, его правопреемнику или третьей стороне, обладающей данным изобретением на других основаниях).

Если несколько людей изобрели один и тот же продукт или процесс одновременно, патент выдается тому лицу, которое первым подало заявку, или тому, чья заявка имеет приоритет.

IV.1.3.5 Интеллектуальная защита интернет-сайтов

В интернете, особенно в отношении веб-сайтов, защита интеллектуальной собственности веб-сайта включает в себя несколько отраслей права[56]:

- в отношении доменного имени:
  - регистрация доменного имени не дает какого-либо определенного исключительного права владельцу;
  - для защиты доменного имени нужно обратиться к следующим юридическим документам:
    - закон о товарных знаках;
    - закон, определяющий названия компаний;
    - право на имя;
    - закон о конкуренции;
- в отношении содержания сайта:
  - и, в особенности, распределения работ через интернет:
    - если содержание было создано только для сайта, оно охраняется законом об авторском праве;
    - перевод существующей работы в цифровой вид и последующее распределение через интернет являются формой воспроизведения, что требует согласия автора оригинала;
    - ссылки на другие сайты: использование простой гиперссылки не нарушает исключительных прав, поскольку оно не включает в себя воспроизведения; внешние ссылки (которые направляют пользователя на определенную страницу на другом сайте, минуя главную страницу того сайта) – другое дело. Вопрос состоит в том, является ли указанная страница произведением или нет. Как правило, такие вопросы регулируются законом о конкуренции, решающим критерием при этом является то, как используются эти гиперссылки. Ключевым понятием здесь является честное использование.

IV.1.3.6 Дополняющий характер технической и юридической защиты

Меры технического характера вводятся для гарантии соблюдения авторского права. Законодательство принимается, для того чтобы эти меры не игнорировались. Таком образом, авторское право получает юридическую защиту, техническую защиту и юридическую защиту технической защиты.

IV.1.4 Спам: некоторые юридические аспекты[57]

IV.1.4.1 Контекст и зловредность

В общих чертах, спам[58] обозначает отправку незатребованных сообщений. Спам обладает следующими характеристиками:

- незатребованные сообщения отправляются в массовом порядке снова и снова;
- сообщение имеет коммерческую или враждебную цель (фишинг (жульническое выуживание информации), захват компьютера, внедрение злонамеренного программного обеспечения

---

[56] См. Филипп Гиллиерон, *Propriété intellectuelle et Internet*, Университет Лозанны (CEDIDAC No. 53), 2003 г.

[57] Данный раздел был написан в сотрудничестве с Игли Таши, помощником аспиранта в Университете Лозанны.

[58] Слово "спам" (spam) первоначально было торговым знаком, зарегистрированным Хормелом, и означало острую свинину и мясо ("spiced pork and meat"), род солонины, поставлявшейся американским солдатам во время Второй мировой войны. Нынешнее значение слова "спам", означающее отсылку незатребованных электронных сообщений, происходит от известного скетча Монти Питона, в котором слово "спам" пелось снова и снова, заглушая голоса других исполнителей.

такого, как вирус, adware (бесплатный программный продукт с находящейся в нем рекламой), spyware (шпионящее программное обеспечение) и т. д.);

– обычно адреса приобретаются без ведома пользователя (при нарушении правил, относящихся к защите личных данных);
– содержание таких сообщений часто является незаконным, обманчивым или вредным.

Поскольку спам не является затребованным, в некоторых обстоятельствах его можно считать агрессивной техникой продаж или рекламы. В наши дни спам принимает вид не только сообщений электронной почты, но и SMS на мобильных телефонах или новом мультимедийном оборудовании таком, как карманные PC.

Из-за спама все интернет-пользователи несут издержки. Эти издержки обычно относятся ко времени, которое занимает обработка таких сообщений, и приобретению инструментов, блокирующих спам. Спам также порождает социальные издержки, касающиеся потери доверия пользователей, более низкой производительности и т. д.

Согласно исследованию анти – спаминговой фирмы Clearswift, опубликованному в *Journal du Net* от 13 сентября 2005 года, спам охватывает следующие категории:

Типы спама	**июнь 2005 г.**
Здравоохранение	43,86%
Продукты	37,65%
Финансы	9,06%
Порнография	5,32%
Мошенничество	1,41%
Спор на деньги	0,1%
Другое	2,32%

Спам может принимать форму различных "афер", одним из наиболее распространенных видов которых является так называемое "письмо из Нигерии"[59]. Фишинг состоит в отправке сообщения будто бы от известного учреждения, например, банка, в котором пользователя просят пройти на поддельный сайт и ввести свои коды доступа и другую важную информацию, которую впоследствии будут использовать без его ведома.

Отправка спама может также осуществляться для разрушительных целей или для блокирования ящика входящей почты получателя, что не дает пользователю получать сообщения и использовать ресурсы интернета. "Бомбардирование" сообщениями принимает различные формы: большие сообщения, создающие проблемы при обработке и временном хранении, большое число сообщений, отправка огромному количеству получателей, для того чтобы на сервере произошла перегрузка или захват адреса отправителя.

IV.1.4.2 Юридические меры против спама

На спам распространяется действие нескольких областей права, в особенности законов о защите данных и о недобросовестной конкуренции; спаммеры также несут уголовную ответственность.

[59] Отправитель представляется наследником недавно умершего богатого человека, иногда в отдаленной стране. "Наследник" утверждает, что у него проблемы с утверждением своих прав, и предлагает использовать банковский счет жертвы в обмен на большую сумму в качестве компенсации за беспокойство жертвы. Жертве нужно предоставить ссуду на расходы, связанные с транзакцией. Очевидно, что это попытка выманить у людей деньги.

Ситуация в Швейцарии

В Швейцарии нет юридических документов, в явном виде регулирующих использование спама.

С точки зрения защиты данных, согласно Федеральному уполномоченному по защите данных Швейцарии и его документу *Aide-mémoire concernant les messages publicitaires indésirables diffusés par courrier électronique (spams)*[60], электронные адреса являются личными данными, которые могут использоваться для идентификации личности. Согласно статье 12/3 Акта о защите данных, "*Как правило, права личности не могут быть нарушены, если данный человек сделал данные доступными общественности и в явном виде не запретил их обработку*". Обработка электронного адреса спаммером является нарушением приватности (ст. 4/3), которое было совершено со злым умыслом (ст. 4/2) и без согласия заинтересованного лица (ст. 13/1). Таким образом, спам является нарушением защиты данных.

"Ст. 4 Принципы

1 Вся обработка личных данных должна предприниматься законным образом.

2 Обработка должна проводиться добросовестно и не должна быть чрезмерной.

3 Личные данные могут обрабатываться только в тех целях, для которых они были собраны, либо для целей, очевидных исходя из обстоятельств, или предоставленных законом."

Акт о защите данных дает заинтересованным лицам право обращаться в суд (ст. 15, которая отсылает к ст. 28 ff Гражданского кодекса Швейцарии).

Европейская директива

В Директиве 95/46/EC от 24 октября 1995 года о защите частных лиц относительно обработки личных данных и о свободном движении таких данных, устанавливаются минимальные стандарты для создания записей и обработки данных. В Статье 10 указывается, что субъект данных должен знать цель, для которой осуществляется сбор данных, а также личность контролера.

Ситуация во Франции

Во Франции, Акт об информационных технологиях и гражданских свободах включает в себя нарушения права на приватность, вытекающие из компьютерных записей или Уголовного кодекса Франции. В исправленной версии данного Акта от 2004 года вводятся 14 статей, предусматривающие более строгое наказание за неправильное использование личных данных.

Ситуация в США

Соединенные Штаты являются самым большим источником спама. 1 января 2004 года Конгресс ввел в действие Акт CAN-SPAM, на основании которого спаммеры могут понести наказание. Данный Акт запрещает "сбор" адресов электронной почты с веб-сайтов и запрещенных программ, которые генерируют адреса при помощи "словарных атак", случайным образом комбинируя буквы и числа.

Спам также представляет проблему с точки зрения недобросовестной конкуренции, когда его используют в рекламных целях.

Спам, реклама и недобросовестная конкуренция

Реклама в интернете регламентируется общими юридическими документами, касающимися рекламы, а не какой-либо определенной юридической структурой. В ноябре 2001 года, швейцарская Комиссия по честной игре в коммерческих связях опубликовала рекомендательную точку зрения, касающуюся спама, который расценивается как особенно агрессивный метод продаж. С точки зрения рекламы, такой метод можно использовать только в соответствии с определенными основными требованиями, будь то "традиционный" бизнес или электронная торговля.

---

[60] См. www.edsb.ch/f/doku/merkblaetter/spam.htm

Эти правила таковы:

- защита молодых пользователей интернета;
- уважение прав человека;
- уважение добросовестной, достоверной и честной рекламы;
- уважение юридической приватности пользователей;
- легкость навигации.

В статье 3 Федерального акта Швейцарии о недобросовестной конкуренции говорится, что: "*Недобросовестная конкуренция в особенности возникает тогда, когда кто-либо:*

[…]

b. предоставляет неточную или недостоверную информацию о себе, своем предприятии, названии компании, продукции, работах, услугах, ценах, инвентаре, методах продаж или ведения бизнеса или, предоставляя такую информацию, дает преимущество третьей стороне над их конкурентами;

c. демонстрирует или использует такие неточные названия или профессиональные обозначения, которые заставляют других верить, что у него имеются определенные отличительные особенности или возможности;

d. предпринимает такие меры, которые приводят к перепутыванию его товаров, работ, услуг или предприятия с товарами, работами, услугами или предприятием другого лица."

Но именно буква h статьи 3 касается самой сути данной проблемы. В ней сказано, что "*Недобросовестная конкуренция в особенности возникает тогда, когда кто-либо:*

[…]

h. препятствует свободе покупателя выбирать, используя особенно агрессивные методы продаж".

При использовании спама в коммерческих целях с описанной выше интенсивностью, он может подпадать под эту статью.

Спам и преступный умысел

Когда спаммеры действуют с преступным умыслом, они несут уголовную ответственность. Даже если их сообщение является коммерческим по характеру, содержание сообщения может стать основанием для судебного преследования.

Спам и порнография

Большинство спам-сообщений приглашают пользователя посетить порнографические сайты. Это является уголовным преступлением, статья 197 Уголовного кодекса Швейцарии, в особенности если сообщение предоставляет информацию лицам, которые не хотят получать ее (ст. 197/2) или лицам моложе 16 лет (ст. 197/1).

Спам, мошенничество, вирусы и продажа запрещенных товаров

Мошенничество – это уголовное преступление, статья 146 Уголовного кодекса Швейцарии. Оно определяется как получение финансовой выгоды от жертвы с целью самообогащения. С этой точки зрения, "письмо из Нигерии" определенно является мошенничеством.

Иногда спам может быть лучшим способом для заражения машин вирусами. В швейцарском законодательстве, если внедрение вируса приводит к нарушению данных (если данные жертвы были изменены, стерты или стали неиспользуемыми), спаммер может понести наказание по статье 144*bis* Уголовного кодекса.

Швейцарским законодательством также запрещено использование спама для продажи медицинских препаратов. Статья 32 Закона Швейцарии о медицинских препаратах и приборах запрещает рекламу, стимулирующую чрезмерное или несоответствующее использование медицинских препаратов, или рекламу медицинских препаратов, которые не могут продаваться на рынке Швейцарии или выдаются только по рецепту врача.

IV.1.4.3 Регулирование спама

Существуют два противоположных метода регулирования спама: подход рассылки по запросу и подход рассылки с правом отказа.

Подход рассылки по запросу больше уважает пользователя интернета, поскольку этот подход состоит в оправке пользователю только той рекламы, которую он явно согласился получать, отметив или не отметив соответствующую клетку; согласие может также и подразумеваться, но в таком случае посетителя нужно четко уведомить о коммерческом характере этой подписки и ее последствиях.

Метод рассылки с правом отказа состоит в "отказе от рассылки" и устанавливает право отказаться от получения сообщений в последствии. Каждое отправленное сообщение должно давать получателю возможность отказаться от подписки. Создавать записи отказов можно получить законным путем (например, купив список отказов) или собрать, используя случайную процедуру.

Швейцарские и американские законодатели выбрали подход рассылки с правом отказа, а в Европейском союзе скорее одобряют подход рассылки по запросу, что было показано на примере Директивы 2002/58/EC, касающейся обработки личных данных и защиты приватности в сфере электронной связи (Директива о приватности и электронной связи).

Поскольку спаммеры чаще всего действуют анонимно и из-за рубежа, судебный процесс дорог и сложен и обычно включает в себя привлечение адвоката.

IV.1.4.4 Технические средства борьбы со спамом

Технические ограничения

Влияние спама можно ограничить, используя технические средства для ограничения, например, числа получателей на одно сообщение, числа сообщений на один источник и числа сообщений за единицу времени.

Черные списки

"Черные списки" работают по принципу, что почту можно классифицировать, используя в качестве критерия репутацию сервера. Репутация почтового сервера, с которого недавно был получен спам, испорчена, поскольку можно предположить, что данный сервер будет присылать больше спама в будущем. Сервер можно идентифицировать по IP адресу.

Фильтры, использующие ключевые слова

Фильтры по ключевому слову блокируют сообщения, содержащие определенные ключевые слова. Они неэффективны, поскольку спаммеры могут легко написать сообщения так, чтобы обойти фильтры.

Технология профилирования

Спам состоит в отправке большого числа идентичных сообщений. Технология профилирования используется для определения профиля содержания сообщения и сравнения его с базой данных содержаний, считающихся спамом.

Политика по борьбе со злонамеренным программным обеспечением

Для установки серверов электронной почты на инфицированные машины все больше используется злонамеренное программное обеспечение (вирусы, "Троянские кони", боты и т. д.). Целью этих действия является облегчение распространения спама. Борьба со спамом также подразумевает искоренение злонамеренного программного обеспечения.

Программное обеспечение против спама может помочь отфильтровывать и блокировать спам на уровне почтового сервера и, таким образом, ограничить его распространение, однако оно не всегда является эффективным. Настоящие сообщения не доходят до получателей (понятие ошибочного допуска), а настоящий спам пропускается (понятие ошибочного отказа).

Отношение пользователя является ключевым аспектом борьбы со спамом. Например, круг проблем можно сузить, если пользователи разумно обращаются с сообщениями (они должны знать о риске кражи идентификационной информации, проверять, как будет использоваться адрес их электронной почты, перед тем, как вписать его в интернет-форму, использовать несколько адресов электронной почты, избегать посещения определенных сайтов, научиться не открывать сообщения от незнакомых отправителей, удалять спам, не читая, никогда не отвечать на спам-сообщения и не проходить по гиперссылкам в них и т. д.)

IV.1.4.5 Взаимодополняемость технических и юридических средств

Поскольку юридические меры мало влияют на распространение спама, требуется технологическое решение. Совладать с явлением спама можно только используя технические и юридические средства. Каждый спаммер, обескураженный словом закона или техническим решением, означает миллионы и миллионы неотправленных сообщений.

IV.1.5 Резюме основных юридических вопросов, относящихся к киберпространству[61]

IV.1.5.1 Юридический статус коммерческого интернета

Юридический статус коммерческого интернета определяется юридическим статусом используемых инструментов информационных технологий.

Что касается электронной почты, вопрос состоит в содержании сообщения, адресе почтового ящика и риске кражи идентификационной информации, отличительного знака или названия компании. Эти вопросы регулируются гражданским правом каждой страны.

Что касается веб-сайтов, понятие работы, как аудиовизуального, так и не аудиовизуального характера, ставит вопросы авторского права. Гиперссылка поднимает вопрос содержания, ответственности того, защищается она или нет, а также проблемы, относящиеся к поисковым службам.

IV.1.5.2 Киберконтракты

Заключение контрактов в интернете вызывает не только юридические вопросы. Оно также требует существования технических механизмов для действительного заключения контрактов (используемые инструменты и процедуры (глобальность, неприкосновенность, делокализация)).

С юридической точки зрения важно следующее:

- оферта, ее статус (удаленная или нет), акцептование оферты;
- реклама и предложение услуг, спам и т. д.;
- исполнение;
- акцептование оферты в интернете, и информационная технология, используемая для обозначения акцептования;
- право на отказ;
- выбор закона и юрисдикции.

Эти пункты регулируются различными европейскими директивами, а именно:

- Распоряжение ЕС № 44/2001 от 22 декабря 2000 года о юрисдикции и признании и выполнении судебных решений в гражданских и коммерческих вопросах;
- Директива 2000/31/ЕС об электронной торговле;
- Директива 98/34/ЕС от 22 июня 1998 года, устанавливающая процедуру для предоставления информации в области технических стандартов и распоряжений;
- Директива 97/7/ЕС о защите потребителей в отношении контрактов на расстоянии.

---

[61] Этот раздел написан в сотрудничестве с Игли Таши, помощником аспиранта в Университете Лозанны.

Важными документами также являются типовой закон UNCITRAL об электронной торговле от 1996 года, Министерская декларация ВТО в Женеве от 1998 года о глобальной электронной торговле и Совместное заявление ЕС–США от 1997 года об электронной торговле.

IV.1.5.3 Электронные документы и подписи

Электронные документы, подписываемые в электронном виде, поднимают проблему подлинности. Цель – гарантировать юридическую подлинность подписи для идентификации подписавшего лица и убедиться в том, что он намеревался подписать данный документ, и, таким образом, берет на себя ответственность за содержание (сообщения).

