ITU Публикации
Исследовательский период 2018–2021 годов

Международный союз электросвязи
Сектор развития

2-я Исследовательская комиссия Вопрос 3

Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности

Отчет о результатах работы по Вопросу 3/2 МСЭ-D

Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности

Исследовательский период 2018–2021 гг.

Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности – Отчет о результатах работы по Вопросу 3/2 МСЭ-D за исследовательский период 2018–2021 годов

ISBN 978-92-61-34104-6 (электронная версия)
ISBN 978-92-61-34114-5 (версия EPUB)
ISBN 978-92-61-34124-4 (версия Mobi)

Фото на обложке: Shutterstock

Выражение признательности

Исследовательские комиссии Сектора развития электросвязи МСЭ (МСЭ-D) обеспечивают нейтральную платформу, где собираются эксперты из правительственных органов, компаний отрасли, организаций электросвязи и академических организаций со всего мира с целью разработки практических инструментов и ресурсов для решения проблем развития. В связи с этим обе исследовательские комиссии МСЭ-D отвечают за разработку отчетов, руководящих указаний и рекомендаций на основе вкладов, полученных от членов. Решения об определении Вопросов для исследования принимаются раз в четыре года на Всемирной конференции по развитию электросвязи (ВКРЭ). Члены МСЭ, собравшиеся на ВКРЭ-17 в Буэнос-Айресе в октябре 2017 года, согласовали для 2-й Исследовательской комиссии на период 2018–2021 годов семь Вопросов в рамках общей темы "Использование услуг и приложений информационно-коммуникационных технологий в целях содействия устойчивому развитию".

Общее руководство подготовкой настоящего отчета по Вопросу 3/2: "**Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности**" и координацию работы осуществлял руководящий состав 2-й Исследовательской комиссии МСЭ-D во главе с председателем г-ном Ахмадом Реза Шарафатом (Исламская Республика Иран), которому оказывали поддержку следующие заместители председателя: г-н Нассер Аль-Марзуки (Объединенные Арабские Эмираты) (сложил полномочия в 2018 г.), г-н Абдельазиз Альзаруни (Объединенные Арабские Эмираты), г-н Филипе Мигел Антунеш Батишта (Португалия) (сложил полномочия в 2019 г.), г-жа Нора Абдалла Хассан Башер (Судан), г-жа Мария Большакова (Российская Федерация), г-жа Селина Дельгадо Кастельон (Никарагуа), г-н Яков Гасс (Российская Федерация) (сложил полномочия в 2020 г.), г-н Ананда Радж Ханал (Республика Непал), г-н Роланд Йоу Кудозиа (Гана), г-н Толибджон Олтинович Мирзакулов (Узбекистан), г-жа Алина Модан (Румыния), г-н Генри Чуквудумеме Нкемаду (Нигерия), г-жа Ке Ван (Китай), г-н Доминик Вюрж (Франция).

Подготовкой Отчета руководили Содокладчики по Вопросу 3/2 г-н Майкл Бейрн (Соединенные Штаты Америки) (сложил полномочия в 2020 г.), г-н Квадво Берджи (Соединенные Штаты Америки) (сложил полномочия в 2020 г.), г-жа Эйми К. Мичем (Соединенные Штаты Америки) и г-н Доминик Вюрж (Франция), с которыми сотрудничали следующие заместители Докладчика: г-н Дамнам Канланфей Баголибе (Того), г-н Амин Адум Бахит (Чад), г-жа Мария Большакова (Российская Федерация), г-жа Сонам Чоки (Бутан), г-н Яков Гасс (Российская Федерация) (сложил полномочия в 2020 г.); г-н Карим Аснау (Алжир), г-н Сиссе Кан ("Африканское гражданское общество в поддержку информационного общества"), г-жа Михо Наганума (Япония), г-н Жан-Давид Родни (Гаити), г-жа Джабин Вахора (Соединенные Штаты Америки), г-жа Синьсинь Вань (Китай), г-н Чэ Сок Юн (Республика Корея), г-н Мохамаду Зару (Мали).

Особая благодарность выражается координаторам по главам за их преданность делу, поддержку и опыт.

Настоящий отчет был подготовлен при поддержке координаторов БРЭ, редакторов, а также группы по подготовке публикаций и секретариата исследовательских комиссий МСЭ-D.

Содержание

Перечень таблиц и рисунков

Таблицы

Рисунок

Резюме

Цель работы по Вопросу 3/2 (Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности) Сектора развития электросвязи МСЭ (МСЭ-D) заключается в разработке отчетов о передовом опыте по различным аспектам кибербезопасности.

В настоящем документе представлен Заключительный отчет по Вопросу 3/2 за прошедший четырехлетний исследовательский период (2018–2021 гг.). Программа работы по Вопросу 3/2 была принята на Всемирной конференции по развитию электросвязи, прошедшей в Буэнос-Айресе в 2017 году (ВКРЭ-17).

Деятельность, проводимая в течение предыдущих исследовательских периодов, была посвящена доступным учебным курсам (2010–2014 гг.) и семинарам-практикумам для ознакомления развивающихся стран с работой широкого круга субъектов и разнообразным контентом (2014–2017 гг.).

В течение исследовательского периода 2018–2021 годов 2-я Исследовательская комиссия МСЭ-D выполнила большинство пунктов программы работы. В этот же исследовательский период был организован семинар-практикум.

Настоящий Отчет по Вопросу 3/2 основан на материалах, содержавшихся во вкладах членов МСЭ, которые поступили в течение этого исследовательского периода. В Отчете представлен обзор спама и вредоносных программных средств, а также способов борьбы с ними. Приведен ряд уроков, которые необходимо учесть при планировании национальных мер реагирования и кампаний по повышению осведомленности в области кибербезопасности. Описаны конкретные действия, предпринимаемые в интересах уязвимых групп населения, в том числе лиц с ограниченными возможностями и детей. Наряду с этим в Отчете представлены различные соображения, касающиеся "умных" городов, новых технологий и защиты данных.

В современном цифровом мире, где в повседневную жизнь граждан и экономику в целом все глубже проникают цифровые технологии, существует повышенный риск роста уязвимости для кибератак и подверженности их воздействию. Кибербезопасность определена как приоритет и важнейшая задача для частного сектора, правительств и пользователей интернета во всем мире, и она имеет решающее значение для обеспечения безопасного и надежного прогресса, который позволит обществу развиваться.

Цель данного Отчета – представить обновленные видение и практику на основе опыта членов МСЭ. Учитывая, что общая среда и ландшафт угроз постоянно меняются, задача Отчета заключается лишь в том, чтобы отразить текущую ситуацию в области кибербезопасности, которая характеризуется высокой степенью изменчивости. Кроме того, выпуск настоящего Отчета происходит в контексте весьма специфических и неведомых ранее обстоятельств: несмотря на отсутствие какой-либо конкретной связи с текущей пандемией, проблема воздействия COVID-19 занимала внимание многих авторов вкладов и отражалась в дебатах, проводимых в ходе работы по Вопросу 3/2.