Примерами важных юридических документов являются Директива 1999/93/ЕС от 13 декабря 1999 года о структуре Евросоюза для электронных подписей (Европейский союз), Закон № 59 от 15 марта 1997 года (Италия), Акт об электронных подписях в глобальной и национальной торговле от 30 июня 2000 года (США), а также Акт об электронной связи от 25 мая 2000 года (Великобритания).

IV.1.5.4 Электронные платежи

Электронные платежи, включающие использование кредитных карт, чеков или электронных денег, могут быть перехвачены третьими лицами, например, когда поставщик услуг связывается с получателем или важную информацию используют неправильно.

Примером юридического документа является Директива 2000/46/ЕС от 18 сентября 2000 года о покровительстве, судебном преследовании и разумном надзоре за деятельностью организаций, занимающихся электронными деньгами.

IV.1.5.5 Защита доменных имен

Доменные имена – это новая форма нематериального имущества, которое может иметь значительную коммерческую ценность. Доменные имена нужно рассматривать с точки зрения того, как они относятся к:

- торговым знакам и доменным именам;
- отличительным знакам;
- названиям фирмы и доменным именам.

В добавление к национальному законодательству о торговых знаках, названиях и патентах, важность представляет Акт по защите потребителей от киберзахвата (США) (ACPA).

IV.1.5.6 Интеллектуальная собственность

Интеллектуальная собственность в интернете поднимает проблемы авторского права, торговых знаков и патентов. Достаточно упомянуть Договор об авторском праве Всемирной организации по охране интеллектуальной собственности (ВОИС) и Договор ВОИС об исполнении и фонограммах, а также европейское законодательство, "Зеленая книга" (официальный правительственный документ, содержащий предложения относительно будущего закона; предоставляется правительству для обсуждения; называется по цвету обложки) об авторском праве и смежных правах в информационном обществе от 1995 года и Директиву 2001/29/ЕС Европейского парламента и Совета от 22 мая 2001 года о гармонизации определенных аспектов авторского права и смежных прав в информационном обществе.

IV.1.5.7 Защита цифровой приватности

Спам – это нарушение права на цифровую приватность (см. Директиву 97/7/ЕС о защите потребителей в отношении контрактов на расстоянии и Директиву 97/66/ЕС, касающуюся обработки личных данных и защиты приватности в области электросвязи, в которой запрещается рассылка прямой почты, использующей спам).

IV.1.5.8 Другие юридические вопросы

Среди многих других юридических вопросов, которые необходимо обдумать при определении соответствующей юридической структуры для использования интернета такие вопросы, как:

- антитрестовское законодательство (см. Антитрестовские рекомендации по сотрудничеству среди конкурентов (США), апрель 2000 года);
- ответственность поставщиков и технических посредников (в какой степени поставщик несет ответственность за деятельность пользователей интернета, преступную деятельность, детскую порнографию и т. д.);
- неприкосновенность тайны переписки.

Раздел IV.2 – Перспективы

IV.2.1 Обучение – профессиональная подготовка – повышение осведомленности всех участников кибербезопасности

Важно, чтобы все участники интернета знали о важности вопросов безопасности и об основных мерах, которые, если их четко определить и благоразумно реализовывать, укрепят уверенность пользователей в обработке данных и технологиях связи, включая интернет. интернет должен быть общественным достоянием, а не содействовать исключительно преступной деятельности.

Необходимо предпринять шаги для развития культуры и многостороннего подхода к безопасности, для того чтобы управлять риском того, что информационные технологии будут использованы с преступной целью. Как государства, так и организации должны рассматривать эти проблемы со стратегической точки зрения.

Выполнять обучение, информирование и подготовку нужно не только в области безопасности и сдерживающих средств, но в области технологий обработки данных и технологий связи. Повышение осведомленности в вопросах безопасности не должно ограничиваться только продвижением культуры безопасности. Сначала должна появиться культура информационных технологий. Участникам нужно также предоставить средства для обучения тому, как справляться с технологическими, оперативными рисками и рисками, связанными с информацией, с которыми они сталкиваются при использовании новых технологий.

Виртуальный характер интернета и его развлекательные возможности могут скрыть от молодых людей или новых пользователей значительные вредоносные возможности интернета. Последствия могут быть печальными как для организаций (компаний, административных или общественных учреждений), так и для частных лиц, ставших жертвами интернета. Управление технологическими рисками означает больше, чем охота на хакеров или создание технологических барьеров. Наиболее серьезные последствия иногда являются следствием простой небрежности, возникшей от незнания, неправильного использования или плохой реализации технологии, чрезмерных полномочий системных администраторов, неправильного управления и т. д.

IV.2.2 Новый подход к безопасности

Осведомленность об уязвимости цифрового мира и сложностях, свойственных контролированию не только информационных и телекоммуникационных технологий и инфраструктур, но и продаваемых решений безопасности, должна поднять серьезные вопросы о нашей зависимости от технологии, которой трудно управлять. То, что данные становятся заложниками систем информационных технологий, – это случайность, которую нельзя игнорировать.

Хочется верить, что технологические и юридические решения компенсируют ошибки и неправильное управление информационными технологиями и электросвязью, как на стратегическом и тактическом, так и на рабочем уровне. Более того, традиционные меры безопасности могут эффективно защитить уязвимые или важные ресурсы людей, организаций и государств, только если они реализуются прозрачными, поддающимися контролю и проверке способами.

Реализация всеобъемлющего подхода к безопасности, включающего предотвращение, охрану, защиту и реакцию означает принятие человеческих, юридических, технологических и экономических средств для осуществления этого подхода.

IV.2.3 Характеристики политики безопасности

Вообще говоря, надежная политика безопасности это результат анализа рисков. Она является всеобъемлющей, согласованной и целенаправленно реагирует на нужды безопасности в данном контексте.

Политика должна:

- быть простой и понятной;
- реализовываться обученным и внимательным персоналом;
- легко реализовываться;
- легко поддерживаться;
- поддаваться проверке и контролю.

Политика безопасности не должна быть статичной. Ее необходимо периодически пересматривать, оптимизировать и адаптировать к изменениям контекста, в котором она реализуется. Нужно, чтобы ее можно было конфигурировать и переделывать в соответствии с профилями пользователей, в свете потоков, контекста и географического положения участников. Политика безопасности будет меняться во времени и пространстве.

Политику безопасности можно разделить на политику управления доступом, защиты, антикризисного управления, исполнения и оптимизации, доверия.

IV.2.4 Идентификация уязвимых ресурсов для защиты

Ясную картину среды и ее защиты можно получить, составив полный и точный список всех ресурсов и участников цепочки безопасности. Идентификация значений различных категорий ресурсов выполняется, для того чтобы определить, насколько они уязвимы (или важны) и, таким образом, какие из ресурсов нужно защищать в первую очередь. Степень уязвимости зависит от последствий потери, изменения или разглашения данных. Чем более серьезны последствия для организации, тем более уязвимым является ресурс.

Каждый ресурс рассматривается как цель безопасности; для того чтобы определить осуществимость политики безопасности для каждой цели с технической и организационной точек зрения, нужно определить текущие риски и то, как они могут возникнуть (из-за ошибки пользователя, неправильного задания параметров, случайности, злонамеренного использования, саботажа, логической атаки и т. д.), исходные и применимые механизмы безопасности (конфигурация, параметры и т. д.), а также технические и организационные ограничения.

IV.2.5 Цели, задачи и фундаментальные принципы кибербезопасности

Целями кибербезопасности являются:

- конфиденциальность (без незаконного доступа): для поддержания секретности информации и ограничения доступа к надежным объектам;
- целостность и точность (без неверной информации, без ошибок): для поддержания целостности и неприкосновенности данных и программ;
- доступность (без задержки): для поддержания продолжительной, непрерываемой и неухудшающейся доступности;
- долговечность (без разрушения): для хранения данных и программного обеспечения так долго, как требуется;
- неотказуемость и приписываемость (без споров): для гарантирования происхождения, источника и правдивости источника;
- уважение цифровой приватности;
- аутентификация (без сомнений в подлинности источника).

Каждую задачу можно разложить на следующие компоненты:

- разработка плана безопасности на основе предварительного анализа рисков;
- определение границ уязвимости, возникающих из использования новых технологий;
- длительная защита на уровне, соизмеримом с возникающими рисками;
- реализация и утверждение структуры, мер, инструментов и процедур безопасности;
- мониторинг, проверка, контроль и развитие информационной системы и ее безопасности;
- оптимизация работы информационной системы в соответствии с требующимся уровнем безопасности;
- соизмерение нужд с рисками и издержками.

Фундаментальные принципы, поддерживающие любое действие по обеспечению кибербезопасности:

- словарь (необходимость установить общий язык, определяющий безопасность);
- последовательность (кибербезопасность появляется, когда гармонично интегрируются инструменты, механизмы и процедуры, необходимые для предотвращения, обнаружения, защиты и устранения ущерба, возникающего в результате ошибок, злого умысла или естественных факторов);
- административная воля (это ответственность администрации за обеспечение доступности средств, необходимых для реализации и управления плана кибербезопасности);
- финансы (стоимость безопасности и мер контроля должны быть пропорциональны риску);
- простота, универсальность и осмотрительность (меры безопасности должны быть простыми, гибкими, простыми для понимания пользователями; они не должны быть провокационными, чтобы не привлечь потенциальных нападающих);
- изменения и непрерывность (безопасность должна быть динамичной, для того чтобы интегрировать изменения системы во времени и необходимость в безопасности и риски; система должна работать долгое время);
- оценка, контроль и адаптация (для того чтобы гарантировать, что уровень безопасности соответствует реальным потребностям).

IV.2.6 Факторы успеха

IV.2.6.1 Стратегические указания

Успешная реализация стратегии безопасности требует:

- стратегической воли;
- простой, точной, понятной и применимой политики безопасности;
- публикации политики безопасности;
- централизованного управления безопасностью и некоторой степени автоматизации процедур безопасности;
- доверия и честности людей, систем и инструментов;
- процедур регистрации, надзора и проверки;
- намерения не подвергать ресурсы опасности;
- юридической структуры, применимой на национальном и международному уровнях;
- уважения юридических ограничения.

IV.2.6.2 Указания для пользователей интернета

Следующие рекомендации представляют собой простые, экономичные и относительно эффективные меры, которые могут предпринимать пользователи интернета, для того чтобы сделать свои ресурсы и электронную деятельность более безопасными[62]:

- выключайте компьютер, когда им не пользуетесь;
- не открывайте электронные сообщения от неизвестных отправителей;
- используйте регулярно обновляемый анти – вирус для минимальной защиты;
- не разглашайте свой пароль и часто меняйте его;
- не сообщайте личные данные о себе или о других через интернет;
- никогда не разрешайте никому использовать ваш счет для выхода в интернет;
- для защиты данных используйте системы шифрования;
- не посещайте непристойные сайты, не загружайте и не используйте нелегальные программы или файлы;
- не участвуйте в действиях в интернете, которые запрещены и наказуемы в невиртуальном мире (мошенничество, клевета и т. д.);
- не хвастайтесь уровнем своей защиты;
- помните, что, как и в невиртуальном мире, каждое действие в интернете совершается частным лицом и это частное лицо может быть нечестным.

IV.2.6.3 Указания для обеспечения безопасности системы электронной почты

Следующие основные рекомендации могут помочь защитить систему электронной почты.

Защитите сервер:

- используя антивирусное программное обеспечение;
- фильтруя сообщения, используя определенные критерии (размер, приложения и т. д.);
- правильно его конфигурируя;
- эффективно управляя им для обеспечения доступности;
- избегая заданных по умолчанию счета эксплуатационных издержек;
- обеспечив его физическую защиту.

В отношении пользователя:

- устанавливайте, управляйте и вводите использование антивирусного программного обеспечения;
- определите правила для использования системы сообщений (не открывать исполняемые файлы и т. д.);
- обеспечьте осведомленность о потенциальных рисках;
- получите обещание использовать ресурсы информационных технологий соответствующим образом;
- правильно сконфигурируйте рабочую станцию каждого пользователя и приложение сообщений;
- применяйте защищенные версии системы электронной почты;
- используйте процедуры шифрования для конфиденциальных сообщений и аутентифицируйте источники.

---

[62] Заимствовано из *Sentiment de sécurité sur Internet,* постмагистерской диссертации по праву, преступности и безопасности, написанной Анной-Софией Перрон, работающей под началом С. Гернаоути-Хелие, Лозанна, 2005 год.

IV.2.6.4 Указания для защиты окружения интернет–экстранет

Следующие основные рекомендации по использованию защитных систем помогут защитить окружение интернет–интранет.

- защитные системы должны быть защищены от незаконного доступа (понятие доверенной системы с защищенной операционной системой);
- весь трафик (входящий и исходящий) должен проходить через защитную систему;
- до прохождения через защитную систему должен допускаться только трафик, определенный политикой безопасности как действительный и авторизованный;
- защитную систему нужно сконфигурировать таким образом, чтобы она отфильтровывала все, что не авторизовано в явном виде;
- защитная система не может быть одновременно веб-сервером компании;
- если данные во внутренней сети уязвимы, доступ в Интернет должен происходить через машины, которые не подсоединены к внутренней сети;
- защитная система не может защитить окружение от атак или незаконного доступа, которые не проходят через нее. Она не эффективна против преступлений, совершаемых внутри компании.

Защитная система – это не антивирус. Поэтому ее нужно защищать от вирусов. В общем говоря, каждая система, обеспечивающая связь (сервера электронной почты, сервера связи и т. д.), каждая машина, содержащая данные (архив, сервер базы данных и т. д.), и каждая рабочая станция должна быть оснащена антивирусным программным обеспечением.

ЧАСТЬ V

Приложения

Приложение A – Глоссарий основных терминов безопасности[63]

Access control – Управление доступом

Механизм, служащий для защиты ресурса (услуги, системы, данных или программы) от ненадлежащего или несанкционированного использования.

Accident – Происшествие

Непредсказуемый инцидент, наносящий ущерб объекту.

Active attack – Активная атака

Атака, изменяющая ресурсы (влияющая на целостность, доступность и конфиденциальность).

Anonymity – Анонимность

Характеристика объекта, чье имя не известно или который не открывает свое имя, разрешение объекту использовать ресурсы без идентификации (инкогнито). Следует уважать желание некоторых пользователей, которые могут иметь серьезную причину для неразглашения своей личности при опубликовании заявлений в интернете, для того чтобы избежать чрезмерного ограничения свободы самовыражения, обеспечить прямое свободное выражение идей и информации и гарантировать защиту от незаконного надзора со стороны общественных и частных организаций. С другой стороны, у судебных и правоохранительных органов должна быть возможность получить информацию о частных лицах, несущих ответственность за незаконную деятельность, в рамках, определяемых национальным законодательством, Европейской конвенцией по правам человека и другими международными соглашениями такими, как Конвенция о киберпреступности.

Antivirus – Антивирус

Программа для обнаружения вируса.

Asset – Имущество

Что-то, имеющее цену и представляющее форму капитала для владельца (понятие уязвимого имущества). В отношении безопасности важно определить имущество и классифицировать его по степени важности, для того чтобы предпринять соответствующие меры защиты и, таким образом, избежать потери имущества или, по крайней мере, минимизировать неблагоприятные последствия его потери.

Asymmetric cryptographic algorithm – Асимметричный алгоритм шифрования

Алгоритм, основанный на использовании пары ключей (один для шифрования данных, другой для расшифровки).

Attack – Атака

Нападение, агрессия или действие, причиняющее ущерб частным лицам или ресурсам. Существуют различные типы компьютерных атак.

---

63 Заимствовано и адаптировано из глоссария в "*Securité informatique et réseaux, cours et exercices corrigés*", С. Гернаоути-Хелие, Дюно, 2006 год.

Auditability – Проверяемость

Степень, в которой можно проанализировать окружение в целях анализа и проверки.

Auditor – Проверяющий

Лицо, осуществляющее проверку.

Authentification – Аутентификация

Акт проверки подлинности. Аутентификация служит для подтверждения (или опровержения) того, что действие, заявления, единица информации являются аутентичными (оригинальными, подлинными). Процесс, используемый для подтверждения подлинности объекта и гарантирования, что идентификационные данные совпадают с идентификационными данными, ранее записанными для данного объекта.

Authencity – Аутентичность

Отличительный признак того, что является аутентичным. Характеристика, разрешающая подтверждение, или сертификацию подлинности. Часто ассоциируется с тем, что единица информации или событие не были изменены, модифицированы или фальсифицированы и что они на самом деле были созданы объектом, который утверждает, что создал их.

Authority – Орган

Объект, обладающий возможностями выполнять назначенные функции. Обычно используется для обозначения объекта, отвечающего за выдачу цифровых сертификатов.

Authorization – Авторизация

Акт санкционирования, разрешения, называния. Разрешение на выполнение определенных действий, предоставление прав, получения доступа к услуге, информации, системе и т. д.

Availability – Готовность

Критерий безопасности, при котором ресурсы доступны и могут использоваться для удовлетворения потребностям (без отказа в авторизованном доступе к системам, услугам, данным, инфраструктуре и т. д.).