Меры реагирования и предлагаемые действия, изложенные в настоящем Отчете, предназначены в помощь при обеспечении высокого уровня кибербезопасности всеми Государствами – Членами МСЭ и могут также служить полезным инструментом преодоления потенциальных кризисов в будущем, в дополнение к другим мерам, реализуемым МСЭ.

В **Главе 1** содержится актуальная информация о спаме и вредоносных программных средствах, а также о мерах по смягчению их воздействия. Следует отметить, что Исследовательская комиссия не получила вкладов, посвященных непосредственно данному вопросу.

В **Главе 2** рассматриваются возможности совершенствования национальных средств кибербезопасности путем повышения осведомленности и создания потенциала.

В **Главе 3** представлена информация о деятельности по защите ребенка в онлайновой среде.

В **Главе 4** рассматриваются проблемы в области кибербезопасности, с которыми сталкиваются лица с ограниченными возможностями.

В **Главе 5** рассматриваются проблемы в области кибербезопасности, связанные с появляющимися технологиями, такими как интернет вещей (IoT) и облачные вычисления.

В **Главе 6** приведены различные точки зрения о потенциале кибербезопасности для обеспечения защиты персональных данных.

И наконец, в **Главе 7** представлены области будущих исследований.

В дополнение к настоящему Отчету следует также отметить, что в рамках Вопроса 3/2 был пересмотрен вопросник, на основе которого составляется Глобальный индекс кибербезопасности (GCI), и представлены замечания и предложения, что позволяет Бюро развития электросвязи (БРЭ) проводить ежегодное обследование среди Государств – Членов МСЭ. В частности, по инициативе Бразилии, в рамках Вопроса 3/2 было разработано обследование, включенное в GCI в качестве приложения. Предложенные изменения были учтены при разработке четвертой версии GCI 2020.

В настоящем Отчете GCI подробно не рассматривается. Вместе с тем в рамках Вопроса 3/2 подчеркивается положительный результат коллективных усилий и плодотворного сотрудничества с БРЭ, так как ответы на включенное в приложение обследование позволят собрать информацию о регуляторной политике, которую БРЭ предоставит членам, и тем самым будет выполнен пункт "n" исследования о круге ведения Вопроса 3/2.

Глава 1 – Обновленная информация о спаме и вредоносных программных средствах, включая меры по смягчению их воздействия

В данном разделе содержится анализ развития спама и вредоносных программных средств, а также описание ряда контрмер, которые необходимо предпринять на национальном, региональном и международном уровнях в соответствии с положениями Резолюции 45 (Пересм. Дубай, 2014 г.) Всемирной конференции по развитию электросвязи (ВКРЭ)[1]о механизмах совершенствования сотрудничества в области кибербезопасности, включая противодействие спаму и борьбу с ним. Таким образом, представленная здесь информация согласуется с пунктами b) и m) Раздела 2 круга ведения Вопроса 3/2, изложенного в Заключительном отчете ВКРЭ-17:

b) обсудить подходы и передовой опыт в области оценки воздействия спама и вредоносных программ в рамках сети, а также меняющихся и возникающих угроз, и представить необходимые меры и руководящие указания, в частности методы смягчения последствий, законодательные и регуляторные аспекты, которые могли бы использовать страны, учитывая существующие стандарты и имеющиеся инструменты;

m) разработать руководство по мерам, направленным на борьбу со спамом и вредоносными программными средствами на национальном, региональном и международном уровнях[2].

1.1 Положении дел в области спама и вредоносных программных средств

Несмотря на отсутствие какого-либо общепринятого определения, в большинстве случаев под термином "спам" понимают незатребованные массовые электронные сообщения, передаваемые по электронной почте или в виде текстовых сообщений с помощью компьютера или мобильного телефона[3]. Потребители обычно сталкиваются со спамом в виде рекламы, в том числе "мусора" или нежелательных рекламных сообщений электронной почты, текстовых сообщений и контактов в социальных сетях.

Хотя спам, как правило, предполагает поиск потенциальных клиентов в коммерческих целях, он может также преследовать преступные цели, включая фишинг, используя аналогичные данные, генерируемые пользователем. Выдавая себя за доверенные третьи лица, злоумышленники используют фишинговые сообщения электронной почты, с тем чтобы побудить адресатов раскрыть свои персональные данные (учетные записи доступа, пароли и т. д.) и/или банковские данные.

Спам создает риски для безопасности подключенных пользователей и организаций, и это связано не только с тем, что он легко распространяется через интернет и службы электронной связи (электронная почта, веб-сайты, социальные сети, SMS и MMS), но и с тем, что он может нести в себе вредоносные программные средства. Страны внедряют различные технические и регуляторные механизмы для борьбы со спамом, и это дает определенные результаты.

Вредоносные программные средства, в свою очередь, переживают значительный бум в последнее время благодаря развитию интернета, в частности мобильного интернета. Вредоносные программные средства – это общий термин для программного обеспечения, предназначенного специально для нанесения вреда компьютерам или компьютерным системам[4].

Кроме того, расширение возможностей для установления соединений, появление новых технологий и рост числа пользователей открыли новые возможности для создания и использования вредоносных программных средств. Такая парадигма усложняет обеспечение кибербезопасности, обнажая проблематичные места и расширяя область атаки, подверженную угрозам, исходящим от вредоносных программных средств. В дополнение к традиционным вредоносным программам (вирусам, червям, троянам, программам-шпионам и программам, содержащим рекламу, спаму, руткитам и т. д.) появились

---

1 МСЭ, Заключительный отчет Всемирной конференции по развитию электросвязи (Буэнос-Айрес,2017 г.), стр. 409.
2 Там же, стр. 727–728.
3 См. Рекомендации МСЭ-Т X.1230–X.1240 о противодействии спаму.
4 См. Добавление 9 к Рекомендациям МСЭ-Т серии X – МСЭ-Т X.1205 "Добавление к руководящим указаниям по сокращению количества вредоносных программных средств в сетях ИКТ".

новые, более изощренные виды вредоносных программных средств, как, например, бот-сети, программы-вымогатели и мобильные вредоносные программы.

Иными словами, борьба со спамом и вредоносными программными средствами имеет жизненно важное значение для безопасности пользователей и развития предприятий.

1.2 Спам и вредоносные программные средства: статистика, тенденции, развитие и воздействие на сети электронной связи

По состоянию на март 2020 года доля спама в мировом трафике сообщений электронной почты составляла 53,95%[5]. В последние годы этот показатель значительно снизился – с 69% в 2012 году до 55% в 2018 году, что, вероятно, обусловлено повышением уровня осведомленности о кибербезопасности и технологическим прогрессом. Большая часть спама, приходящего в адрес пользователей, носит рекламный характер, включая характер маркетинговой информации. Согласно результатам одной из оценок, спам обходится предприятиям почти в 20,5 миллиардов долларов США в год в виде потери производительности и технических расходов. Предполагается, что эта сумма может вырасти до 257 миллиардов долларов США в год, если спам продолжит расти текущими темпами[6].