Backdoor, trapdoor – Лазейка, черный ход

Обычно обозначает часть кода, включенного в программное обеспечение, позволяющую неавторизованным объектам контролировать системы, копировать информацию и т. д. без ведома владельца.

Backup plan – План резервного копирования

Набор технических и оперативных мер, предназначенных для гарантии устойчивости информации и продолжительности действий, вне зависимости от того, какие возникли проблемы.

Breach – Нарушение

Эффект или повреждение, возникшее из-за акта агрессии или атаки, влияние которых может быть: материальным (физическое или материальное изменение, логические сбои, дезорганизация процедур и т. д.), логическим (недоступность, потеря целостности, нарушение конфиденциальности), стратегическим (в особенности в отношении финансов, дополнительных затрат на размещение, транспортировку, электросвязь, экспертизу, покупку/аренду аппаратного и программного обеспечения, персонал, привлечение соисполнителей, оперативные издержки (размер прибыли, движение денежной наличности, издержки клиента), потеря фондов или товаров и т. д.).

Bug – Ошибка (в программе)

Ошибка программирования. По аналогии, понятийный дефект или дефект реализации, который обнаруживается при неполадках.

Certificate, public-key certificate – Сертификат, сертификат открытого ключа

Набор данных, выпускаемый органом сертификации (доверенной третьей стороной) и использующийся для обеспечения услуг безопасности (конфиденциальности, аутентификации, целостности). Цифровой сертификат использует шифрование открытым ключом. Сертификат включает значение открытого ключа субъекта, заверенное тем, что данный сертификат подписан выпускающим органом сертификации.

Certification Authority – Органы сертификации (CA)

Доверенная третья сторона для создания, подписания и публикации сертификатов открытого ключа.

Chief Security Officer – Директор по компьютерной безопасности (CSO)

Человек, отвечающий за безопасность систем информационных технологий.

Cipher – Шифр

Алгоритм шифрования, используемый для трансформации простого текста в зашифрованный текст.

Ciphertext – Зашифрованный текст – см. *Cryptogram – Криптограмма.*

Compliance – Соответствие

Согласованность, слаженность, соответствие стандартам.

Confidentiality – Конфиденциальность

Содержание информации и транзакций в секрете. Характерная черта того, что секретно. Цель безопасности – предотвращение раскрытия информации неавторизованным третьим сторонам, а также защита этой информации от прочтения, перехвата и незаконного копирования, намеренного или случайного, при хранении, обработке или передаче (понятие конфиденциальности данных).

Cookies – Кукис, "куки-файл"

Файлы, записываемые на машину пользователя интернета без его ведома при посещении пользователем определенных сайтов, собирающие информацию о пользователе с целью адаптации предлагаемых пользователю веб-услуг.

Countermeasure – Контрмера

Системная функция, мера, процедура или механизм безопасности, предназначенный для снижения уровня уязвимости, а также на борьбу с угрозой ее реализации.

Cryptanalysis – Криптанализ

Набор методов, используемый для анализа ранее зашифрованной информации, для того чтобы расшифровать ее; поэтому криптанализ называют "декодированием". Чем лучше работает система шифрования, тем сложнее становится криптанализ.

Cryptogram, ciphertext – Криптограмма, зашифрованный текст

Данные, которые были криптографически преобразованы. Зашифрованные данные, текст или сообщение. Данные, получаемые в результате шифрования.

Cryptographic algorithm – Алгоритм шифрования

Алгоритм, использующийся для шифрования данных для того, чтобы сделать их конфиденциальными; основан на математической функции и ключе шифрования.

Cryptographic period – Криптографический период

Период времени, в течение которого системные ключи не меняются.

Cryptography – Криптография

Математическое приложение, используемое для записи информации таким образом, чтобы сделать ее непонятной для тех, кто не имеет средств для расшифровки. См. *Шифрование*.

DDoS (distributed denial of service) – Распределенный отказ в обслуживании

Атака насыщения (или отказа в обслуживании), осуществляемая одновременно с нескольких систем.

Digest – Профиль

Строка символов, образующаяся, когда к последовательности данных применяется хэш-функция.

Digital signature – Цифровая подпись

По аналогии с рукописной подписью, цифровая подпись, полученная при помощи асимметричного алгоритма шифрования, используется для аутентификации отправителя сообщения и подтверждения целостности сообщения.

Direct losses – Прямые потери

Определяемые убытки, ставшие непосредственным результатом дефекта безопасности.

Dissuasion – Отговаривание

Средство, использующееся для удерживания нападающих от совершения нападения путем убеждения их в том, что то, что они получат, незначительно по сравнению с потерями, которые может понести система, которой они угрожают.

DoS (denial of service) – Отказ в обслуживании

Атака насыщения, направленная на вызов сбоев в системе так, чтобы она не могла дальше работать должным образом.

Efficiency – Эффективность

Качество того, что имеет ожидаемый эффект, что приносит полезные результаты. Характеристика мер безопасности, являющихся важными и обладающими реальными возможностями защищать ресурс.

Emergency plan – Аварийный план

Набор технических и организационных мер, предназначенных для оптимальной реакции на серьезное происшествие, вредное для организации и влияющее на беспрепятственное выполнение операций.

Encryption, encipherment – Шифрование

Криптографическое преобразование данных (криптограмма) для обеспечения конфиденциальности. Шифрование состоит в том, что для любого, кто не имеет ключа расшифровки, данные становятся непонятными. Простой текст зашифровывается при помощи алгоритма и ключа шифрования, в результате получает зашифрованный текст, который можно расшифровать, используя соответствующий ключ расшифровки (кроме случаев, когда шифрование является необратимым). Операция, обратная шифрованию называется дешифровкой или расшифровкой.

Ethics – Этика

Дисциплина, касающаяся того, что хорошо или плохо. Свод моральных правил, принятых обществом.

Failure – Авария

Неполадки, сбои, делающие ресурс недоступным.

Firewall – Защитная система

Аппаратное или программное обеспечение, используемое для изоляции или маскировки ресурсов, фильтрования данных, контролирования потоков и, следовательно, защиты окружения частной информации организаций, подключенных к интернету.

Flaming – Флэйминг

Метод, состоящий в отправке большого числа неуместных сообщений, для того чтобы подорвать доверие в дискуссионной группе.

Flooder – Флудер

Злонамеренная программа, используемая для замедления связи между поставщиком доступа и пользователем интернета или для отсоединения пользователя.

Hack, Hacker – Взлом, хакер

Акт незаконного проникновения в систему. Человек, который, по какой бы то ни было причине, незаконно проникает в чужую систему без авторизации. Атака может быть активной или пассивной.

Hacking – Хакерство

Ряд действий, совершаемых для повреждения системы информационных технологий.

Hash function – Хэш-функция

В контексте шифрования, хэш-функция также называется функцией профиля (сообщения). Начав с данных сообщения, хэш-функция генерирует профиль сообщения, т. е. своего рода цифровой отпечаток пальца (контрольная сумма файла), который короче исходного сообщения и малопонятен. Затем профиль сообщения зашифровывается при помощи частного ключа отправителя и прикрепляется к передаваемому сообщению. После получения сообщения и контрольной суммы файла получатель расшифровывает контрольную сумму файла при помощи открытого ключа отправителя, пересчитывает контрольную сумму файла полученного сообщения при помощи той же хэш-функции и сравнивает полученное значение с контрольной суммой полученного файла. Если результаты совпадают, получатель убеждается в подлинности отправителя и целостности сообщения, поскольку, если в сообщение были внесены изменения, даже незначительные, контрольная сумма значительно изменится.

Identification – Идентификация

Процесс, в ходе которого можно распознать ранее идентифицированный объект.

Identity – Идентификационная информация

Информация, используемая для обозначения и различения, если возможно уникальным однозначным образом, определенного объекта в домене имен.

Impact – Влияние

Выражает уровень последствий атаки (**финансовое влияние**: издержки на атаку; **логическое влияние**: подрыв доступности, целостности, конфиденциальности; **стратегическое влияние**: подрыв деятельности организации; **материальное влияние**: реальный, непосредственно наблюдаемый эффект).

Impact gravity – Серьезность влияния

Установление серьезности происшествия, утяжеленное частотой возникновения происшествий. Важно измерить серьезность влияния, для того чтобы уточнить и назначить приоритеты требований безопасности. Например: отсутствие влияния/незначительное влияние (0), небольшое влияние (1), умеренное влияние (2), сильное влияние (3), разрушительное влияние (4).

Imputability – Приписываемость

Качество, благодаря которому возможно с уверенностью приписать пользователю операцию, осуществленную в определенное время. Благодаря этому факту можно определить, кто будет нести ответственность в случае нарушения правил.

Indirect losses – Косвенные потери

Потери, косвенно вызванные дефектом безопасности.

Integrity – Целостность

Состояние чего-либо, что остается нетронутым. Критерий безопасности, который, если он соблюдается, позволяет гарантировать, что ресурс не был изменен (модифицирован или уничтожен) незаконным способом.

Intranet – Внутренняя сеть (интранет)

Внутренняя, частная сеть организации, использующая интернет-технологию и обычно изолированная от интернета при помощи защитных систем.

Intrusion detection system (Система обнаружения вторжений) (IDS)

Система, обнаруживающая происшествия, результатом которых могут быть нарушения политики безопасности, а также диагностирующая потенциальные нарушения.

IPSec (Internet Protocol security) – Безопасность протокола Интернет

Версия IP, предлагающая услуги безопасности. IPSec открывает логический канал связи (IP туннель) между двумя корреспондентами в общем интернете. Концы туннеля аутентифицированы, и можно зашифровывать передаваемые по нему данные (понятие зашифрованного канала или виртуальной сети).

IPv6 (Internet Protocol version 6) – Протокол Интернет версия 6

Обновленная версия IPv4, включающая в себя, помимо всего прочего, интегрированные механизмы для реализации услуг безопасности (аутентификация объектов источника и объектов назначения, конфиденциальность передаваемых данных).

Key – Ключ

Ключ шифрования или расшифровки, обычно математическое значение алгоритма шифрования. Если ключи шифрования не являются открытыми ключами, их не следует разглашать: они являются секретным средством защиты другого секрета (информация, которая была зашифрована, для того чтобы гарантировать ее конфиденциальность).

Key management – Управление ключами

Управление ключами шифрования; генерирование, распространение, архивация, уничтожение ключей в ходе реализации политики безопасности.

Logic bomb – Логическая бомба

Злонамеренная программа, запускаемая при определенном событии (таком, как день рождения), предназначенная для нанесения вреда системе, в которой она находится.

Loss of essential service – Потеря важной службы (услуги)

Полная или частичная недоступность или неисправная работа ресурсов, необходимых системе или организации для нормального функционирования.

Malevolent – Злонамеренный

Говорится о враждебных действиях, направленных на повреждение ресурсов организации. Такие действия могут совершаться напрямую или косвенно людьми внутри организации или вне ее (кража аппаратного обеспечения, данных, разглашение конфиденциальной информации, нарушения и т. д.).

Malware – Злонамеренное программное обеспечение

Общий термин, относящийся к программам таким, как вирус, червь или "Троянский конь" или любой другой форме атакующего программного обеспечения, действующего более или менее независимо.

Masquerade – Имитация

Тип атаки, основанный на заманивании системы в ловушку.

Non-repudiation – Неотказуемость

Возможность не допустить, что отправитель отрицает отправку сообщения или выполнение действия. Гарантии доступности улик, которые можно передать третьей стороне и использовать для доказательства того, что событие или действие произошло. Доказательство того, что сообщение было отправлено определенным лицом в определенное время и не было модифицировано впоследствии. Третья сторона должна подтвердить подлинность таких доказательств в любое время. Без неотказуемости, отправители сообщений и получатели могут отрицать получение или отправку указанной информации.

No-opt – Без выбора

Услуга, при которой клиенты не могут выбирать, как используется информация о них (возможно, нарушается их право на цифровую приватность).

Notarization – Подтверждение подлинности, заверение

Регистрация данных для доказательства.

One-way hash function – Однонаправленная хэш-функция

Функция, которую можно использовать для вычисления контрольной суммы данных, но не для генерирования данных, имеющих определенную контрольную сумму. Данной функции нужно избегать противоречий, т. е. когда один и тот же профиль генерируется из разных сообщений.

Passive attack – Пассивная атака

Атака, не изменяющая цель (пассивное прослушивание, нарушение конфиденциальности).

Password – Пароль

Конфиденциальная информация, предоставляемая авторизованным пользователем для доказательства своей подлинности во время процедуры аутентификации при запросе доступа к ресурсу.

Patch – Заплата, файл с исправлениями

Обновление программного обеспечения, направленное на ликвидацию слабых мест, обнаруженных после установки программного обеспечения.

Penetration tests – Испытания на проникновение

Используются для анализа и проверки степени защиты систем и качества работы механизмов безопасности.

Phreaking – Взлом, фрикинг

Незаконное или неправильное использование услуг электросвязи за счет частного лица или оператора (сетевым взломщиком).

Prevention – Предотвращение, превентивность

Набор мер, предпринимаемых для предотвращения опасности и рисков, направленных на предотвращение угроз, а также на сокращение частоты происшествий для обеспечения защиты.

Privacy protection – Защита приватности

Защитные меры для гарантии того, что информация о деятельности пользователя интернета не разглашается нежелательным сторонам и не используется для целей, на которые обладатель этой информации не дал согласия. Защита приватности относится к праву частных лиц проверять подлинность касающейся их информации, которую можно собирать напрямую или косвенно при помощи наблюдения за их работой в интернете и за тем, какие сайты они посещают.

Private key – Секретный ключ

Ключ, используемый в асимметричных механизмах шифрования (шифрование открытым ключом), который принадлежит объекту и должен держаться в секрете.

Privilege-management infrastructure (PMI) – Инфраструктура управления привилегиями

Инфраструктура, поддерживающая управление привилегиями, авторизацией и допуском к закрытой информации.

Protection – Защита

Действие по охране, состояние защищенности. Говорится о мере безопасности, которая помогает обнаружить, нейтрализовать или сократить эффект от атаки.

Public key – Открытый ключ

В асимметричном шифровании – открытый ключ объекта нужно сделать доступным для тех, кто хочет отправлять этому объекту зашифрованные данные, с тем чтобы этот объект мог расшифровать данные, используя соответствующий частный ключ.

Шифрование открытым ключом

Система асимметричного шифрования, использующая шифр из двух ключей или пару ключей, один из которых является секретным ключом, а другой – открытым ключом, который можно публиковать. Два ключа дополняют друг друга и неотделимы друг от друга. Использовать математическую связь между ключами для вычисления частного ключа невозможно.

Public key infrastrusture – Инфраструктура открытых ключей (PKI)

Инфраструктура, поддерживающая реализацию асимметричного шифрования (шифрования открытым ключом), а также, помимо всего прочего, управление и распределение ключей шифрования и цифровых сертификатов.

Reliability – Надежность

Способность системы бесперебойно работать в течение заданного периода времени.

Repudiation – Отказуемость

Факт отрицания того, что кто-то принимал участие во всем или части обмена.

Revocation – Аннулирование

Уведомление о том, что частный ключ потерял свою целостность. Соответствующий сертификат открытого ключа больше использовать нельзя. Что касается контрактов, аннулирование также относится к праву отзыва оферты или акцептования оферты.

Risk – Риск

Относительная вероятность того, что угроза материализуется, измеряемая в выражении вероятности и влияния.

Risk analysis, risk assessment – Анализ риска, управление рисками

Процесс определения и оценки рисков (оценка вероятности возникновения и влияния).

Risk management – Управление рисками

Постоянный процесс оценки рисков, выполняемый организацией, для того чтобы контролировать риски и удерживать их на приемлемом уровне. Может использоваться для определения политики безопасности, наилучшим образом адаптированной для защиты имущества организации.

Sabotage – Саботаж

Злонамеренное действие, вандализм, намеренное причинение вреда, нацеленное на нарушение нормальной работы организации, инфраструктуры, услуги или ресурса; может привести к потерям.

Safety – Безопасность

Качество того, что не является вредоносным.

Secure sockets layer – Протокол-слой безопасных соединений (SSL)

Программное обеспечение, используемое для защиты обменов через интернет, разработанное компанией Netscape и поддерживаемое большинством веб-браузеров на рынке.

Security – Безопасность

Ситуация, при которой кто-либо или что-либо не подвергается никакой опасности. Механизм, направленный на предотвращение вредоносного события или на ограничение последствий такого события. **Физическая безопасность**, например, относится к мерам, предпринимаемым для защиты окружения с физической и материальной точек зрения, в то время как **логическая безопасность** относится к процедурам программного обеспечения и средствам защиты.

Security administrator – Администратор по безопасности

Частное лицо, ответственное за установление или реализацию всей или части политики безопасности.

Security audit – Проверка безопасности

Методический анализ всех компонентов, участников, политик, мер, решений, процедур и средств безопасности, используемых организацией для защиты окружения, выполняемый с целью проверки на соответствие, оценивающий соотношение между развертываемыми организационными, техническими, человеческими и финансовыми ресурсами и существующими рисками, а также действиями по оптимизации, рационализации и улучшению.

Security measures – Меры безопасности

Все технические, организационные, юридические, финансовые, человеческие, процедурные ресурсы и способы действия, используемые для достижения целей безопасности, устанавливаемых политикой безопасности. Обычно они классифицируются по функциональной роли (превентивные меры, меры защиты, сдерживающие меры и т. д.).

Security need – Нужды безопасности

Для среды, требующей защиты, определение и выражение уровней готовности, целостности и конфиденциальности, связанных с ресурсами и ценностями, требующими защиты.

Security policy – Политика безопасности

Система отсчета безопасности, установленная организацией, отражающая ее стратегию безопасности и устанавливающая средства реализации.

Sensitivity – Чувствительность, уязвимость

Характеристика объекта, показывающая его значимость или важность.

Session key – Ключ сеанса связи

Секретный ключ, генерируемый при помощи системы асимметричного шифрования, когда корреспонденты открывают рабочий сеанс, время существования которого ограничено данным сеансом; данный ключ используется для шифрования больших объемов данных при помощи алгоритма симметричного шифрования.

S-http

Защищенная версия протокола http, разрешающая защищенные обмены между клиентом и веб-сервером.

Sniffer – Сниффер

Программное обеспечение, используемое для прослушивания данных, передаваемых по сети.

Sniffing – Пассивное прослушивание сети

Действие по пассивному прослушиванию для получения параметров соединения, которые затем используются без ведома их законных владельцев для совершения нарушений.

Social engineering – Бытовая махинация

Методы, процедуры и способы, используемые злонамеренными нападающими, которые обычно пользуются доверчивостью пользователей, для того чтобы получить их пароли и параметры соединения и присвоить их цифровую идентификационную информацию для проникновения в систему под видом авторизованных пользователей.

Spammer – Спаммер

Кто-то, занимающийся спамом.

Spam – Спам

Техника, включающая в себя отправку незатребованных сообщений системе электронных сообщений.

Spoofer – Спуфер

Кто-либо, занимающийся получением доступа обменным путем.

Spoofing – Спуфинг – Имитация соединения, получение доступа обманным путем

Техника, используемая для присвоения IP адресов для проникновения в систему.

Spyware – Шпионящее программное обеспечение

Программа, отправляющая нападающему важную информацию от инфицированного компьютера.

Steganography – Стеганография

Метод, используемый для сокрытия информации внутри другой информации для тайной передачи или хранения. "Водяные знаки" – это стеганографическое приложение, состоящее в помещении на изображение неудаляемых знаков.

Threat – Угроза

Признак, указание, предвестник опасности. Действие или событие, которое вероятно произойдет, станет атакой на окружение или ресурс и нарушит безопасность.

Traffic analysis – Анализ трафика

Наблюдение за потоками информации между объектами источника и места назначения и изучение их (присутствие, отсутствие, количество, направление, частота и т. д.).

Trapdoor – see *Backdoor* – Черный ход – см. *Лазейка*

Trojan horse – "Троянский конь"

Злонамеренная программа, скрытая внутри легальной программы и внедряющаяся в системы с целью нанесения ущерба (похищение времени процессора, искажение, изменение, уничтожение данных и программ, нарушение функционирования, прослушивание и т. д.).

Trust – Доверие

Уверенность в ком-либо или в чем-либо (качественный, субъективный и довольно относительный критерий).

User charter – Устав пользователя

Документ, составляемый организацией, в котором перечисляются права и обязанности работников этой организации в отношении использования информационных технологий и ресурсов электросвязи, которые предоставляет им данная организация; подписывается заинтересованными сторонами.

User profile – Профиль пользователя

Список атрибутов пользователя, помогающих управлять сетями и системами, к которым подключены данные пользователи (параметры идентификации и аутентификации, права доступа, авторизации и другая полезная информация), для управления доступом, составления счетов и т. д.

Virtual private network – Виртуальная частная сеть (VPN)

Это понятие относится к использованию протокола IPSec для открытия частного канала связи внутри незащищенной общей сети. Часто используется организациями для подключения к различным сайтам компании через интернет при сохранении конфиденциальности передаваемых данных.

Virus – Вирус

Злонамеренная программа, внедряемая в систему без ведома пользователя. Программа обладает способностью к самокопированию (в том же виде или, в случае полиморфного вируса, в измененном виде), может повредить окружение, в котором выполняется, а также заразить других пользователей, с которыми данная система состоит в контакте. Существуют различные виды вирусов в зависимости от сигнатуры, поведения, метода воспроизводства, инфицирования машин, вызываемых неполадок и т. д. **Черви**, "**Троянские кони"** и **логические бомбы** являются злонамеренными кодами, которые принадлежат к общему семейству вирусов.

Vulnerability – Уязвимость

Дефект безопасности, который может привести к намеренному или случайному нарушению политики безопасности.

Приложение B – Оглавление стандарта ИСО/МЭК 17799:2005, которое служит в качестве справочника для управления безопасностью

Введение
- 0.1 Что такое информационная безопасность?
- 0.2 Зачем нужна информационная безопасность?
- 0.3 Как установить требования безопасности
- 0.4 Определение рисков безопасности
- 0.5 Выбор средств контроля
- 0.6 Отправная точка информационной безопасности
- 0.7 Важные факторы успеха
- 0.8 Разработка своих собственных рекомендаций

1 Область применения

2 Термины и определения

3 Структура данного стандарта
- 3.1 Пункты
- 3.2 Основные категории безопасности

4 Оценка и снижение рисков
- 4.1 Определение рисков безопасности
- 4.2 Снижение рисков безопасности

5 Политика безопасности
- 5.1 Политика информационной безопасности
  - 5.1.1 Документ политики информационной безопасности
  - 5.1.2 Обзор политики информационной безопасности

6 Организация информационной безопасности
- 6.1 Внутренняя организация
  - 6.1.1 Обязательства управления по отношению к информационной безопасности
  - 6.1.2 Координация информационной безопасности
  - 6.1.3 Распределение ответственности за информационную безопасность
  - 6.1.4 Процесс авторизации средств обработки информации
  - 6.1.5 Соглашения о конфиденциальности
  - 6.1.6 Взаимодействие с властями
  - 6.1.7 Взаимодействие с группами лиц, имеющими общие интересы
  - 6.1.8 Независимый обзор информационной безопасности
- 6.2 Внешние участники
  - 6.2.1 Определение рисков, связанных с внешними участниками
  - 6.2.2 Обеспечение безопасности при работе с клиентами
  - 6.2.3 Обеспечение безопасности в соглашениях с третьей стороной

7 Управление имуществом
- 7.1 Ответственность за имущество
  - 7.1.1 Опись имущества
  - 7.1.2 Владение имуществом
  - 7.1.3 Приемлемое использование имущества
- 7.2 Классификация информации
  - 7.2.1 Рекомендации по классификации
  - 7.2.2 Маркировка и обработка информации

8 Безопасность человеческих ресурсов
- 8.1 До приема на работу
  - 8.1.1 Роли и ответственность
  - 8.1.2 Отбор
  - 8.1.3 Постановления и условия приема на работу
- 8.2 Во время работы
  - 8.2.1 Управление ответственностью
  - 8.2.2 Осведомленность, образование и подготовка в области информационной безопасности
  - 8.2.3 Дисциплинарный процесс
- 8.3 Прекращение или смена работы
  - 8.3.1 Прекращение ответственности
  - 8.3.2 Возвращение имущества
  - 8.3.3 Аннулирование прав доступа

9 Физическая безопасность и безопасность окружения
- 9.1 Защищенные области
  - 9.1.1 Границы физической безопасности
  - 9.1.2 Физические средства управления точками входа
  - 9.1.3 Обеспечение безопасности офисов, комнат и оборудования
  - 9.1.4 Защита от внешних угроз и угроз окружения
  - 9.1.5 Работа в защищенных областях
  - 9.1.6 Области доступа, доставки и загрузки
- 9.2 Безопасность оборудования
  - 9.2.1 Размещение и защита оборудования
  - 9.2.2 Служебные программы поддержки
  - 9.2.3 Безопасность кабельной системы
  - 9.2.4 Поддержка оборудования
  - 9.2.5 Безопасность оборудования вне помещения
  - 9.2.6 Безопасная передача или повторное использование оборудования
  - 9.2.7 Удаление собственности

10 Управление связями и процессами
- 10.1 Оперативные процедуры и ответственность
  - 10.1.1 Документированные способы эксплуатации
  - 10.1.2 Управление изменениями
  - 10.1.3 Отделение обязанностей
  - 10.1.4 Разделение возможностей развития, испытания и работы
- 10.2 Управление поставкой услуги третьей стороной
  - 10.2.1 Поставка услуги
  - 10.2.2 Наблюдение и пересмотр услуг третьей стороны
  - 10.2.3 Замена управления на услуги третьей стороны
- 10.3 Системное планирование и одобрение
  - 10.3.1 Управление возможностями
  - 10.3.2 Одобрение системы
- 10.4 Защита от злонамеренного и мобильного кода
  - 10.4.1 Средства управления против злонамеренного кода
  - 10.4.2 Средства управления против мобильного кода

10.5 Резервное копирование
10.5.1 Резервное копирование информации
10.6 Управление сетевой безопасностью
10.6.1 Управление сетью
10.6.2 Безопасность сетевых услуг
10.7 Работа с носителями данных
10.7.1 Управление съемными носителями данных
10.7.2 Размещение носителей данных
10.7.3 Процедуры обработки информации
10.7.4 Безопасность системной документации
10.8 Обмен информацией
10.8.1 Политика и процедуры обмена информацией
10.8.2 Соглашения об обмене
10.8.3 Физические носители данных в пути
10.8.4 Электронные сообщения
10.8.5 Системы деловой информации
10.9 Услуги электронной коммерция
10.9.1 Электронная коммерция
10.9.2 Транзакции в интернете
10.9.3 Общедоступная информация
10.10 Мониторинг
10.10.1 Контрольная регистрация
10.10.2 Использование систем мониторинга
10.10.3 Защита информации в журналах регистрации
10.10.4 Журналы регистрации администратора и оператора
10.10.5 Регистрация сбоев
10.10.6 Тактовая синхронизация

11 Управление доступом
11.1 Коммерческие требования, предъявляемые к управлению доступом
11.1.1 Политика управления доступом
11.2 Управление доступом пользователя
11.2.1 Регистрация пользователя
11.2.2 Управление привилегиями
11.2.3 Управление паролем пользователя
11.2.4 Обзор прав доступа пользователя
11.3 Ответственность пользователя
11.3.1 Использования пароля
11.3.2 Необслуживаемое оборудование пользователя
11.3.3 Политика "чистый стол – чистый экран"
11.4 Управление доступом к сети
11.4.1 Политика по использованию сетевых услуг
11.4.2 Аутентификация пользователя для внешних соединений
11.4.3 Идентификация оборудования в сетях
11.4.4 Удаленная защита диагностики и конфигурации порта
11.4.5 Изоляция в сетях
11.4.6 Управление сетевым соединением
11.4.7 Контроль сетевой маршрутизации

- 11.5 Контроль доступа операционной системы
  - 11.5.1 Защищенные процедуры регистрации абонента
  - 11.5.2 Идентификация и аутентификация пользователя
  - 11.5.3 Система управления паролем
  - 11.5.4 Использование системных утилит
  - 11.5.5 Прерывание сессии
  - 11.5.6 Ограничения времени соединения
- 11.6 Управление доступом для приложений и информации
  - 11.6.1 Ограничения в доступе к информации
  - 11.6.2 Изоляция чувствительной системы
- 11.7 Мобильные вычисления и телеработа
  - 11.7.1 Мобильные вычисления и связь
  - 11.7.2 Телеработа

12 Создание, развитие и поддержка информационных систем
- 12.1 Требования к информационным системам, касающиеся безопасности
  - 12.1.1 Анализ и определение требований безопасности
- 12.2 Правильная обработка в приложениях
  - 12.2.1 Подтверждение входных данных
  - 12.2.2 Контроль внутренней обработки
  - 12.2.3 Целостность сообщения
  - 12.2.4 Подтверждение выходных данных
- 12.3 Криптографические средства управления
  - 12.3.1 Политика использования криптографических средств управления
  - 12.3.2 Управление ключами
- 12.4 Безопасность системных файлов
  - 12.4.1 Контроль операционного программного обеспечения
  - 12.4.2 Защита тестовых данных системы
  - 12.4.3 Управление доступом к исходному тексту программы
- 12.5 Безопасность процессов развития и поддержки
  - 12.5.1 Процедуры управления изменениями
  - 12.5.2 Технический обзор приложений после смены операционной системы
  - 12.5.3 Ограничения, налагаемые на изменения в пакетах программного обеспечения
  - 12.5.4 Утечка информации
  - 12.5.5 Разработка программного обеспечения, порученная соисполнителю
- 12.6 Управление технической уязвимостью
  - 12.6.1 Контроль технической уязвимости

13 Управление инцидентами в области информационной безопасности
- 13.1 Сообщение о событиях и недостатках информационной безопасности
  - 13.1.1 Сообщение о событиях безопасности
  - 13.1.2 Сообщение о недостатках безопасности
- 13.2 Управление инцидентами и усовершенствованиями в области безопасности
  - 13.2.1 Ответственность и процедуры
  - 13.2.2 Получение опыта из инцидентов в области безопасности
  - 13.2.3 Сбор улик

14 Управление непрерывностью ведения бизнеса
- 14.1 Аспекты информационной безопасности управления непрерывностью бизнеса
  - 14.1.1 Включение информационной безопасности в процесс управления непрерывностью ведения бизнеса
  - 14.1.2 Непрерывность бизнеса и определение риска
  - 14.1.3 Разработка и реализация долгосрочных планов, включающих безопасность информации
  - 14.1.4 Структура планирования непрерывности бизнеса
  - 14.1.5 Проверка, поддержка и переоценка планов непрерывности бизнеса

15 Совместимость
- 15.1 Совместимость в юридическими требованиями
  - 15.1.1 Определение применяющегося законодательства
  - 15.1.2 Права интеллектуальной собственности (IPR)
  - 15.1.3 Защита записей организации
  - 15.1.4 Защита данных и тайна личной информации
  - 15.1.5 Предотвращение неправильного использования оборудования, обрабатывающего большие количества
  - 15.1.6 Регулирование криптографических средств управления
- 15.2 Совместимость со стандартами и политикой безопасности, также как техническая совместимость
  - 15.2.1 Совместимость с политикой и стандартами безопасности
  - 15.2.2 Проверка технической совместимости
- 15.3 Вопросы проверки информационных систем
  - 15.3.1 Средства управления информационными системами
  - 15.3.2 Защита инструментов проверки информационных систем

Библиография и указатели

Приложение C – Мандат и деятельность МСЭ-D в области кибербезопасности

Более подробную информацию
см. на веб-сайте: www.itu.int/ITU-D/cybersecurity

Совпадение приоритетов и действий данной Программы в области кибербезопасности и борьбы со спамом, и Женевского плана действий ВВУИО и Тунисской программы можно увидеть по почти идентичному сопоставлению, приведенному ниже. В Тунисской программе 2005 года МСЭ была определена в качестве ведущей организации для содействия и продвижения действий, направленных на реализацию Женевского плана действий в области укрепления доверия и безопасности при использовании ИКТ. В Дохинском плане действий, принятом на Всемирной конференции по развитию электросвязи МСЭ в марте 2006 года, члены МСЭ решили, что кибербезопасность и борьба со спамом являются в Программе 3 приоритетными.

Направление действия C.5 ВВУИО (Укрепление доверия и безопасности при использовании ИКТ) и Мандат МСЭ в области безопасности и борьбы со спамом

Направление действия ВВУИО C.5	Отношение Мандата МСЭ к C.5
12. Доверие и безопасность относятся к главным опорам информационного общества.	Реагирование на проблемы кибербезопасности для реализации потенциала сетей для предоставления защищенных и доступных приложений электронных услуг.
a) Содействовать сотрудничеству между государствами в рамках Организации Объединенных Наций и со всеми заинтересованными сторонами в рамках соответствующих форумов с целью укрепления доверия пользователей, повышения надежности и защиты целостности как данных, так и сетей; анализа существующих и потенциальных угроз в области ИКТ; а также решения других вопросов информационной безопасности и безопасности сетей.	Для сведения к минимуму, предотвращения и выявления киберугроз необходимо также содействовать дальнейшему расширению охвата и сотрудничества в целях сбора и распространения информации, касающейся кибербезопасности; а также наладить обмен передовым опытом для оказания эффективной взаимной помощи, принятия ответных мер и исправления ситуации среди членов и между правительственными органами, деловыми кругами и гражданским обществом.
b) Органам государственного управления в сотрудничестве с частным сектором необходимо предупреждать, обнаруживать проявления киберпреступности и ненадлежащего использования ИКТ и реагировать на эти проявления путем разработки руководящих принципов, которые учитывали бы ведущуюся в этой области работу; изучения законодательства, которое дает возможность эффективно расследовать и подвергать преследованию ненадлежащее использование; содействия эффективным мерам взаимопомощи; усиления на международном уровне институциональной поддержки профилактики таких инцидентов, их обнаружения и ликвидации их последствий; а также путем содействия образованию и повышению осведомленности.	Разработка руководящих указаний, инструментария для планирования и подготовка пособий по техническим и политическим аспектам кибербезопасности. Разработка набора руководств по кибербезопасности, предназначенных для органов, ответственных за выработку политики, и других соответствующих секторов. Предоставление помощи Государствам – Членам Союза в разработке законов и типового законодательства по предупреждению киберпреступности. Разработка учебных материалов по техническим стратегиям и техническому развитию для внедрения кибербезопасности.