По одной из оценок, на различные аферы и мошенничество приходится около 2,5% всего спама, при этом значительная часть таких операций (92%) может иметь вредоносный характер, т. е. может быть связанной с использованием вредоносных программных средств для причинения вреда пользователям или нарушения безопасности их ИТ-систем в тех или иных целях[7]. Согласно другой оценке, в 2018 году было выявлено около 812,67 миллионов различных случаев заражения вредоносными программными средствами[8]. Доля вредоносных программ для мобильных устройств увеличилась на 54%, а программ-вымогателей – на 350%; при этом ежегодные финансовые потери, связанные с заражением программами-вымогателями, оцениваются в 6 миллиардов долларов США (до 2021 г.).

Поскольку спам и вредоносные программные средства могут генерировать значительный трафик, они могут оказывать существенное негативное воздействие на инфраструктуру и операторов сетей и, следовательно, на пользовательский опыт потребителей. Кроме того, вызванные спамом проблемы, включая обусловленные ими проблемы в работе сетей, могут нанести ущерб репутации операторов.

Для решения таких проблем, включая потенциально массивные потоки нежелательного трафика, и обеспечения качества сети операторам может потребоваться разработать новые инструменты, в том числе инвестировать в защиту и расширение существующей инфраструктуры. Так, поставщики услуг могли бы инвестировать в антиспамовые фильтры для повышения качества предлагаемых ими услуг. Это может привести к тому, что у операторов и поставщиков услуг электронной связи возникнут дополнительные затраты.

1.3 Методы, применяемые для борьбы со спамом и вредоносными программными средствами и снижения их воздействия

1.3.1 Технические методы борьбы со спамом и вредоносными программными средствами и снижения их воздействия

Незатребованные сообщения электронной почты – это один из основных каналов передачи вредоносных программных средств. Для эффективной борьбы со спамом и вредоносными программами необходимо разорвать цепочку передачи. По мере развития технологий такие инструменты, как антиспамовые фильтры и антивирусное программное обеспечение, остаются эффективными механизмами для борьбы со спамом и вредоносными программами. Эффективность таких инструментов можно повысить, если использовать их вместе с новыми технологиями, такими как искусственный интеллект (ИИ). Учитывая это, один из методов надлежащей практики для пользователей предполагает регулярное обновление антиспамовых фильтров и антивирусного программного обеспечения.

---

5 Statista, Global spam volume as percentage of total e-mail traffic from January 2014 to September 2020, by month.
6 Spam Laws, Spam statistics and facts.
7 DataProt, What's on the other side of your inbox – 20 SPAM statistics for 2021.
8 PurpleSec, 2021 Cyber Security Statistics- The Ultimate List of stats, data & trends.

Кроме того, для сокращения таких цепочек передачи поставщики услуг могут прибегнуть к применению соответствующей политики, как, например, в отношении инфраструктуры политики отправителя[9], идентификации почты с использованием доменных ключей[10], аутентификации сообщений, создания отчетов и определения соответствия по доменному наименованию[11], а также к внесению в списки блокировки в режиме реального времени.

Операторы сетей электронной связи и поставщики услуг интернета также могут принимать определенные меры для решения проблем, связанных с блокировкой IP-адресов. Одним из примеров таких мер является применение протокола безопасности граничных шлюзов с использованием инфраструктуры открытых ключей ресурсов[12]. К числу других инициатив относятся:

– взаимосогласованные нормы безопасности маршрутизации, предназначенные для совместного предотвращения перехвата маршрутов, подмены IP-адресов и других вредоносных действий на основе новейших технологий, которые могут привести к распределенным атакам типа "отказ в обслуживании" (DDoS), перехвату информации, потере доходов, нанесению вреда репутации и т. д.[13];

– рабочая группа по борьбе со злоупотреблениями рассылкой сообщений, вредоносными программами и мобильной связью, регулярно публикующая примеры передового опыта борьбы со злонамеренными сообщениями, всеми типами вредоносных программ (включая бот-сети), спамом, вирусами, атаками типа "отказ в обслуживании" (DoS) и любыми другими видами злоупотреблений в сети[14].

Среди других инициатив, направленных на борьбу со спамом и вредоносными программными средствами, – Общество Интернета[15], Ассоциация глобальной системы подвижной связи[16], проект Spamhaus[17], Рабочая группа по борьбе с фишингом[18]и Коалиция против шпионского ПО[19].

1.3.2 Регуляторные подходы к борьбе со спамом и вредоносными программными средствами и снижению их воздействия

Учитывая проблемы и затраты, с которыми сопряжена борьба со спамом и вредоносными программными средствами, в последние годы некоторые регионы и страны приняли новую или укрепили существующую законодательную базу, с тем чтобы обеспечить наличие инструментов для активизации борьбы с такими атаками. При разработке законодательства и политики страны руководствуются внутренними требованиями, такими как Общий регламент защиты данных (GDPR) Европейского союза, согласно которому для сбора данных необходимо получить согласие соответствующего пользователя.

Еще одним примером является Конвенция Африканского союза о кибербезопасности и защите персональных данных (Конвенция Малабо), согласно которой государствам-участникам в Африканском регионе рекомендуется включить предлагаемый комплекс стандартов в национальное законодательство. Статья 4.3 Конвенции гласит: "*на территории государств-участников запрещается осуществление прямого маркетинга на основе любых форм связи с использованием в какой бы то ни было форме сведений о лице, не предоставившем предварительного согласия на получение услуг или продуктов упомянутого прямого маркетинга с помощью таких средств*". Тем не менее Конвенция разрешает осуществлять прямой маркетинг при определенных условиях. В частности, "*прямой маркетинг с помощью электронной почты разрешается при условии, что: a) сведения об адресате были получены непосредственно от него (нее); b) получатель дал согласие на то, чтобы с ним связались маркетинговые партнеры; iii) прямой маркетинг касается аналогичных продуктов или услуг, предоставляемых одним и тем же физическим или юридическим лицом*" (п. 4.4).

---

9 Mimecast, Everything you need to know about SPF.
10 DKIM.org, DomainKeys Identified Mail (DKIM).
11 DMARC, Domain-based Message Authentication, Reporting and Conformance.
12 RFC Editor, RFC 6480- An Infrastructure to Support Secure Internet Routing, February, 2012.
13 MANRS, Mutually Agreed Norms for Routing Security.
14 Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG), Why M³AAWG?.
15 Общество Интернета, Комплект материалов Общества Интернета по кибербезопасности.
16 GSMA, GSMA Security.
17 Spamhaus, Spamhaus ZEN + DBL + RPZ.
18 APWG, Unifying the global response to cybercrime through data exchange research and public awareness.
19 Anti-Spyware Coalition, Internet, Marketing y Actualidad.

По мере внедрения как GDPR Европейского союза, так и Конвенции Малабо можно будет оценить и определить всю полноту их воздействия на снижение масштабов спама и использования вредоносных программных средств.

1.3.3 Вклады по Вопросу 3/2, касающиеся борьбы со спамом и вредоносными программными средствами и смягчения вызванных ими последствий

В рамках исследовательского периода ряд стран и Членов Секторов МСЭ представили дополнительные примеры методов, применяемых для борьбы со спамом и вредоносными программными средствами.

– Авторы некоторых вкладов рассказали о том, как они осуществляют сбор информации об угрозах кибербезопасности в режиме реального времени в целях разработки на этой основе стратегий обеспечения надежной кибербезопасности. В условиях эпохи информационных технологий данные в режиме реального времени имеют ключевое значение для защиты информации. Комбинированное принятие мер, направленных на повышение осведомленности о ситуации и поиск потенциальных киберугроз, помогает странам и государственным и частным организациям выявлять угрозы по мере их возникновения и, таким образом, обеспечивать более эффективную защиту своих ресурсов. Поэтому для того, чтобы помочь защитить организации от целевых атак и устойчивых угроз, крайне важно разработать устойчивые сетевые стратегии, опирающиеся на аналитические данные по безопасности[20].

– Авторы некоторых вкладов составляют карты угроз киберпреступности, с тем чтобы понять различные варианты воздействия спама и вредоносных программных средств на пользователей интернета (например, фишинг и мошенничество при проведении лотерей) и предприятия (например, несанкционированный доступ к системе и атаки типа DoS). Так, в 2017 году Кот-д'Ивуар провел мониторинг угроз и преступлений в области киберпреступности, осуществив их учет с помощью Платформы для борьбы с киберпреступностью (PLCC), что позволило собрать ценную качественную информацию для направления оперативной деятельности в целях улучшения просвещения потребителей и представителей предприятий. Были выявлены признаки мошенничества при предоставлении услуг мобильных денег; при этом было задокументировано 453 случая такого мошенничества, в результате которых сумма нанесенного ущерба составила почти 800 000 долларов США. Мошенничество в области услуг мобильных денег – это хорошо продуманная афера, при которой после перевода средств на счет или со счета мобильных денег с помощью команд USSD (неструктурированные данные дополнительных услуг) мошенники звонят жертве и утверждают, что возникла проблема с переводом; если им удается завладеть доверием жертвы, мошенники могут удаленно снять деньги со счета мобильных денег жертвы, используя те же самые команды USSD[21].

– Авторы некоторых вкладов рассказали о том, как они организовывают открытые и прозрачные процессы, направленные на определение необходимых мер и побуждение соответствующих заинтересованных сторон принять такие меры в целях значительного снижения угроз, возникающих в результате автоматизированных и распределенных атак (например, с использованием бот-сетей). С появлением новых бот-сетей, способных оказывать огромное давление на сети за счет использования данных со скоростью свыше одного терабита в секунду, традиционные методы смягчения последствий атак типа DDoS, заключающиеся в резервировании ресурсов поставщиками услуг сетевого доступа, теряют свою эффективность. Для смягчения последствий автоматизированных и распределенных кибератак государственному и частному секторам необходимо поддерживать сотрудничество на непрерывной основе[22].

– Компания может эффективно защитить себя от угрозы атак с использованием программ-вымогателей, предприняв ряд простых мер. В недавно опубликованном консультативном заключении, посвященном программам-вымогателям, Национальный центр кибербезопасности (NCSC) Соединенного Королевства рекомендует применять ряд простых методов для снижения рисков, в частности:

  • поддержание устройств и сетей в актуальном состоянии (например, осуществляя оперативное внесение обновлений и исправлений, а также их регулярное сканирование);

  • предотвращение и обнаружение боковых перемещений в корпоративных сетях;

---

[20] Документ 2/167 ИК2 МСЭ-D, Symantec Corporation (Соединенные Штаты Америки).
[21] Документ 2/174 ИК2 МСЭ-D, Кот-д'Ивуар.
[22] Документ SG2RGQ/153 + Приложения ИК2 МСЭ-D, Соединенные Штаты Америки.

- применение сканера вирусов;
- резервное копирование всех файлов[23].

Полный и подробный перечень рекомендаций доступен на веб-сайте NCSC[24].

– Авторы некоторых вкладов рассказали о том, как они создают гибкую национальную систему кибербезопасности, адаптированную к меняющимся потребностям. Так, Соединенное Королевство приступило к осуществлению Программы активной киберзащиты, в рамках которой основные усилия направлены на принятие положительных технических мер по улучшению онлайновой среды для всех. Данная программа принесла существенную и ощутимую пользу правительственным сетям. Она реализуется в интересах сетей государственной службы Соединенного Королевства и направлена на то, чтобы продемонстрировать практическую пользу и возможные последующие шаги[25]. Через год после начала осуществления программы Соединенное Королевство представило обновленную информацию о ней в рамках непрерывной работы над преодолением соответствующих вызовов[26].

– Авторы некоторых вкладов предпринимают меры по повышению осведомленности представителей уязвимых сообществ (например, лиц с ограниченными возможностями) об их подверженности повышенному риску. Спамеры и хакеры используют все более изощренные методы для определения наличия инвалидности у потенциальных жертв взлома. Иногда "угонщики" используют инвалидность человека, с тем чтобы выдать себя за лицо, чей адрес электронной почты был взломан[27].

– Авторы некоторых вкладов внедряют службы регистрации заявлений о фишинговых сообщениях электронной почты. Сбор информации о вредоносных сообщениях электронной почты с помощью краудсорсинга и принятие мер в отношении задействованных в этом доменов и других лиц – это эффективный инструмент для снижения масштабов киберпреступности и мошенничества. Так, в течение первых четырех месяцев работы Службы регистрации заявлений о подозрительных электронных сообщениях NCSC Соединенного Королевства и полиция лондонского Сити устранили свыше 16 000 онлайновых угроз, информация о которых была получена от населения[28].

---

23 Документ SG2RGQ/155 ИК2 МСЭ-D, Соединенное Королевство.
24 Национальный центр кибербезопасности (NCSC), Guidance: Mitigating malware and ransomware attacks.
25 Документ SG2RGQ/55 ИК2 МСЭ-D, Соединенное Королевство.
26 Документ SG2RGQ/175 ИК2 МСЭ-D, Соединенное Королевство.
27 Документ 2/71 ИК2 МСЭ-D, Глобальная инициатива по расширению охвата информационно-коммуникационными технологиями (G3ict).
28 Документ SG2RGQ/234 ИК2 МСЭ-D, Соединенное Королевство.