Направление действия ВВУИО С.5	Отношение Мандата МСЭ к С.5
c) Органы государственного управления и другие заинтересованные стороны должны активно поощрять обучение пользователей и повышать их осведомленность относительно неприкосновенности частной жизни при работе в онлайновом режиме и способов ее защиты.	Содействие в повышении уровня осведомленности и выявление ключевых вопросов в целях поддержания культуры кибербезопасности и подготовка рекомендаций относительно примеров передового опыта по поддержке приложений на базе ИКТ и минимизации киберугроз
d) Принимать необходимые меры на национальном и международном уровнях для защиты от спама.	Разработка общего понимания по вопросам о спаме, а также киберугрозах, включая принятие контрмер. Принятие во внимание, по мере необходимости, соответствующей работы других заинтересованных сторон: ОЭСР, сторон основных соглашений по кибербезопасности и борьбе со спамом.
e) 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.	Организация практикумов, собраний и семинаров для решения технических, правовых, политических и стратегических задач, касающихся кибербезопасности. Предоставление помощи Государствам – Членам Союза в разработке законов и типового законодательства по предупреждению киберпреступности.
f) Продолжать укрепление надежности 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 данных и прав потребителей.	Определение потребностей в сфере кибербезопасности и предложение вариантов развития защищенных приложений на базе ИКТ. Содействие в повышении уровня осведомленности и выявление ключевых вопросов в целях поддержания культуры кибербезопасности и подготовка рекомендаций относительно примеров передового опыта по поддержке приложений на базе ИКТ и минимизации киберугроз.
g) Обмениваться образцами наилучшей практики в области информационной безопасности и безопасности сетей и поощрять их использование всеми заинтересованными сторонами.	Разработка инструментария для содействия совместному использованию информации по вопросам технологий и политики и примеров передового опыта, относящихся к кибербезопасности. Посредничество в региональном и межрегиональном сотрудничестве, а также поддержка соответствующих инициатив по созданию потенциала на региональном уровне.

Направление действия ВВУИО С.5	Отношение Мандата МСЭ к С.5
h) Предложить заинтересованным странам назначить координаторов для реагирования в режиме реального времени на происшествия в сфере безопасности и объединить этих координаторов в открытую совместную сеть для обмена информацией и технологиями реагирования на происшествия.	Сюда можно было бы отнести, в том числе, разработку меморандумов о взаимопонимании (МоВ) между заинтересованными Государствами – Членами Союза в целях повышения кибербезопасности. С участием нескольких заинтересованных сторон реализовать Проект, [...] вырабатывающий решения в нескольких областях, включая: 1 Назначение координаторов на национальном уровне. 2 Реагирование на инциденты, наблюдение за ними и извещение о них Анализ примеров передового опыта по созданию и эксплуатации средств слежения, оповещения, реагирования на случаи нарушения безопасности, а также восстановления безопасности, которые могут использовать Государства – Члены Союза для создания своих национальных средств.
i) Поощрять дальнейшее развитие безопасных и надежных приложений для упрощения осуществления сделок в онлайновом режиме.	Определение потребностей в сфере кибербезопасности и предложение вариантов развития защищенных приложений на базе ИКТ.
j) Поощрять активное участие заинтересованных стран в проводимой Организацией Объединенных Наций деятельности по укреплению доверия и надежности при использовании ИКТ.	Привлечение Государств-Членов, Членов секторов и ассоциативных членов МСЭ: Делать вклады для 1-й Исследовательской комиссии МСЭ-D по данному вопросу и участвовать в осуществлении проектов Бюро развития электросвязи. Содействовать укреплению доверия и безопасности при использовании ИКТ на национальном, региональном и международном уровнях при помощи действий, описанных в пункте 12[64] Женевского плана действий.

[64] Пункт 12 – это полный текст Направления действия С.5 ВВУИО, приведенный в колонке 1 данного документа.

Мандат МСЭ-D в области кибербезопасности и борьбы со спамом

В рамках решений, принятых членами МСЭ на Полномочных конференциях МСЭ 2002 и 2006 годов (ПК02 и ПК06), а также Всемирных конференций по развитию электросвязи 2002 и 2006 годов (ВКРЭ-02 и ВКРЭ-06), Мандат МСЭ-D в области кибербезопасности, киберугроз и борьбы со спамом включен в следующие решения:

1 Программа 3 ВКРЭ-02 и ВКРЭ-06 – Электронные стратегии и приложения на базе ИКТ.

2 Резолюция 45 ВКРЭ-06 – Механизмы совершенствования сотрудничества в области кибербезопасности, включая борьбу со спамом.

3 Приложение 2 к Резолюции 2 ВКРЭ-06 – Вопрос 22 1-й Исследовательской комиссии МСЭ-D – Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности.

4 Резолюция 130 (Пересм. Анталия 2006 г.) – Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий.

1 Программа 3, Дохинский план действий ВКРЭ-2006 (электронные стратегии и приложения ИКТ)

Приоритеты

a) Проблемы кибербезопасности следует рассматривать в рамках настоящей Программы, с тем чтобы реализовать потенциал сетей для предоставления защищенных и доступных электронных услуг и приложений.

b) В настоящей Программе должно быть также разработано общее понимание по вопросам о спаме, а также киберугрозах, включая принятие контрмер.

c) Для сведения к минимуму, предотвращения и выявления киберугроз необходимо также содействовать дальнейшему расширению охвата и сотрудничества в целях сбора и распространения информации, касающейся кибербезопасности; а также наладить обмен передовым опытом для оказания эффективной взаимной помощи, принятия ответных мер и исправления ситуации среди членов и между правительственными органами, деловыми кругами и гражданским обществом.

d) БРЭ должно также играть содействующую роль в региональном и межрегиональном сотрудничестве, а также поддерживать соответствующие инициативы по созданию потенциала на региональном уровне.

e) Сюда можно было бы отнести, в том числе, разработку меморандумов о взаимопонимании (МоВ) между заинтересованными Государствами – Членами Союза в целях повышения кибербезопасности.

Задачи

a) Разработка руководящих указаний, инструментария для планирования и подготовка руководств по техническим и политическим аспектам кибербезопасности.

b) Разработка набора руководств по кибербезопасности, предназначенных для органов, ответственных за выработку политики, и других соответствующих секторов.

c) Разработка учебных материалов по техническим стратегиям и техническому развитию для внедрения кибербезопасности.

d) Организация практикумов, собраний и семинаров для решения технических, правовых, политических и стратегических задач, касающихся кибербезопасности.

e) Предоставление помощи Государствам – Членам Союза в разработке законов и типового законодательства по предупреждению киберпреступности.

f) Определение потребностей в сфере кибербезопасности и предложение вариантов развития защищенных приложений на базе ИКТ. Содействие в повышении уровня осведомленности и выявление ключевых вопросов в целях поддержания культуры кибербезопасности и подготовка рекомендаций относительно примеров передового опыта по поддержке приложений на базе ИКТ и минимизации киберугроз.

g) Разработка инструментария для содействия совместному использованию информации по вопросам технологий и политики и примеров передового опыта, относящихся к кибербезопасности.

h) Принятие во внимание, по мере необходимости, соответствующей работы других заинтересованных сторон: ОЭСР, сторон основных соглашений по кибербезопасности и борьбе со спамом, таких как *Лондонский план действий* и *Меморандум о взаимопонимании по противодействию спаму Сеул-Мельбурн*.

2 Резолюция 45 ВКРЭ-2006 – Механизмы укрепления сотрудничества в области кибербезопасности, включая борьбу со спамом (выдержки)

напоминая

предоставляемую ею существенную поддержку Программе 3 (Электронные стратегии и приложения на базе ИКТ), подтверждая, что в рамках этой программы будут выполняться основные задачи по Направлению деятельности С5 Тунисской программы "Укрепление доверия и безопасности при использовании ИКТ",

отмечая,

что Резолюция 50 (Флорианополис, 2004 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) по кибербезопасности посвящена исключительно исследованию технических аспектов уменьшения воздействия этого явления;

настоятельно призывает Государства – Члены Союза

предоставить необходимую поддержку в выполнении настоящей Резолюции,

решает

поручить Директору Бюро развития электросвязи

a) организовать, в соответствии с Программой 3 и на основе вкладов членов, собрания Государств – Членов Союза и Членов Сектора для обсуждения путей повышения кибербезопасности, включая, среди прочего, заключение МоВ между заинтересованными Государствами – Членами Союза с целью повышения кибербезопасности и борьбы со спамом;

b) представить отчет о результатах этих собраний Полномочной конференции (Анталия, 2006 г.).

Итог Резолюции 45: Проект по укреплению сотрудничества в области кибербезопасности и борьбы со спамом

Сектору развития электросвязи в соответствии с Программой 3 с участием нескольких заинтересованных сторон разработать глобальный Проект, связывающий существующие инициативы и задачу реагировать на нужды развивающихся стран.

Данный проект, начало которого запланировано на 2007 год, будет сосредоточен на выработке решений в следующих областях:

1 Сильное законодательство.

2 Разработка технических мер.

3 Создание промышленных партнерств, особенно с поставщиками услуг интернета, операторами подвижной связи и ассоциациями по прямому маркетингу.

4 Осведомленность заказчиков и представителей отрасли о мерах противодействия спаму и примерах передового опыта в области безопасности интернета.

5 Международное сотрудничество на уровне правительств, отрасли, заказчиков, коммерческих предприятий и групп по противодействию спаму для обеспечения глобального и скоординированного подхода к данной проблеме.

В дополнение к перечисленному выше в ходе обсуждений и выступлений были также определены направления, представленные далее без разбивки по приоритетному значению, также являющиеся важными для сотрудничества и оказания содействия Государствам-Членам, которые МСЭ-D может осуществлять совместно с объединениями, обладающими признанным опытом в области кибербезопасности и борьбы со спамом:

a) Формирование общего представления о проблеме.

b) Соответствующее национальное законодательство.

c) Создание человеческого и организационного потенциала.

d) Правоприменительная деятельность (в сфере создания потенциала).

e) Национальная политика и стратегии в области кибербезопасности.

f) Обмен информацией между странами и соответствующими заинтересованными сторонами.

g) Назначение национальных координаторов.

h) Мониторинг и оценка хода выполнения существующих инициатив.

i) Реагирование на происшествия, наблюдение и предупреждение.

j) Оценка уязвимых мест и угроз в области кибербезопасности.

k) Эффективные инструменты и приложения для сети и кибербезопасности.

l) Партнерства.

m) Международное сотрудничество.

Информация по проекту:

– Проект под названием "Проект по расширению сотрудничества в области кибербезопасности и борьбы со спамом" будет длиться 4 года начиная с 2007 года и являться частью оперативного плана БРЭ на 2007 год.

– На сессиях Совета МСЭ будут предоставляться ежегодные отчеты о ходе деятельности по его выполнению.

– При выполнении проекта следует учитывать решения ВКРЭ-06, касающиеся мандата Сектора развития в области кибербезопасности и борьбы со спамом.

– Проект должен быть в первую очередь направлен на оказание содействия развивающимся странам в вышеуказанных областях путем налаживания жизненно важного сотрудничества в области кибербезопасности и борьбы со спамом.

– В отношении соответствующего законодательства следует должным образом учитывать работу в данной области Совета Европы по оказанию содействия странам в разработке национального законодательства, соответствующего положениям Конвенции о борьбе с киберпреступностью.

– Осуществление деятельности в рамках данного проекта должно основываться на поступивших от стран просьбах, особое внимание уделяя развивающимся странам.

– После разработки проект должен быть представлен потенциальным финансирующим объединениям, включая Государства-Члены, частный сектор и международные организации, такие как Всемирный банк и Европейская комиссия.

3 Резолюция 2 ВКРЭ-2006 – Вопрос 22 1-й Исследовательской комиссии МСЭ-D – Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности

a) Провести обзор, составить каталог, дать описание и повысить уровень осведомленности по:

- основным проблемам, с которыми сталкиваются национальные органы, отвечающие за выработку политики, и все заинтересованные стороны при формировании культуры кибербезопасности,
- основным источникам информации и помощи в области формирования культуры кибербезопасности,
- успешным примерам передового опыта, накопленного национальными органами, отвечающими за выработку политики, работе со всеми заинтересованными сторонами в области обеспечения кибербезопасности и формировании культуры кибербезопасности,
- специфическим проблемам, с которыми сталкиваются развивающиеся страны при решении вопроса защиты сетей, а также примерам передового опыта в этой области;

b) Проанализировать примеры передового опыта по созданию и эксплуатации средств слежения, оповещения, реагирования на случаи нарушения безопасности, а также восстановления безопасности, которые могут использовать Государства – Члены Союза при создании своих национальных возможностей.

Предоставлять отчет или отчеты для членов по вопросам, указанным в разделе 2, выше. Такой(ие) отчет(ы) будет(ут) отражать информацию о том, что защищенные информационно-коммуникационные сети неразрывно связаны с построением информационного общества и с социально-экономическим развитием всех стран.

4 Резолюция 130 (Пересм. Анталия 2006 г.) – Усиление роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий

решает

придать этой работе в рамках МСЭ высокий приоритет в соответствии с его сферами компетенции и опытом,

поручает Генеральному секретарю и директорам Бюро

1 проанализировать:

i) работу, проделанную на настоящее время МСЭ и другими соответствующими организациями, и инициативы по противодействию с существующим и будущим угрозам таким, как вопросы противодействия спаму, для того чтобы укрепить доверие и безопасность при использовании ИКТ;

ii) ход работы по выполнению настоящей Резолюции и роль МСЭ как ведущей/содействующей организации по Направлению деятельности С5 ВВУИО при помощи консультативных групп, в соответствии с Уставом и Конвенцией МСЭ;

2 способствовать доступу к инструментам, необходимым для укрепления доверия и безопасности при использовании ИКТ, для всех Государств-Членов, в соответствии с разработанными ВВУИО положениями об универсальном и недискриминационном доступе к ИКТ для всех стран;

3 продолжать поддерживать портал кибербезопасности как средство совместного использования информации о национальных, региональных и международных инициативах, связанных с кибербезопасностью во всем мире;

4 ежегодно представлять Совету отчет об этой деятельности и, в надлежащих случаях, вносить предложения,

поручает Директору Бюро развития электросвязи

1 разрабатывать, в соответствии с результатами ВКРЭ-06 и проведенного затем, во исполнение Резолюции 45 (Доха, 2006 г.) этой конференции, собрания, проекты расширения сотрудничества в области кибербезопасности и противодействия спаму для удовлетворения потребностей развивающихся стран, в тесном сотрудничестве с соответствующими партнерами;

2 оказывать необходимую финансовую и административную поддержку для этих проектов в пределах имеющихся ресурсов и изыскивать дополнительные ресурсы (в денежной и натуральной форме) для осуществления этих проектов в рамках соглашений о партнерстве;

3 обеспечивать координацию этих проектов в контексте общей деятельности МСЭ в роли ведущей/содействующей организации по Направлению деятельности С5 ВВУИО;

4 координировать эти проекты с деятельностью и программами исследовательских комиссий МСЭ-D по этой теме;

5 продолжать сотрудничать с соответствующими организациями с целью обмена передовым опытом и распространения информации, например путем проведения совместных семинаров-практикумов и курсов профессиональной подготовки;

6 ежегодно представлять Совету отчет об этой деятельности и, в надлежащих случаях, вносить предложения.

Обзор деятельности МСЭ-D по реализации Направления деятельности С.5 ВВУИО –Укрепление доверия и безопасности при использовании ИКТ

1 Введение

ИКТ обладают потенциалом для поставки основных услуг в области электронного здравоохранения, электронного обучения, электронной коммерции и электронного правительства населению развивающихся стран, где многие граждане все еще не имеют доступа к физическим инфраструктурам таким, как больницы, школы или услуги государственного управления.

Электронное взаимодействие докторов с пациентами, доступ к услугам государственного управления через интернет, использование интернета для продажи товаров и услуг удаленным клиентам – все это возможно сегодня благодаря достижениям в области информационных технологий и электросвязи. Способность приложений ИКТ заполнять некоторые пробелы в доступе к основным услугам и оказывать помощь развивающимся странам так, чтобы они могли стать полноправными участниками информационного общества, может реализоваться.

Преимущества информационного общества для правительств, предприятий и граждан могут полностью реализоваться, только если решаются проблемы безопасности и надежности, и реализуются решения, касающиеся киберпреступности, имеющего юридическую силу законодательства, кражи идентификационных данных, тайны личных данных и защиты важных информационных систем. Большая зависимость от ИКТ как средство для стимулирования социального и экономического развития, а также скорость, с которой можно получать доступ к важным информационным системам и данным, манипулировать ими и уничтожать, поставили кибербезопасность на первое место как одну из важнейших проблем, с которыми сталкивается развивающееся информационное общество и экономика, основанная на знаниях.

2 Деятельность и инициативы

В качестве части мандата, принятого членами МСЭ на Полномочной конференции и Всемирных конференциях и Ассамблеях, МСЭ, выступая в качестве ведущей/содействующей организации Направления действия С.5 ВВУИО, совместно со своими партнерами, предпринимает множество действий, направленных на укрепление доверия и безопасности при использовании ИКТ.