Глава 2 – Совершенствование средств кибербезопасности на национальном уровне: повышение осведомленности и создание потенциала

На протяжении последних лет ИКТ переживают стремительное развитие и внедрение инновационных решений. Во всем мире они играют важную роль, позволяя странам расширять свою цифровую экономику и поддерживать социальное процветание. Кроме того, как показала пандемия COVID-19, в своей повседневной жизни люди все больше зависят от ИКТ. Учитывая такие реалии странам крайне необходимо не сворачивать принятие значимых мер, направленных на совершенствование и повышение качества средств кибербезопасности на национальном уровне для защиты от связанных с ней рисков и преодоления соответствующих вызовов.

В настоящей главе рассматриваются ключевые направления деятельности по совершенствованию средств кибербезопасности на национальном уровне, в том числе:

- создание соответствующих национальных органов по вопросам кибербезопасности;
- группы реагирования на нарушение компьютерной защиты (CERT)/группы реагирования на инциденты в сфере компьютерной безопасности (CSIRT)/группы реагирования на компьютерные инциденты (CIRT);
- кампании, направленные на повышение осведомленности в области кибербезопасности;
- системы управления рисками в области кибербезопасности;
- государственно-частное партнерство;
- прочие инициативы по созданию потенциала.

В рамках данного исследовательского периода ряд организаций представили вклады, посвященные соответствующим вопросам. В **Приложении 1** содержится перечень соответствующих текущих мероприятий в области кибербезопасности, проводимых Государствами-Членами, организациями, частным сектором и гражданским обществом на национальном, региональном и международном уровнях. В **Приложении 2** содержится перечень соответствующих примеров передового опыта и извлеченных уроков, представленных некоторыми из указанных организаций.

2.1 Создание соответствующих национальных органов по вопросам кибербезопасности

Появление новых достижений и инновационных решений в секторе ИКТ происходит на фоне усугубления рисков и вызовов в области кибербезопасности. Для преодоления таких вызовов правительствам необходимо непрерывно осуществлять оценку и доработку существующих на национальном уровне средств и стратегий в области кибербезопасности, в том числе создавая соответствующие национальные органы по вопросам кибербезопасности. В течение исследовательского периода Государства-Члены рассказали о своих подходах к созданию таких органов. В разных странах применяются разные подходы, что обусловлено внутренними структурами управления, правилами, положениями и политикой.

Органы, занимающиеся вопросами кибербезопасности, обладают разным опытом и специализацией, однако, как правило, выполняют одни и те же ключевые функции, включая разработку и координацию внедрения регуляторной политики, разработку и проведение кампаний, направленных на повышение уровня осведомленности о кибербезопасности, предоставление пользователям (от крупных организаций до отдельных лиц и малых предприятий) актуальной информации, а также подготовку заявлений и руководящих указаний по инцидентам в области кибербезопасности. Учитывая весь спектр вопросов, подпадающих под сферу кибербезопасности, правительствам крайне важно создать условия, необходимые для координации действий и поддержания сотрудничества между различными органами и структурами, а также между государственным и частным секторами.

Например, NCSC Соединенного Королевства сотрудничает с другими компетентными государственными органами и руководит усилиями, направленными на обеспечение ощутимого снижения воздействия, вызванного атаками с помощью программ-вымогателей[29]. В случае возникновения такой атаки организациям рекомендуется обращаться в Национальное агентство по борьбе с преступностью, сертифицированную компанию по реагированию на киберинциденты или инициативу "Партнерство по обмену информацией в области кибербезопасности". Национальный центр кибербезопасности в сотрудничестве с Национальным агентством по борьбе с преступностью руководил усилиями, предпринимавшимися в Соединенном Королевстве в ответ на атаку с использованием программы-вымогателя WannaCry. При возникновении каждого инцидента центр публикует заявления и руководящие указания как для крупных организаций, так и для домашних пользователей и малых предприятий. Наиболее актуальная информация также размещается на странице учетной записи центра в Twitter (@NCSC).

Бразилия приняла свою Национальную стратегию в области кибербезопасности (E-Ciber), которая была ратифицирована президентом Бразилии и опубликована в феврале 2020 года[30]. При разработке этой прогрессивной стратегии, представляющей собой внедряемую федеральным правительством концепцию кибербезопасности на период 2020-2023 годов, Бразилия применила исчерпывающий и всеобъемлющий подход с привлечением многочисленных заинтересованных сторон, в том числе представителей правительства, частного сектора и академических организаций. Ратифицировав E-Ciber, Бразилия дополнила законодательную базу ранее отсутствовавшим компонентом. В соответствии с E-Ciber Бразилия определила 10 стратегических направлений, наметив по каждому из них определенные меры и инициативы. К таким направлениям, в частности, относятся следующие:

– усиление управления деятельностью в сфере кибербезопасности;
– внедрение модели централизованного управления национальной кибербезопасностью;
– доработка национальной правовой базы в сфере кибербезопасности;
– расширение международного сотрудничества Бразилии в области кибербезопасности.

В Бенине различные государственные структуры участвуют в управлении ИКТ в стране[31]. Агентство по информационным услугам и системам (ASSI), бывшее Бенинское агентство по информационно-коммуникационным технологиям (ABETIC), – это национальный орган, отвечающий за практическую реализацию программ и разработку стратегий развития защищенных цифровых информационных систем и услуг в стране. В сферу его ответственности входит ряд ключевых направлений деятельности, в том числе:

– реализация ключевых проектов в области "умного" управления и электронной коммерции;
– разработка, обновление и практическая реализация генеральных планов национальных информационных систем;
– обеспечение технической, прикладной и финансовой согласованности национальных информационных систем и услуг;
– обеспечение хостинга и контроля важнейших данных и информации государства и операторов важнейшей инфраструктуры, а также безопасного доступа к таким данным и информации.

В Чаде Национальное управление информационной безопасности и электронной сертификации (ANSICE), созданное в феврале 2015 года, подчиняется непосредственно администрации президента[32]. Управление функционирует с января 2018 года и обладает широкими полномочиями и компетенцией, в том числе в области обеспечения безопасности информационных систем и сетей по всей стране.

Соединенное Королевство также представило информацию об обновленном исследовании внедрения надлежащей практики обеспечения безопасности устройств интернета вещей (IoT) пользователей. В частности:

– был опубликован Свод правил и норм по обеспечению безопасности пользователей IoT, в котором изложены 13 общих принципов (доступен также на немецком, испанском, французском, японском, корейском, китайском и португальском языках);

---

29 Документ SG2RGQ/155 ИК2 МСЭ-D, Соединенное Королевство.
30 Документ SG2RGQ/216 ИК2 МСЭ-D, Бразилия.
31 Документ 2/152 ИК2 МСЭ-D, Бенин.
32 Документ 2/136 ИК2 МСЭ-D, Чад.

– были проведены общественные консультации по предлагаемым нормативным и законодательным актам;

– было поддержано внедрение первого всемирно применимого стандарта безопасности в области интернета вещей ETSI EN 303 645[33], который был опубликован Европейским институтом стандартизации в области электросвязи (ETSI). Многие организации уже внедрили данный и предшествовавший ему стандарт, ETSI TS 103 645, при производстве своей продукции и организации механизмов сертификации;

– заинтересованным сторонам было предложено представить свое мнение о регуляторных предложениях Соединенного Королевства в отношении сферы применения, обязательств, требований безопасности и подхода к обеспечению соблюдения;

– Министерству цифровых технологий, культуры, средств массовой информации и спорта и NCSC было поручено совместно разработать руководящие указания и онлайновые вебинары для производителей продукции в области IoT, которые неоднократно проводились с учетом различных часовых поясов;

– было обеспечено обновление ситуационной карты с нанесением на нее существующих стандартов, а также было оказано содействие организациям во внедрении надлежащей практики во всех сферах IoT[34].

2.2 Группы реагирования на нарушение компьютерной защиты (CERT)/группы реагирования на инциденты в сфере компьютерной безопасности (CSIRT)/ группы реагирования на компьютерные инциденты (CIRT)

Национальный потенциал для реагирования на инциденты (в виде CERT/CSIRT/CIRT) – это ключевой инструмент для решения оперативных задач в области кибербезопасности. Он способствует координации действий, направленных на сбор и обработку информации, касающейся кибербезопасности, а также на принятие мер реагирования на инциденты в области безопасности. В течение исследовательского периода исследовательская комиссия получила ключевые вклады по данной теме от Государств-Членов и Членов Секторов МСЭ, при этом многие них высказали единое мнение о том, что национальные группы CERT/CSIRT/CIRT должны выполнять функцию основного контактного центра по вопросам кибербезопасности и координационного центра по реагированию на возникающие инциденты.

Так в апреле 2016 года была учреждена Бутанская группа реагирования на компьютерные инциденты (BtCIRT) для усиления кибербезопасности в стране путем содействия координации действий, направленных на сбор и обработку информации, касающейся кибербезопасности, и создания национального потенциала для борьбы с инцидентами в области компьютерной безопасности[35]. BtCIRT является подразделением, действующем при Департаменте информационных технологий и электросвязи Министерства информации и связи. В соответствии со своим мандатом BtCIRT выступает в качестве национального контактного центра по вопросам кибербезопасности и представляет страну на международных форумах. Передача одной организации функции по координации всех инициатив в области кибербезопасности позволяет предотвратить дублирование предпринимаемых мер и достигаемых результатов. Поскольку большинство международных форумов и групп, занимающихся вопросами кибербезопасности, взаимодействуют с группами CIRT, уполномоченными осуществлять деятельность на национальном уровне, правительствам необходимо определить CIRT или назначить одну организацию, которая будет руководить реализацией национальных инициатив и планов в области кибербезопасности.

Несмотря на то, что BtCIRT была создана как контактный центр по вопросам кибербезопасности в Бутане, ей было нелегко завоевать доверие заинтересованных сторон, главным образом вследствие того, что она была относительно новым органом и имела ограниченные технические возможности. Кроме того, крупные корпорации, такие как операторы электросвязи и банки, уже обладают надежной инфраструктурой ИКТ и необходимыми техническими возможностями, что затрудняет сотрудничество между ними и правительством. Сотрудничество и взаимодействие между заинтересованными сторонами, особенно поставщиками услуг интернета и CIRT, необходимо для поиска и внедрения согласованных решений по безопасности пользователей интернета. Бутан обратился к международным организациям с просьбой оказать помощь в наращивании жизненно необходимого технического потенциала BtCIRT.

---

[33] ETSI, Стандарт ETSI EN 303 645, Cyber Security for Consumer Internet of Things: Baseline Requirements.
[34] Документ SG2RGQ/241 ИК2 МСЭ-D, Соединенное Королевство.
[35] Документ SG2RGQ/79 ИК2 МСЭ-D, Бутан.

Наконец, литовская компания NRD Cyber Security предложила, чтобы национальные и отраслевые группы CSIRT не только выступали в качестве основного контактного центра по инцидентам в области кибербезопасности, но и координировали реагирование на них, а также способствовали созданию и стимулировали формирование в стране дополнительного независимого и распределенного потенциала для противодействия киберугрозам[36].

2.3 Кампании, направленные на повышение осведомленности

В мире наблюдается широкое использование ИКТ со стороны различных заинтересованных сторон – от правительств и коммерческих организаций до организаций местного уровня и отдельных граждан. Однако многие пользователи не в полной мере осознают сопряженные с этим риски с точки зрения кибербезопасности. Для некоторых развивающихся стран недостаточный уровень осведомленности пользователей является наиболее труднопреодолимым вызовом. Во вкладах, полученных в течение исследовательского периода, прослеживается общее понимание того, что кампании по повышению осведомленности о кибербезопасности играют важную роль в преодолении таких вызовов. Основная цель таких кампаний заключается в том, чтобы стимулировать внедрение моделей безопасного поведения в онлайновой среде.

Страны и предприятия стремятся найти креативные пути разработки эффективных кампаний, в том числе для охвата широкого круга пользователей.

Так, Мексика поделилась своим опытом разработки и проведения обследования среди пользователей интернета, который можно взять за основу для внедрения различных подходов к проведению кампаний по повышению осведомленности о кибербезопасности[37].

В некоторых странах провели обследования, с тем чтобы выявить основные проблемы граждан и на основе полученных результатов разработать кампании по повышению осведомленности. Опираясь на свой опыт, Мексика также представила следующие извлеченные уроки:

– установите и обновите антивирусную защиту;
– регулярно меняйте пароли и следите за тем, чтобы они были надежными (т. е. используйте комбинацию цифр, букв и специальных символов);
– регулярно создавайте резервные копии данных;
– подключайтесь только к защищенным общественным сетям.

Еще один пример представил Бутан, где BtCIRT разработала программы повышения осведомленности, направленные на удовлетворение потребностей в области кибербезопасности, возникающих в связи с повседневной профессиональной и персональной деятельностью конечных пользователей по стране в целом[38]. Участникам было показано, как осуществляют атаки мошенники, использующие социальную инженерию и фишинг, как безопасно общаться с помощью электронной почты и в социальных сетях и каковы общие угрозы и меры, направленные на их устранение. Разработанные Бутаном программы повышения осведомленности оказались весьма успешными в плане информирования пользователей о рисках в области безопасности и получили положительные отзывы. В настоящее время в центре внимания BtCIRT находятся государственные служащие, однако группа надеется расширить свою целевую аудиторию, включив в нее детей и пользователей, представляющих уязвимые группы населения.