В данном отчете кратко определяются некоторые действия, которые были реализованы, а также запланированные действия. Действия разделяются на пять основных областей деятельности (**Защита приложений ИКТ, Законодательство, Политика, стратегия и создание потенциала, Повышение осведомленности и сотрудничество среди членов**). В отчете также даются некоторые ссылки на другие источники информации о деятельности, важной для достижения целей Направления действия С.5 ВВУИО и приглашает все заинтересованные стороны объединить усилия по укреплению доверия и безопасности в ИКТ.

2.1 Защита Приложений ИКТ – реализация Проекта

Проблемы безопасности являются препятствием для использования ИКТ для определенных важных для выполнения основной миссии связи услуг таких, как электронное правительство, электронная коммерция, электронные платежи и электронное здравоохранение, где важно защитить чувствительные данные, обеспечить целостность данных и транзакций и установить подлинность сторон. Решая эти проблемы безопасности и надежности и реализуя практические решения, приходит понимание настоящего потенциала МСЭ по представлению доступных услуг с добавленной стоимостью.

Практические решения для увеличения потенциала ИКТ по предоставлению широкого круга важных услуг, построенных на технологиях безопасности и надежности, позволили странам сделать шаг от простых систем распространения информации к проведению важных транзакций и предоставлению населению широкого круга услуг.

Благодаря МСЭ несколько развивающихся стран впервые стали активно участвовать в развертывании и использовании решений, основанных на технологиях безопасности и надежности, таким образом, расширяя преимущества ИКТ в таких областях, как правительство и услуги здравоохранения.

Проекты, использующие продвинутые технологии безопасности и надежности, основанные на инфраструктуре открытых ключей (PKI), включая биометрическую аутентификацию, смарт карты, цифровые сертификаты X.509 МСЭ и технологии цифровой подписи, реализовывались и реализуются в **Барбадосе, Бутане, Болгарии, Буркина-Фасо, Камбодже, Камеруне, Кот-д'Ивуаре, Грузии, Ямайке, Парагвае, Перу, Сенегале, Турции, Замбии** и других странах, запланированных на 2007 год.

2.1.1 Грузия

Данный проект МСЭ решает поставленные задачи путем предоставления экономичных решений для безопасной передачи, доступа и обработки цифровых правительственных документов, таким образом, увеличивая эффективность и прозрачность правительственных услуг. Высшим должностным лицам Министерства транспорта и связи Грузии были предоставлены решения для расширения автоматизации документооборота и деловых операций, что позволило чиновникам ставить цифровую подпись и распространять официальные документы, таким образом, заменив медленные и достаточно дорогие бумажные методы. Авторизованный доступ к важным документам стал возможным при помощи решений безопасности и надежности для установления подлинности авторизованного персонала в Министерстве.

2.1.2 Парагвай

Данный проект обеспечил операторов и поставщиков услуг платформой для реализации безопасного и надежного механизма на основе интернета для обмена важной информацией (такой, как декларация о доходах) с национальным регулирующим ведомством (CONATEL) в электронном формате. В данном проекте защищенные и высоконадежные решения ИКТ используются для упрощения процесса выдачи лицензий операторам телефонов – автоматов, кроме того, увеличивается эффективность деловых процессов данного регулирующего ведомства.

2.1.3 Барбадос и Ямайка

Этим странам оказывалась помощь в создании национальной структуры политики использования цифровой сертификации и деятельности органов сертификации. Помощь МСЭ также включала в себя определение технологических спецификаций и стратегическое руководство для реализации национальной платформы на Барбадосе и Ямайке по выдаче и управлению цифровыми сертификатами, предоставлению надежных услуг аутентификации и обеспечению безопасности и надежности для транзакций электронного правительства и электронного бизнеса. После принятия Парламентом Ямайки Акта об электронных транзакциях в конце 2006 года, эксперты оказывали этой стране помощь для гарантирования соответствия платформы управления идентификационной информацией и смежными стратегиями законодательству. Планируется, что эта инфраструктура открытых ключей, финансируемая совместно МСЭ и правительством Ямайки, начнет свою работу в 2007 году.

2.1.4 Камерун

Данный проект МСЭ обеспечивает защищенную передачу важных правительственных документов через интернет и предоставляет правительственные услуги на интернет-основе гражданам в городах и отдаленных районах, где физической административной инфраструктуры не существует. Основанные на электронной подписи и технологиях шифрования, такие решения, как строгая аутентификация, конфиденциальность данных и неотказуемость, дают возможность бороться с некоторыми угрозами кибербезопасности, включая кражу идентификационной информации.

2.1.5 Болгария

Помощь МСЭ в реализации платформы кибербезопасности делает возможной защищенную связь между Министерством транспорта и связи, Министерством финансов, Советом министров и Комиссией по регулированию связи (CRC) при помощи использования PKI и приложений, поддерживающих PKI. Помощь МСЭ делает возможной защищенное, эффективное и экономичное взаимодействие между высшими должностными лицами в правительстве, таким образом, дополняя живые встречи и увеличивая производительность. Все данные, которыми обмениваются чиновники-участники, защищаются, и под ними ставится цифровая подпись, используются конфиденциальность, неотказуемость, целостность данных, а также методы строгой аутентификации на основе сертификатов.

2.1.6 Турция

Одной из стратегических целей данного проекта является улучшение услуг здравоохранения в Турции путем развития защищенной среды информации о здоровье, позволяющей поставщикам услуг здравоохранения (первая помощь и вспомогательная медицинская помощь), специалистам в области здравоохранения и гражданам иметь легкий и безопасный доступ к информации, связанной со здоровьем, при помощи использования последних ИКТ.

Основными пунктами данного проекта является разработка систем информации о первой помощи, поддерживающих систему семейных врачей, реализация электронных записей о здоровье и разработка взаимодействующих систем между поставщиками услуг здравоохранения, включая центры оказания первой помощи, больницы и государственные/частные страховые компании.

2.1.7 Бутан

Для удовлетворения потребностей сельского населения в получении доступа к услугам, для получения которых потребовалось бы несколько дней пути в административную столицу, МСЭ реализовал для Бутана национальную платформу, основанную на Инфраструктуре открытых ключей, включая биометрическую аутентификацию, строгое шифрование и технологии целостности данных. Финансируемая МСЭ и Правительством Бутана, данная платформа кибербезопасности предоставляет услуги по управлению идентификационной информацией и подтверждению ее подлинности, аутентификации на основе сертификатов, цифровым подписям, конфиденциальности данных и услуг по целостности данных. Благодаря этой поддержке МСЭ, пользователи в удаленных районах Бутана смогут получить доступ к важным услугам, основанным на технологиях надежности и безопасности, что, таким образом, расширит возможности и преимущества ИКТ в поставке услуг сельскому и городскому населению.

2.1.8 Глобальный проект по кибербезопасности и борьбе со спамом

МСЭ организовала первую встречу Государств-Членов, и Членов Секторов для обсуждения способов усиления сотрудничества по вопросам кибербезопасности, включая борьбу со спамом. Данное событие было предназначено для достижения следующих трех основных целей:

a) Выработать общую точку зрения и, по возможности, прийти к соглашению в области кибербезопасности и спама там, где необходимо, чтобы для усиления сотрудничества между Государствами-Членами существовал какой-либо механизм взаимоотношений.
b) Определить возможные механизмы и, помимо всего прочего, меморандум о понимании среди заинтересованных Государств-Членов для усиления сотрудничества по вопросам кибербезопасности, включая спам.
c) На основе вклада Государств-Членов сделать предложения в форме отчета, который необходимо представить на рассмотрение на Полномочной конференции 2006 года.

В результате встречи Государства-Члены определили основные насущные проблемы (см. список, ниже) для глобального сотрудничества в области кибербезопасности и борьбы со спамом.

a) Формирование общего представления о проблеме.
b) Разработка и введение в действие соответствующего сильного национального законодательства.
c) Создание человеческого и организационного потенциала.
d) Правоприменительная деятельность (в сфере создания потенциала).
e) Разработка национальной политики и стратегии в области кибербезопасности.
f) Содействие обмену информацией между странами и соответствующими заинтересованными сторонами.
g) Назначение национальных координаторов.
h) Мониторинг и оценка хода выполнения существующих инициатив.
i) Реализация решений по реагированию на инциденты, наблюдение и предупреждение.
j) Оценка уязвимых мест и угроз в области кибербезопасности.
k) Внедрение эффективных инструментов и приложений для сети и кибербезопасности.
l) Партнерства.
m) Международное сотрудничество.

Собрание пришло к консенсусу в том, что МСЭ-D должен играть ключевую роль в объединении существующих инициатив и обеспечивать базу, объединяющую данные инициативы в целях удовлетворения потребностей развивающихся стран.

Отчет об этой встрече был представлен на Полномочной конференции МСЭ в Анталии в 2006 году, где он был еще раз одобрен в качестве ключевой деятельности МСЭ по реализации механизмов сотрудничества в области кибербезопасности и борьбы со спамом. Данный проект, который будет реализовываться в рамках Всемирного проекта под названием "Проект по укреплению сотрудничества по вопросам кибербезопасности и борьбы со спамом", продлится 4 года начиная с 2007 года и станет частью Оперативного плана Сектора развития электросвязи на 2007 год.

Информация по проекту:

- Проект под названием "Проект по расширению сотрудничества в области кибербезопасности и борьбы со спамом" будет длиться 4 года начиная с 2007 года и являться частью оперативного плана БРЭ на 2007 год.
- На сессиях Совета МСЭ будут предоставляться ежегодные отчеты о ходе деятельности по его выполнению.
- При выполнении проекта следует учитывать решения ВКРЭ-06, касающиеся мандата Сектора развития в области кибербезопасности и борьбы со спамом.
- Проект должен быть в первую очередь направлен на оказание содействия развивающимся странам в вышеуказанных областях путем налаживания жизненно важного сотрудничества в области кибербезопасности и борьбы со спамом.
- В отношении соответствующего законодательства следует должным образом учитывать работу в данной области Совета Европы по оказанию содействия странам в разработке национального законодательства, соответствующего положениям Конвенции о борьбе с киберпреступностью.
- Осуществление деятельности в рамках данного проекта должно основываться на поступивших от стран просьбах, особое внимание уделяя развивающимся странам.
- После разработки проект должен быть представлен потенциальным финансирующим объединениям, включая Государства-Члены, частный сектор и международные организации, такие как Всемирный банк и Европейская комиссия.

2.2 Законодательство

Помощь развивающимся странам в разработке типового законодательства и законов по борьбе со спамом

Участники Всемирного симпозиума МСЭ для регулирующих органов попросили МСЭ оказать им помощь в разработке законодательства по борьбе со спамом. В Главе 7 публикации МСЭ *Тенденции в реформировании электросвязи*, *2006 год*, описывается и анализируется содержание типового законодательства по борьбе со спамом, включая положения об использовании обеспеченных правовой санкцией кодексов поведения для поставщиков интернет-услуг. Такие кодексы поведения запретили бы клиентам поставщиков интернет-услуг использовать их в качестве источника спама и смежных нарушений таких, как получение доступа обманным путем и мошенничество, а также запретили бы поставщикам интернет-услуг заключать равноправные соглашения с другими поставщиками интернет-услуг, не поддерживающих аналогичные кодексы поведения. С Главой 7 ***Тенденций в реформировании электросвязи***, ***2006 год***, *Противостоять международной волне спама*, можно ознакомиться в интернете по адресу:
www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf

2.3 Политика, стратегия и создание потенциала

2.3.1 Практикумы и семинары

МСЭ организовал национальные и региональные практикумы и семинары, рассматривающие политику и технологические стратегии для кибербезопасности в нескольких странах таких, как Азербайджан, Барбадос, Камерун, Чили (для государств Mercusor – Бразилия, Парагвай, Аргентина, Уругвай), Латвия (для стран Центральной и Восточной Европы, СНГ и стран Балтии), Монгола, Пакистан, Парагвай, Перу (Андский регион Латинской Америки), Румыния, Сейшельские Острова, Сирийская арабская республика и Узбекистан.

В Камеруне, Замбии, Барбадосе, Ямайке, Болгарии, Бутане и Сирии была организованная деятельность по созданию человеческого и организационного потенциала в области технологий, политики и стратегий кибербезопасности.

2.3.2 Всемирная встреча

В Женеве была организована Всемирная встреча, которую посетили около 50 экспертов по безопасности и более 500 делегатов из 120 стран. На встрече обсуждались технологические, стратегические, тактические и юридические вопросы, относящиеся к решениям в области электронных подписей, цифровых сертификатов и шифрования для развивающихся стран.

2.3.3 Региональный симпозиум МСЭ по вопросам электронного правительства и IP для Арабского региона

Безопасность и надежность были основными темами, обсуждавшимися на этом Симпозиуме, результатом которого стала Дубайская декларация, в которой подчеркивалась необходимость непрерывной деятельности МСЭ в области кибербезопасности электронных приложений и услуг. На этой встрече собрались стратеги из Арабского региона, чтобы обсудить общие вопросы и общую структуру решения основных проблем в области кибербезопасности. На 2007 год запланирована последующая деятельность в определенных областях, представляющих интерес для данного региона (таких, как управление идентификационной информацией и электронная подпись).

2.3.4 Симпозиум ООН во время Конференции "Мир здоровья IT"

Во время Конференции "Мир здоровья IT" МСЭ, ВОЗ, ЮНЕСКО, ЮНИТАР и промышленные партнеры организовали симпозиум ООН, где кибербезопасность в области здравоохранения стала одной из самых обсуждаемых тем. На симпозиуме ООН, который прошел 10 октября 2006 года в женевском Палэкспо, собрались члены четырех агентств ООН для обсуждения, помимо других вопросов, важнейшей роли кибербезопасности для медицинских транзакций и приложений, а также транзакций и приложений здравоохранения. Более подробную информацию см. на веб-сайте: www.worldofhealthit.org/about/about_partners.asp

2.4 Повышение осведомленности

2.4.1 Публикации и статьи

***Руководство по кибербезопасности для развивающихся стран* ©ITU 2006**

Справочное руководство по кибербезопасности было разработано для помощи развивающимся и наименее развитым странам в создании местного потенциала и повышения осведомленности в некоторых ключевых моментах безопасности для информационного общества. В данном справочном руководстве объясняются некоторые из основных проблем, спам, злонамеренное программное обеспечение (вирусы, черви, трояны), неприкосновенность важной инфраструктуры, недостаток аутентификации, необходимость конфиденциальности и целостности данных. Также рассматриваются учебные примеры в области законодательства по кибербезопасности, а также примеры методов, применяемых для защиты важных инфраструктур. Копию данного руководства можно бесплатно скачать с сайта МСЭ- D:

www.itu.int/ITU-D/e-strategy/publications-articles/

***Исследования в области законодательства по неприкосновенности личных данных, безопасности и предотвращению киберпреступности* ©ITU 2006**

Существуют определенные аспекты ИКТ, которые нуждаются в защите с юридической точки зрения, особенно это касается существующего законодательства по безопасности данных и правам интеллектуальной собственности, а также традиционных форм преступлений, совершенных с

использованием новой информационной супермагистрали таких, как кража идентификационной информации, мошенничество и вымогательство. Очевидно, что юридические потребности нужно пересматривать и адаптировать к ИКТ, также нужно признать, что существуют новые типы преступлений с использованием компьютера, и для аутентификации информационных потоков требуются новые устройства безопасности.

В данной исследовательской работе уделяется внимание юридическим мерам, необходимым для защиты национальных интересов развивающихся стран и обеспечения развития ИКТ и электронной коммерции, а также обеспечение защиты инфраструктуры при помощи соответствующих мер защиты. В качестве важных компонентов кибербезопасности нужно рассматривать три всеобъемлющих принципа. Это конфиденциальность, целостность и доступность. Три данные вопроса частично перекрываются. Иногда трудно провести четкую границу между различными категориями и определить, какой тип законодательства будет адекватно охватывать определенную область. Электронную версию данной публикации можно скачать с сайта МСЭ об электронных стратегиях на: www.itu.int/ITU-D/e-strategy/publications-articles/

***Новое руководство для развивающихся стран по кибербезопасности* ©ITU 2007.**

К концу 2006 года МСЭ завершил разработку нового справочного материала, направленного на повышение осведомленности в вопросах кибербезопасности и облегчение деятельности по созданию человеческих и организационных возможностей. Также отмечается потребность в разработке общей точки зрения по вопросам киберугроз и мер противодействия. Эта публикация объемом 160 страниц в основном направлена на предоставление справочного материала и рекомендаций развивающимся странам. Она представляет собой обзор различных форм киберпреступлений, включая краткий очерк о киберпреступниках. В ней объясняются текущие уязвимые места интернета и кибератаки, цифровые улики и основные принципы судебных и компьютерных расследований, также дается глоссарий терминов, связанных с киберпреступностью и ссылки. Данное новое руководство вместе с предыдущим (по кибербезопасности) будет одним из основных материалов для плановых действий, направленных на создание человеческого и организационного потенциала в области кибербезопасности и борьбы с киберпреступностью. Первоначально изданное на английском языке, это руководство будет переведено на все шесть языков МСЭ и станет доступно заинтересованным странам во втором квартале 2007 года в бумажном виде, а также в электронном виде на сайте МСЭ.