Еще один пример креативного подхода, приведенный Бутаном, – учреждение ежегодного национального конкурса веб-сайтов, организованного Департаментом информационных технологий и электросвязи Министерства информации и связи[39]. Участие в конкурсе принимают все государственные веб-сайты, лучший из которых определяется по следующим основным критериям:

– практичность и надежность;
– контент и актуальность;

---

[36] Документ 2/172 ИК2 МСЭ-D, NRD Cyber Security (CS) (Литва).
[37] Документ 2/165 ИК2 МСЭ-D, Мексика.
[38] Документ SG2RGQ/79 ИК2 МСЭ-D, Бутан.
[39] Документ SG2RGQ/135 ИК2 МСЭ-D, Бутан.

– безопасность и время безотказной работы;
– внешний вид;
– интерактивный дизайн.

Аналогичным образом в ноябре 2019 года Бразилия через Национальное агентство электросвязи (ANATEL) приступила к реализации кампании по повышению уровня осведомленности в области кибербезопасности под названием #ConexãoSegura (Безопасное соединение)[40]. В рамках кампании потребителям были даны рекомендации по защите персональных данных и созданию безопасных паролей. Кампания была разработана в ответ на жалобы потребителей о попытках мошенничества, а также с тем чтобы развеять сомнения относительно того, как защитить персональные данные. С началом пандемии COVID-19 и резким увеличением числа новых афер в помощь пользователям были созданы новые посты о мошенничестве и махинациях в связи коронавирусом. Они были размещены в социальных сетях Anatel, включая Facebook, Twitter, Instagram и LinkedIn. Ниже приведены некоторые примеры передового опыта, использованного в ходе кампании:

– используйте все возможности для обеспечения безопасности, предоставляемые мобильными приложениями, как, например двухфакторная аутентификация;
– создавайте надежные и безопасные пароли, комбинируя прописные и строчные буквы, цифры и специальные символы;
– опасайтесь сообщений электронной почты и других сообщений с прикрепленными счетами и всегда обращайтесь в отдел по работе с клиентами компании для проверки подлинности документа;
– не предоставляйте персональные данные или пароли, отвечая на звонки неизвестных лиц[41].

Соединенное Королевство представило исследование передового опыта обеспечения устойчивой системы кибербезопасности малых и средних предприятий, рассказав об усилиях, предпринимаемых для повышения киберустойчивости организаций по всей стране[42]. Одним из примеров таких усилий является коммуникационная кампания "Киберосведомленность", которая не ограничивается лишь повышением уровня осведомленности, а направлена на повсеместное внедрение базовых моделей поведения для обеспечения кибербезопасности. Реализация ориентированной на общественность и малые предприятия кампании была начата в апреле 2020 года, после того как кампания была оперативно доработана с учетом изменения характеристик киберугроз в связи пандемией COVID-19. В рамках этой кампании велась пропаганда действенных мер по смягчению воздействия угроз, в дополнение к которым были разработаны новые руководящие указания по обеспечению безопасности при выполнении работы на дому, переводе деятельности предприятий в онлайновую среду и использовании видеоконференцсвязи. Среди других инструментов:

– "Руководство для малого бизнеса: кибербезопасность";
– "Руководство для малого бизнеса: реагирование и восстановление", содержащее план последовательных действий, с помощью которого МСП могут подготовиться к киберинцидентам и смягчить их потенциальное воздействие;
– "Exercise in a Box", бесплатный онлайновый инструмент, направленный на то, чтобы помочь МСП проверить свою киберустойчивость и пройти микрокурс, не имея при этом каких-либо основательных технических знаний;
– Руководство по COVID-19, призванное помочь предприятиям обеспечить свою безопасность при адаптации к пандемии и охватывающее такие темы, как работа на дому и перевод деятельности предприятия в онлайновую среду.

Соединенное Королевство также представило подробную информацию о поддерживаемой правительством программе сертификации Cyber Essentials, которая направлена на то, чтобы предприятия могли защитить свои товары от кибератак без необходимости соблюдения многочисленных сложных стандартов. Cyber Essentials была разработана таким образом, чтобы участие в ней могли принимать все организации,

---

40 Документ SG2RGQ/215 ИК2 МСЭ-D, Бразилия.
41 Информация о кампании "Безопасное соединение", проводимой Anatel, размещена на веб-сайте по адресу: https://www.anatel.gov.br/consumidor/component/content/article/109-manchetes/960-conexaoseguro-confira-dicas-para-proteger-dados-pessoais.
42 Документ SG2RGQ/272 ИК2 МСЭ-D, Соединенное Королевство.

включая те, которые не обладают какими-либо начальными знаниями в области кибербезопасности или не имеют в своей структуре специальной кибергруппы.

2.4 Системы управления рисками в области кибербезопасности

Системы управления рисками в области кибербезопасности имеют жизненно важное значение как для правительственных, так и для неправительственных организаций. Такие системы, как правило, предусматривают добровольное участие и обеспечивают управление цифровыми рисками на основе руководящих указаний и примеров передового опыта. В течение исследовательского периода исследовательская комиссия получила вклады от организаций, в которых были представлены различные примеры систем управления рисками в области кибербезопасности и методы их внедрения.

Так, Национальный институт стандартов и технологий (NIST) Соединенных Штатов Америки недавно обновил свою Систему для укрепления кибербезопасности важнейшей инфраструктуры[43]. Данная система представляет собой направляемую бизнесом проактивную основу для добровольного управления киберрисками, которая предназначена для компаний всех размеров, работающих в различных секторах экономики. Она обеспечивает общую отправную точку и язык для оценки киберрисков. Система может легко адаптироваться, позволяя организациям, независимо от их размера, степени риска нарушения кибербезопасности или опыта в области кибербезопасности, применять принципы и передовой опыт управления рисками для укрепления безопасности и способности к восстановлению важнейшей инфраструктуры.

Система была разработана в результате успешного сотрудничества государственного и частного секторов в области управления рисками нарушения кибербезопасности, вклад в которое в течение года на добровольных началах внесли свыше 3000 заинтересованных сторон в лице предприятий, академических организаций, правительства и международных партнеров.

В основе системы лежат действующие международные стандарты и руководящие указания, а также передовой опыт предприятий, которые доказали свою эффективность с точки зрения защиты систем ИТ от киберугроз, обеспечения конфиденциальности коммерческой информации и защиты неприкосновенности частной жизни и гражданских свобод и которые направлены на содействие защите важнейшей инфраструктуры на основе управления рисками. Кроме того, данная система обеспечивает структуру для организации практической работы, а также инструменты, помогающие применять и внедрять стандарты и методы. Благодаря ссылкам на всемирно признанные стандарты кибербезопасности, система имеет универсальный характер и может служить в качестве международной модели управления киберрисками.