2.5 Сотрудничество между членами

Для облегчения обмена опытом и наилучшими практиками среди членов Сектор развития электросвязи МСЭ (МСЭ-D) предоставляет платформу в виде исследовательской комиссии, где Государства-Члены могут достичь соглашения о едином подходе к проблемам кибербезопасности и борьбы со спамом. В сентябре 2006 года прошла первая встреча группы по Вопросу исследовательской комиссии МСЭ-D, касающемуся кибербезопасности, на которой была одобрена программа работы на новый период. На период 2006–2009 гг. работа Программы и ожидаемые результаты для группы по этому Вопросу Исследовательской комиссии МСЭ-D включают следующее:

а) провести обзор, составить каталог, дать описание и повысить уровень осведомленности по:

- основным проблемам, с которыми сталкиваются национальные органы, отвечающие за выработку политики, и все заинтересованные стороны при формировании культуры кибербезопасности,
- основным источникам информации и помощи в области формирования культуры кибербезопасности,

- успешным примерам передового опыта, накопленного национальными органами, отвечающими за выработку политики, работе со всеми заинтересованными сторонами в области обеспечения кибербезопасности и формировании культуры кибербезопасности,
- специфическим проблемам, с которыми сталкиваются развивающиеся страны при решении вопроса защиты сетей, а также примерам передового опыта в этой области;

b) Проанализировать примеры передового опыта по созданию и эксплуатации средств слежения, оповещения, реагирования на случаи нарушения безопасности, а также восстановления безопасности, которые могут использовать Государства – Члены Союза при создании своих национальных возможностей.

Предоставлять отчет или отчеты для членов по вопросам, указанным в разделе 2, выше. Такой(ие) отчет(ы) будет(ут) отражать информацию о том, что защищенные информационно-коммуникационные сети неразрывно связаны с построением информационного общества и с социально-экономическим развитием всех стран.

3 Резюме

Кибербезопасность касается всех стран и ее следует принимать всерьез. Для развивающихся стран Приложения ИКТ, основанные на защищенных и высоконадежных платформах, могут предоставлять важнейшие услуги населению в таких областях, как здравоохранение, финансы, государственное управление и коммерция.

Развитые страны могут также получить эти преимущества в добавление к необходимости защищать свои важные инфраструктуры и охранять важные данные и транзакции.

Проблемы, имеющиеся в данной области, можно эффективно решать при помощи сотрудничества и совместной работы правительств, деловых кругов, международных организаций, гражданского общества и других заинтересованных сторон. Повышение основной осведомленности о проблемах и возможностях, создание потенциала на местах, реализация законодательства, реализация проектов, предоставляющих защищенные и высоконадежные решения, и разработка соответствующих стратегий – вот лишь некоторые из основных областей, в которых партнеры могут совместно работать для достижения общей цели, которой является безопасное и глобальное информационное общество для всех.

МСЭ, в рамках своего мандата, выступает с инициативами путем реализации проектов, облегчающих обмен информацией, создание потенциала, повышение осведомленности и реализацию платформы для партнерства и сотрудничества, решая проблемы кибербезопасности на глобальном уровне. Для достижения целей, определенных ВВУИО, МСЭ приглашает всех заинтересованных сторон объединить усилия для укрепления безопасности и доверия при использовании ИКТ.

Приложение D – Основные вопросы МСЭ-Т, относящиеся к безопасности, предназначенные для изучения в исследовательский период с 2005 по 2008 год

Выдержки из
www.itu.int/ITU-T/studygroups/com17/questions.html

Вопросы, порученные 17-й Исследовательской комиссии МСЭ-Т (исследовательский период 2005–2008 гг.)

17-я исследовательская комиссия: Безопасность, языки и программное обеспечение электросвязи

Вопрос 2/17 – Справочные услуги, справочные системы, сертификаты открытого ключа/ атрибутов

2.1 Справочные услуги

a) Какие требуются новые определения и профили услуг, которые могут воспользоваться широко поддерживаемыми технологиями справочного обслуживания, например, X.500 и LDAP?

b) Какие изменения следует внести в Рекомендации серий E и F и/или какие новые Рекомендации требуются для определения расширений, корректировки ошибок в существующих определениях и профилях справочного обслуживания?

2.2 Справочные системы

a) Какие дополнения требуется внести в Справочник для обеспечения лучшей поддержки существующих и потенциальных пользователей Справочника, например, более строгую последовательность информации Справочника на дублирующих сайтах, поддержку работы на указанных пользователем связанных агрегатах атрибутов справочника, улучшение показателей работы при поиске большого числа возвращаемых результатов или разрешение недоразумений, вызываемых многочисленными поставщиками справочных услуг, имеющих разную информацию с идентичными именами?

b) Какие дополнения следует внести в Справочник для поддержки и взаимодействия с услугами, реализуемыми при помощи использования спецификации LDAP IETF, включая возможное использование XML для получения доступа к справочникам.

c) Какие другие дополнения требуется внести в Справочник, для того чтобы сделать возможным его использование в различных средах, например, в среде с ограниченными ресурсами такой, как беспроводные сети и мультимедийные сети?

d) Какие еще дополнения требуется внести в Справочник для улучшения поддержки таких областей, как интеллектуальная сеть, сети связи и справочное обслуживание общего пользования?

e) Какие требуются изменения в Рекомендациях серии X.500 и/или какие новые Рекомендации требуются для описания дополнений, корректировки ошибок в Справочнике?

Работа справочных систем будет выполняться в сотрудничестве с JTC 1 ISO/IEC в рамках их работы по расширению ISO/IEC 9594, который содержит общий текст с Рекомендациями X.500–X.530. Также будет поддерживаться взаимосвязь и тесное сотрудничество с IETF особенно в области LDAP.

2.3 Сертификаты открытого ключа/ атрибутов

a) Какие дальнейшие дополнения следует внести в сертификаты открытого ключа, атрибутов, чтобы их можно было использовать в различных средах таких, как беспроводные сети и мультимедийные сети?

b) Какие дальнейшие дополнения требуются для сертификатов открытого ключа и сертификатов атрибутов для повышения их полезности в таких областях, как биометрия, аутентификация, управление доступом и электронная коммерция?

c) Какие изменения требуется произвести в Рекомендации X.509 для определения дополнений и корректировки ошибок в X.509?

Работа сертификатов открытого ключа/атрибутов будет выполняться в сотрудничестве с JTC 1 ИСО/МЭК в рамках их работы по расширению ИСО/МЭК 9594-8, который содержит общий текст с Рекомендациями X.509. Также будет поддерживаться взаимосвязь и тесное сотрудничество с IETF особенно в области PKI.

Вопрос 4/17 – Проект безопасности систем связи

Предмет безопасности имеет множество областей и аспектов применения. Безопасность может применяться почти ко всем аспектам телекоммуникационной и информационной технологии. Подходы, определяющие требования безопасности, могут называться "снизу–вверх" или "сверху–вниз".

– Подход "снизу–вверх" – это такой подход, когда эксперты этой области продумывают меры безопасности, чтобы укрепить и защитить свою определенную часть сети, т. е. биометрику, криптографию и т. д. Это наиболее часто применяющийся способ, однако он дает только фрагментарную информацию о том, как безопасность изучается в различных организациях.

– Подход "сверху–вниз" является стратегическим высокоуровневым способом рассмотрения безопасности. Он требует знания всей картины. Это также и более сложный подход, потому что найти экспертов, обладающих глубокими знаниями всех частей сети и, следовательно, требований их безопасности, сложнее, чем узких специалистов со знанием определенной области или нескольких областей.

– Альтернативой является комбинация подходов "снизу–вверх" и "сверху–вниз" с попыткой координации и совмещения различных участков. Применение данного подхода достаточно сложно, принимая во внимание меняющиеся интересы и программы.

Данный Вопрос посвящен определению точки зрения, координации и организации полного спектра деятельности по безопасности связи в рамках МСЭ-Т. К вопросу безопасности будет применен подход "сверху–вниз" в сотрудничестве с другими исследовательскими комиссиями и SDO. Данный проект направлен на получение более сфокусированных усилий на уровне проекта и стратегии.

Вопросы

a) Что может быть сделано для проекта безопасности систем связи?

b) Каковы процессы, рабочие вопросы, методы работы и временная шкала для данного проекта для достижения необходимых результатов?

c) Какие справочники по безопасности и руководства должен представить и поддерживать МСЭ?

d) Какие необходимы практикумы по безопасности?

e) Что нужно, чтобы создать эффективные взаимоотношения с другими организациями по разработке стандартов, для того чтобы способствовать работе в области безопасности?

f) Каковы этапы и критерии успеха?

g) Как можно стимулировать интерес членов сектора и администраций и поддерживать динамику работы в области безопасности?

h) Как можно сделать функции безопасности более привлекательными на рынке?

i) Как ясно выразить ключевые преимущества для правительств и необходимость защиты глобальных экономических интересов, которые зависят от надежной и защищенной инфраструктуры электросвязи?

Вопрос 5/17 – Архитектура и структура безопасности

Принимая во внимание угрозы безопасности среде связи и современные достижения в области контрмер против угроз безопасности, следует изучить новые требования и решения безопасности

Следует изучать безопасность новых типов сетей, а также безопасность новых типов услуг.

Вопросы

a) Как можно определить полное, согласованное решение безопасности связи?

b) Какова архитектура полного, согласованного решения безопасности связи?

c) Какова структура применения архитектуры безопасности для создания нового решения безопасности?

d) Какова структура применения архитектуры безопасности для оценки (и, соответственно, улучшения) существующего решения безопасности?

e) Какова архитектурная основа безопасности?

   i) Что такое архитектура безопасности для возникающих технологий?

   ii) Какова архитектура сквозной безопасности?

   iii) Какова архитектура безопасности для мобильной среды?

   iv) Какие требуются технические архитектуры безопасности? Например:

      a) Что такое архитектура безопасности открытых систем?

      b) Что такое архитектура безопасности сетей на основе IP?

      c) Что такое архитектура безопасности СПП?

f) Как следует обновить типовые Рекомендации моделей верхнего и нижнего уровня безопасности для адаптации их к меняющейся среде, какие новые Рекомендации могут потребоваться?

g) Как следует структурировать стандарты архитектуры в соответствии с существующими Рекомендациями по безопасности?

h) Как следует обновить Рекомендации по структуре безопасности для адаптации их к появляющимся технологиям, какие новые Рекомендации по структуре могут потребоваться?

i) Как применяются услуги безопасности для обеспечения решений безопасности?

Вопрос 6/17 – Кибербезопасность

Были введены многочисленные механизмы защиты и обнаружения такие, как защитные системы и системы обнаружения вторжения (IDS), однако большая часть из них концентрируется только на технических аспектах. Поскольку эти технические решения являются важными, требуются дополнительные рассмотрения и обсуждения по кибербезопасности с точки зрения международной стандартизации.

Вопросы

Следует изучить следующие области кибербезопасности:

- процессы распределения, обмена и разглашения информации об уязвимости;
- стандартная процедура для операций по управлению инцидентами в киберпространстве;
- стратегия защиты ключевой инфраструктуры сети.

Вопрос 7/17 – Управление безопасностью

Вопросы

a) Как следует определять и управлять рисками безопасности в системах электросвязи?

b) Как следует определять и управлять информационным имуществом для систем электросвязи?

c) Как следует определять конкретные вопросы управления для компаний, предоставляющих услуги электросвязи?

d) Как следует правильно конструировать системы управления безопасностью информации (ISMS) для компаний, предоставляющих услуги электросвязи, в соответствии с уже существующими стандартами ISMS?

e) Как следует управлять случаями нарушений безопасности электросвязи?

Вопрос 8/17 – Телебиометрика

Вопросы

a) Как можно улучшить идентификацию и аутентификацию пользователей при помощи безопасных и защищенных методов телебиометрии?

b) Как новая часть IEC 60027 "Физиологическое подмножество", используемая в МСЭ-Т, предоставляет элементы для подходящей модели классификации безопасных и защищенных телебиометрических устройств?

c) Какую систему отсчета уровней безопасности следует использовать для претворения в жизнь безопасных и защищенных телебиометрических решений в иерархической структуре?

d) Как следует определять вопросы технологий биометрической аутентификации для электросвязи?

e) Как следует определять требования технологий биометрической аутентификации для электросвязи на основе технологии шифрования такой, как PKI?

f) Как следует определять модель и процедуру технологий биометрической аутентификации для электросвязи на основе технологии шифрования такой, как PKI?

Вопрос 9/17 – Защищенные услуги связи

Вопросы

a) Как следует идентифицировать и определять защищенные услуги связи в мобильной связи или интернет-услугах?

b) Как следует определять и обращаться с угрозами услугам связи?

c) Каковы технологии безопасности для поддержки защищенных услуг связи?

d) Как следует осуществлять и поддерживать защищенную связь между услугами связи?

e) Какие методы безопасности требуются для защищенных услуг связи?

f) Какие методы безопасности или протоколы безопасности требуются для появляющихся защищенных интернет-услуг?

g) Какие протоколы защищенных соединений следует применять для защищенных услуг связи?

h) Каковы глобальные решения безопасности для защищенных услуг связи и их приложений?

Приложение E – Литература

Справочник, описывающий стандарты безопасности МСЭ-Т, применяемые в мире электросвязи:

> *Security in telecommunications and information technology: an overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunication. ITU-T, October 2004:* www.itu.int/itudoc/itu-t/86435.html

Некоторые справочные работы

Ross Anderson: Security Engineering, A Guide To Building Dependable Distributed Systems, Wiley, 2001, ISBN 0-471-38922-6

Matt Bishop: Computer security: art and science, Addisson-Wesley, 2002, ISBN 0-201-44099-7

Ulyses Black: Internet Security Protocols, Protecting IP Traffic, Prentice Hall, ISBN 0-13-014249-2

Dorothy E. Denning: Information Warfare and Security, Addison-Wesley, 1999, ISBN 0-201-43303-6

Arnaud Dufour, Solange Ghernaouti-Hélie: *Internet – PUF, Que sais-je?* N° 3073 – ISBN 2-13-053190-3

Niels Ferguson, Bruce Schneier: Practical Cryptography, Wiley, 2003, ISBN 0-471-22357-3

Solange Ghernaouti-Hélie: *Internet & Sécurité – PUF Que sais-je?* N° 3609 – ISBN 2-13-051010-8

Solange Ghernaouti-Hélie: *Sécurité informatique et réseaux, cours et exercices corrigés* – Dunod 2006.

Raymond Panko: Corporate Computer and Network Security, Prentice Hall, 2004, ISBN 0-13-038471-2

Guillaume Poulin, Julien Soyer, Marc-Éric Trioullier: *Sécurité des architectures Web, "ne pas prévoir c'est déjà gémir"*, Dunod, 2004.

Bruce Schneier: Beyond Fear, Thinking Sensibly About Security In An Uncertain World, Copernicus Books, 2003, ISBN 0-387-02620-7

Bruce Schneier: Secrets and Lies: Digital Security in a Networked World, Wiley, 2000, ISBN 0-471-25311-1

Bruce Schneier: Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition, Wiley, 1996, ISBN 0-471-11709-9

Simon Singh: Histoire des codes secrets, JC Lattès, 1999, ISBN 2-7096-2048-0

William Stallings: Cryptography And Network Security, Principles and Practice, Prentice Hall, 1999, ISBN 0-13-869017-0

William Stallings: Network And Internetwork Security, Principles and Practice, Prentice Hall, 1995, ISBN 0-13-180050-7

William Stallings: Network Security Essentials, Applications and Standards, Prentice Hall, 2000, ISBN 0-13-016093-8

Сайты для справки

Сайты на французском языке:

Сайт французского премьер-министра: www.premier-ministre.gouv.fr

(См. в частности раздел: *Technologie de l'information dans la thématique: communication*)

www.internet.gouv.fr: сайт, связанный с развитием информационного общества

Портал французской государственной службы: www.service-public.gouv.fr. Охватывает все интернет-услуги, см. раздел "*se documenter*"

Сайт французской государственной службы в области права: www.legifrance.gouv.fr

Сайт французской службы документации: www.ladocfrancaise.gouv.fr

www.foruminternet.org/: информационный и дискуссионный форум в области права, интернета и сетей

Французская национальная комиссия по гражданским свободам: www.cnil.fr

Главное управление Франции по борьбе с преступлениями, связанными с ИКТ: www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic

Станция наблюдения за безопасностью информационных систем и сетей: www.ossir.org

Clusif: www.clusif.asso.fr

Обзор киберпреступности: www.clusif.asso.fr/fr/production/ouvrages/

Другие сайты

CERT: www.cert.org (Команда компьютерной "скорой помощи")

NIST: www.nist.gov (Национальный институт стандартов и технологий США)

NSA: www.nsa.gov Национальное Агентство безопасности США)

CSE: www.cse.dnd.ca (канадский Центр безопасности электросвязи)

CESG: www.cesg.gov.uk (Британское национальное техническое управление страхованием информации)

BSI: www.bsi.bund.de (Федеральное агентство информационной безопасности Германии) – сайт на немецком и английском языках

DSD: www.dsd.gov.au (Дирекция защиты сигналов, работающая в Австралии и Новой Зеландии). Сайт, посвященный цифровому наблюдению и информационной безопасности.

Национальный центр преступлений "белых воротничков": IFCC – интернет – центр жалоб на мошенничество:
www1.ifccfbi.gov/index.asp; Internet Fraud – Crime Report – 2004:
www1.ifccfbi.gov/strategy/2004_IC3Report.pdf

Бюллетени

Криптограмма – Брюс Шнайер: [schneier@counterpane.com]
crypto-gram-list@listserv.modwest.com

Бюллетень интернет-форума по правам: infolettre@listes.foruminternet.org

Бюллетени о безопасности US-CERT: security-bulletins@us-cert.gov

Бюллетень информации о киберполиции: cyberpolice.over-blog.com/
cyberpolice.over-blog.com [newsletter@over-blog.com]

Приложение F – Директивы ОЭСР для безопасности информационных систем и сетей: К культуре безопасности

Предисловие

Использование информационных систем и сетей, а также вся среда информационной технологии сильно изменилась с 1992 года, когда ОЭСР впервые выпустила *Рекомендации по безопасности информационных систем*. Эти непрерывные изменения дают значительные преимущества, но также требуют гораздо большего внимания к безопасности со стороны правительств, деловых кругов, других организаций и отдельных пользователей, которые разрабатывают, владеют, предоставляют, управляют услугами и используют информационные системы и сети ("участники").

Все более мощные персональные компьютеры, конвергенция технологий и широкое использование интернета вытеснили скромные, изолированные системы в преимущественно закрытых сетях. Сейчас участники становятся все более взаимосвязанными, часто связь осуществляется через границы государств. Кроме того, интернет поддерживает такие ключевые инфраструктуры, как энергетика, транспорт и финансы и играет важную роль в том, как компании ведут бизнес, как правительство предоставляет услуги гражданам и предприятиям и как отдельные граждане взаимодействуют между собой и обмениваются информацией. Характер и тип технологий, составляющих коммуникационно-информационную инфраструктуру, также значительно изменились. Число устройств доступа к инфраструктуре увеличилось и теперь включает в себя фиксированные, беспроводные и мобильные устройства, все больший процент доступа осуществляется при помощи соединений типа "всегда включено". Следовательно, характер, объем и чувствительность передаваемой информации изменились и значительно расширились.

Как результат увеличившихся взаимосвязей, информационные системы и сети теперь подвергаются все большему числу и разнообразных угроз и становятся уязвимыми. Это ставит перед безопасностью новые задачи. По этим причинам данное Руководство применяется ко всем участникам нового информационного общества и требует большей осведомленности и понимания проблем безопасности, а также разработки "культуры безопасности".

F.1 К культуре безопасности

Данное Руководство реагирует на постоянно меняющуюся среду безопасности, способствуя развитию культуры безопасности, то есть концентрируется на безопасности развития информационных систем и сетей и формировании нового образа мышления и поведения при использовании информационных систем и сетей и взаимодействия внутри них. Данное Руководство ознаменует полный разрыв с тем периодом времени, когда защита разработки и использования сетей и систем слишком часто была запоздалой. Участники становятся все более зависимыми от информационных систем, сетей и смежных служб, которые должны быть надежными и безопасными. Обеспечить эффективную безопасность может только подход, уделяющий должное внимание интересам всех участников и характеру систем, сетей и смежных служб.

Каждый участник играет важную роль в обеспечении безопасности. Участники, в соответствии с их ролью, должны быть осведомлены о существующих рисках безопасности и превентивных мерах, брать на себя ответственность и предпринимать действия по укреплению безопасности информационных систем и сетей.

Развитие культуры безопасности потребует как лидерских качеств, так и активного участия. Результатом этого развития должно стать повышение приоритета планирования и управления безопасностью, а также понимание потребностей всех участников в безопасности. Вопросы безопасности должны быть темой для размышления и ответственного отношения на всех уровнях государственной власти и предприятий среди всех участников. Данное Руководство составляет основу работы по созданию культуры безопасности в обществе. Оно позволит участникам учитывать безопасность при разработке и использовании всех информационных систем и сетей. Предлагается, чтобы все участники приняли и культуру безопасности и способствовали развитию ее как образа мышления, оценки и действий в соответствии с работой информационных систем и сетей.

F.2 Цели

Целями данного руководства являются:

- Содействие культуре безопасности среди всех участников в качестве средства защиты информационных систем и сетей.
- Повышение осведомленности о рисках, касающихся информационных систем и сетей; стратегии, практики, мер и процедур, доступных для реагирования на данные риски; а также необходимость их принятия и реализации.
- Укрепление доверия среди всех участников информационных систем и сетей и того, как они обеспечиваются и используются.
- Создание общей точки отсчета, которая поможет участникам понимать вопросы безопасности и уважать этические ценности при разработке и реализации согласованных стратегий, практик, мер и процедур для безопасности информационных систем и сетей.
- Содействие сотрудничеству и соответствующему обмену информацией между всеми участниками при разработке и реализации согласованных стратегий, практик, мер и процедур.
- Обеспечение понимания всеми участниками, задействованными в разработке или реализации стандартов безопасности как важной цели.

F.3 Принципы

Следующие девять принципов являются взаимодополняющими и должны рассматриваться как единое целое. Они касаются участников всех уровней, включая уровень стратегии и оперативный уровень. В рамках данного Руководства ответственность участников меняется в зависимости от их роли. Всем участникам поможет осведомленность, образование, обмен информацией и профессиональная подготовка, что будет способствовать лучшему пониманию безопасности и практик. Усилия по укреплению безопасности информационных систем и сетей должны соответствовать ценностям демократического общества, в особенности потребности в открытом и свободном потоке информации и основным проблемам неприкосновенности частной жизни[65].

[65] В дополнение к данному Руководству по безопасности ОЭСР разработала дополнительные рекомендации, касающиеся руководства в других вопросах, важных для мирового информационного общества. Они относятся к неприкосновенности частной жизни (ОЭСР *Руководство, управляющее защитой частной жизни и трансграничными потоками личных данных,* 1980 г.) криптографии (*ОЭСР Руководство по криптографической политике,* 1997 г.). Данное Руководство по безопасности следует читать вместе с этими Руководствами.

1) Осведомленность

Участникам следует знать о необходимости информационных систем и сетей в безопасности, а также о том, что они могут сделать для укрепления безопасности.

Осведомленность о рисках и доступных способах защиты – это первая ступень обеспечения безопасности информационных систем и сетей. Информационные системы и сети могут подвергаться как внутренним, так и внешним рискам. Участники должны понимать, что нарушения безопасности могут нанести значительный вред другим из-за взаимосвязи и взаимозависимости. Участники должны быть осведомлены о конфигурации и доступных обновлениях своей системы, ее месте в сетях, передовом опыте, которые они могут применять для укрепления безопасности, и о потребностях других участников.

2) Ответственность

Все участники несут ответственность за безопасность информационных систем и сетей.

Участники зависят от взаимосвязанных локальных и глобальных информационных систем и сетей, они должны осознавать свою ответственность за безопасность этих информационных систем и сетей. Они должны нести ответственность в соответствии со своими ролями. Участникам следует регулярно пересматривать свои собственные стратегии, меры и процедуры и убеждаться, что они соответствуют среде. Те, кто разрабатывает, создает и поставляет продукцию и услуги, должны рассматривать безопасность системы и сети и своевременно распространять соответствующую информацию, включая обновления так, чтобы пользователи смогли лучше понять функции безопасности продукции и услуг и их ответственность в отношении безопасности.

3) Реакция

Участникам следует действовать своевременно и сообща для предотвращения, обнаружения и реагирования на случаи нарушения безопасности.

Признавая взаимосвязь информационных систем и сетей, а также вероятность быстрого и широко распространенного ущерба, участникам следует действовать своевременно и сообща для реагирования на случаи нарушения безопасности. Им также следует обмениваться информацией об угрозах и уязвимых местах и реализовывать процедуры для быстрого и эффективного сотрудничества для предотвращения, обнаружения и реагирования на случаи нарушения безопасности. Там, где это возможно, данный процесс может включать в себя обмен информацией и сотрудничество между государствами.

4) Этика

Участникам следует уважать законные интересы других.

Принимая во внимание распространение информационных систем и сетей в нашем обществе, участникам нужно осознавать, что их действия или бездействие может навредить другим. Поэтому этичное поведение становится чрезвычайно важным, участникам следует стремиться к разработке и применению передового опыта, а также поощрять поведение, учитывающее потребности в безопасности и уважающее законные интересы других.

5) Демократия

Безопасность информационных систем и сетей должна быть совместима с важными ценностями демократического общества.

Безопасность следует реализовывать в соответствии с ценностями, признаваемыми демократическими обществами, включая свободу выражения мыслей и идей, свободу информации, конфиденциальность информации и связи, соответствующую защиту личной информации, открытость и прозрачность.

6) Оценка риска

Участникам следует проводить оценку риска

Оценка риска выделяет угрозы и уязвимые места. Она должна иметь достаточно широкую основу, чтобы охватить ключевые внутренние и внешние факторы, такие как технологический, физический и человеческий факторы, стратегии и услуги третьих сторон в отношении безопасности. Оценка риска позволит определить приемлемый уровень риска и поможет в выборе соответствующих средств управления риском причинения потенциального вреда информационным системам и сетям в свете характера и важности защищаемой информации. Из-за увеличивающихся взаимосвязей между информационными системами, оценка риска должна включать рассмотрение потенциального вреда, который может исходить от других или быть причинен другим.

7) Разработка и реализация безопасности

Участникам следует считать безопасность важным элементом информационных систем и сетей.

Для оптимизации безопасности, системы, сети и стратегии необходимо правильно разрабатывать, реализовывать и координировать. Основным, но не единственным аспектом, является разработка и применение соответствующих мер защиты и решений по ликвидации или ограничению потенциального вреда от определенных угроз и уязвимых мест. Требуются как технические, так и не технические средства защиты и решения, они должны быть пропорциональны ценности информации в системах и сетях организации. Безопасность должна быть основным элементом всей продукции, услуг, систем и сетей и составной частью модели и архитектуры системы. Для конечных пользователей модель и реализация системы состоит, по большей части, в выборе и конфигурировании продукции и услуг для своей системы.

8) Управление безопасностью

Участникам следует придерживаться всеобъемлющего подхода к управлению безопасностью.

Управление безопасностью должно основываться на оценке риска, и должны быть динамичным, охватывать все уровни деятельности участников и все аспекты их работы. Управление безопасностью должно также включать дальновидное реагирование на возникающие угрозы, предотвращение, обнаружение и реагирование на происшествия, восстановление системы, продолжительную поддержку, пересмотр и проверку. Политики, практики, меры и процедуры безопасности информационных систем и сетей должны координироваться и интегрироваться для создания гармоничной системы безопасности. Требования, предъявляемые к управлению безопасностью, зависят от уровня участия, роли данного участника, степени риска и системных требований.

9) Повторная оценка

Участникам следует пересматривать и повторно оценивать безопасность информационных систем и сетей и вносить соответствующие изменения в политику, практику, меры и процедуры безопасности.

Постоянно обнаруживаются все новые угрозы и уязвимые места, они постоянно меняются. Участникам следует постоянно пересматривать, заново оценивать и модифицировать все аспекты безопасности для сокращения возникающих рисков.

Рекомендация Совета, касающаяся руководства по безопасности систем и сетей: К культуре безопасности

СОВЕТ,

Учитывая Конвенцию об Организации экономического сотрудничества и развития от 15 декабря 1960 года, и, в частности, Статьи 1 b), 1 c), 3 a) и 5 b) этой конвенции;

Учитывая Рекомендацию Совета, касающуюся Руководства по защите неприкосновенности частной жизни и трансграничных потоков личных данных от 23 сентября 1980 года [C(80)58(Окончательный)];

Учитывая Декларацию о трансграничных потоках данных, принятую Правительствами Государств-членов ОЭСР 11 апреля 1985 года [Приложение к C(85)139];

Учитывая Рекомендацию Совета, касающуюся Руководства по криптографической политике от 27 марта 1997 года [C(97)62/Окончательный];

Учитывая Декларацию министерства о защите неприкосновенности частной жизни в глобальных сетях от 7–9 декабря 1998 года [Приложение к C(98)177/Окончательный];

Учитывая Декларацию министерства об аутентификации для электронной торговли от 7–9 декабря 1998 года [Приложение к C(98)177/Окончательный];

Признавая, что информационные системы и сети используются все больше и представляют все большую ценность для органов государственного управления, предприятий, других организаций и отдельных пользователей;

Признавая, что все более важная роль информационных систем и сетей, увеличивающаяся зависимость от них при обеспечении стабильности и эффективности национальных экономик и международной торговли, а также социальной, культурной и политической жизни, требуют специальных усилий по защите и укрепления доверия;

Признавая, что информационные системы и сети, а также их международное распространение, сопровождаются новыми увеличивающимися рисками;

Признавая, что данные и информация, хранящиеся и передаваемые по информационным системам и сетям подвержены угрозам различных способов нелегального доступа, использования, незаконного присвоения, изменения, передачи злонамеренного кода, отказа в обслуживании или уничтожения и потребует соответствующей защиты;

Признавая, что существует необходимость повышать осведомленность о рисках, угрожающих информационным системам и сетям, а также о стратегиях, практиках, мерах и процедурах, имеющихся в наличии для реагирования на эти риски; кроме того, существует необходимость поощрять соответствующее поведение, что является решающим шагом на пути развития культуры безопасности;

Признавая, что существует необходимость в пересмотре текущей политики, практик, мер и процедур для гарантии того, что они соответствуют развивающимся проблемам, угрожающим информационным системам и сетям;

Признавая, что существует общий интерес в укреплении безопасности информационных систем при помощи культуры безопасности, которая способствует международной координации и сотрудничеству для решения проблем, возникающих из-за потенциального вреда, который сбои безопасности могут нанести национальной экономике, международной торговле и участию в социальной, культурной и политической жизни;

И далее признавая, что *Руководство по безопасности информационных систем и сетей: К культуре безопасности*, приведенное в Приложении к данной Рекомендации, носит добровольный характер и не влияет на суверенные права государств;

И признавая, что данное Руководство не предполагает, что для безопасности существует только одно решение, и не рекомендует, какие стратегии, практики, меры и процедуры подходят в каждой конкретной ситуации, скорее оно предоставляет структуру принципов для достижения лучшего понимания того, как участники могут способствовать развитию культуры безопасности и извлекать из нее пользу;

РЕКОМЕНДУЕТ данное *Руководство по безопасности информационных систем и сетей: к культуре безопасности* органам государственного управления, предприятиям, другим организациям и отдельным пользователям, которые разрабатывают, владеют, предоставляют, управляют, обслуживают и используют информационные системы и сети;

РЕКОМЕНДУЕТ чтобы Государства-Члены:

Создавали новые, делали поправки к старым стратегиям, практикам, мерам и процедурам так, чтобы они отражали и учитывали *Руководство по безопасности информационных систем и сетей: к культуре безопасности* путем принятия культуры безопасности и содействия ей так, как изложено в Руководстве;

Консультировались, координировали работу и сотрудничали на национальном и международном уровнях для реализации данного Руководства;

Распространяли данное Руководство в государственном и частном секторе, в том числе органам государственного управления, предприятиям, другим организациям и отдельным пользователям с целью содействовать культуре безопасности и побудить все заинтересованные стороны нести ответственность и предпринимать необходимые меры по реализации данного Руководства в соответствии со своей ролью;

Своевременно сделали данное Руководство доступным для стран-нечленов;

Пересматривали данное Руководство каждые пять лет, для того чтобы поощрить международное сотрудничество по вопросам, касающимся безопасности информационных систем и сетей;

ПОРУЧАЕТ Комитету по информационной, компьютерной политике и политике связи ОЭСР содействовать реализации данного Руководства.

Данная рекомендация заменяет Рекомендацию Совета, касающуюся Руководства по безопасности информационных систем от 26 ноября 1992 года [C(92)188/Окончательный].

История процесса

Руководство по безопасности были впервые написаны в 1992 году, а позже пересмотрены в 1997 году. Настоящий пересмотр был предпринят в 2001 году рабочей группой по вопросам безопасности информации и неприкосновенности частной жизни (WPISP), в соответствии с мандатом от комитета по информационной, компьютерной политике и политике связи (ICCP), а его выпуск был ускорен вследствие трагедии 11 сентября.

Редактирование было выполнено Экспертной комиссией WPISP, встречи которой прошли в Вашингтоне, DC, 10–11 декабря 2001 года, Сиднее 12–13 февраля 2002 года и Париже 4 и 6 марта 2002 года. Встречи рабочей группы WPISP прошли в Париже 5–6 марта 2002 года, 22–23 апреля 2002 года и 25–26 июня 2002 года.

Настоящее *Руководство по безопасности информационных систем и сетей: к культуре безопасности* ОЭСР было принято в качестве Рекомендации Совета ОЭСР на 1037-й сессии этой организации 25 июля 2002 года.

Международный союз электросвязи
Бюро развития электросвязи (БРЭ)
Place des Nations
CH-1211 GENEVA 20
Switzerland

Для более подробной информации обращаться:
ИКТ и кибербезопасность
Эл. почта: cybmail@itu.int
Веб-сайт: www.itu.int/ITU-D/cyb

Отпечатано в Швейцарии
Женева, 2009 г.