Принимая во внимание замечания и предложения заинтересованных сторон, NIST внес следующие обновления в версию 1.1 данной системы:

– заявление о применимости данной системы к "технологиям", включая, как минимум, информационные и операционные технологии, киберфизические системы и IoT;
– доработка руководящих указаний для обеспечения возможности применения системы к управлению рисками, связанными с деятельностью цепочек поставок;
– изложение в краткой форме информации об актуальности и пользе предусмотренных системой показателей для проведения организацией самооценки;
– предоставление дополнительной информации о проведении самооценки для выявления рисков в области кибербезопасности;
– усиление учета требований к авторизации, аутентификации, проверке идентичности и раскрытию информации об уязвимостях;
– предоставление административных обновлений к информационным ссылкам для отражения прогресса, достигнутого частными и государственными организациями с точки зрения соблюдения стандартов и руководящих указаний.

Кроме того, в Бутане Королевский орган регулирования денежного обращения (центральный банк) издал директиву, направленную на содействие внедрению системы кибербезопасности для финансовых

[43] Документ SG2RGQ/151 ИК2 МСЭ-D, Соединенные Штаты Америки.

учреждений в целях повышения устойчивости банковской системы к неизвестным и сложным киберрискам[44]. В данной директиве предусмотрены приведенные ниже положения.

– Все банки-участники должны стремиться соблюдать Отраслевой стандарт безопасности данных платежных карт, направленный на защиту среды данных о держателях карт. Кроме того, в дополнение к своим собственным мерам кибербезопасности банки должны внедрить стандарт ISO/IEC 27001:2013, касающийся систем управления информационной безопасностью.

– В директиве говорится о необходимости создания группы реагирования на киберинциденты в финансовых учреждениях для содействия активному сотрудничеству и эффективному обмену информацией по вопросам кибербезопасности между банками и Королевским органом регулирования денежного обращения. Группа будет активно отслеживать киберугрозы, планировать и координировать меры по противодействию им в целях предотвращения рисков для кибербезопасности и в кратчайшие сроки сообщать о всевозможных инцидентах соответствующему руководителю или органу. Недавно была сформирована кибергруппа для банков, ведущую роль в деятельности которой играет Королевский орган регулирования денежного обращения.

– Банки-участники должны также внедрить соответствующую систему контроля за обеспечением кибербезопасности и принять безотлагательные ответные меры по обеспечению базовой информационной безопасности.

В качестве отдельного примера можно привести создание в Китае индекса оценки национальных перспектив с точки зрения планирования, разработки и внедрения компонентов сетевой безопасности на основе трехуровневых показателей с возрастающей степенью сложности[45]. На первом уровне оцениваются пять показателей:

– политика: национальные стратегии, законодательство, государственные учреждения, международное сотрудничество;

– промышленность: развитие сектора обеспечения безопасности сетей в среде, определяемой рыночными факторами, включая условия развития, масштаб, конкурентоспособность предприятий и самодостаточность;

– технологии: уровень исследований, разработок и применения технологий в области обеспечения национальной безопасности, включая научно-исследовательские проекты, инвестиции, технические стандарты и подготовку персонала;

– потенциал: уровень защиты и предотвращения угроз безопасности сетей, включая восприятие рисков, защиту безопасности, меры реагирования в чрезвычайных ситуациях и активную защиту;

– ресурсы: ресурсы, необходимые для поддержки создания потенциала, включая ресурсы сетевой инфраструктуры, осведомленность в вопросах безопасности и международное влияние.

Индексом также предусмотрены 19 показателей второго уровня и 53 показателя третьего уровня. Согласно системе оценки индекса, каждый показатель оценивается по шкале от 0 до 1 балла; при этом количество баллов не должно превышать 53. Расчеты по каждому показателю основаны на официальной информации, находящейся в открытом доступе и опубликованной на национальных и международных веб-сайтах, а также научно-исследовательскими учреждениями.

2.5 Государственно-частное партнерство

Без посторонней помощи государственные органы не в состоянии улучшить положение дел в области национальной кибербезопасности. Для достижения успеха при осуществлении мер и проектов в области кибербезопасности необходимо выстроить прочные партнерские отношения между субъектами государственного и частного секторов.

Национальный институт стандартов и технологий Соединенных Штатов Америки разработал Систему для укрепления кибербезопасности важнейшей инфраструктуры на основе коллективных усилий в рамках государственно-частного партнерства[46]. Как было отмечено в более подробной форме в Разделе 2.4, институт обеспечил привлечение всех заинтересованных сторон к разработке обновленной версии, тем

[44] Документ SG2RGQ/135 ИК2 МСЭ-D, Бутан.
[45] Документ 2/155 ИК2 МСЭ-D, Китай.
[46] Документ SG2RGQ/151 ИК2 МСЭ-D, Соединенные Штаты Америки.

самым побудив их максимально придерживаться предусмотренных системой принципов. Благодаря тому, что заинтересованные стороны участвовали в разработке версии 1.1 системы и их предложения и замечания были учтены при этом, повысилась вероятность соблюдения и внедрения ими передовой практики, руководящих указаний и стандартов, содержащихся в ней.

В Республике Корея Министерство науки и информационно-коммуникационных технологий разработало Базовый план национальной кибербезопасности на 2019 год для частного сектора по результатам консультаций с соответствующими заинтересованными сторонами, включая академические организации, предприятия и общественные организации[47]. Планом было предусмотрено выполнение двух задач: обеспечение безопасности киберпространства и развитие отрасли информационной безопасности. Основные стратегические проекты в рамках этих усилий были направлены на расширение сети кибербезопасности, содействие развитию отрасли информационной безопасности и усиление инфраструктуры информационной безопасности.

Учитывая стремительно меняющуюся среду ИКТ, министерство намерено обновлять план на ежегодной основе. Кроме того, дважды в год проводятся заседания Консультационного совета государственного и частного секторов Республики Корея, на которых отслеживается ход выполнения плана и выявляются области, требующие улучшения.

Еще одним примером того, насколько важную роль государственно-частное партнерство (ГЧП) играет в разработке всеобъемлющих национальных стратегий кибербезопасности, как указано в Разделе 2.1, является национальная стратегия кибербезопасности Бразилии E-Ciber. ГЧП выделено особое место среди ключевых стратегических направлений, предусмотренных E-Ciber. Среди них – содействие созданию условий для сотрудничества, широкого участия, обеспечения безопасности и формирования доверительных отношений между государственным и частным секторами и гражданским обществом, а также расширение партнерства в области кибербезопасности между ними, академическими организациями и гражданским обществом.

В качестве еще одного наглядного примера ГЧП Бразилия представила обзорную информацию о своем опыте проведения в 2018 году национальных тренировочных занятий по кибербезопасности, известных как учения "Киберстража", в рамках которых акцент был сделан на важнейшей национальной инфраструктуре[48]. В 2019 году Бразилия провела последующие учения, значительно расширив круг участников за счет включения в него представителей министерств обороны, юстиции и иностранных дел, Управления ведомственной безопасности, вооруженных сил, органов федеральных правительственных учреждений, таких как Anatel, национальных CSIRT, Центрального банка Бразилии, государственных и частных банков, компаний в области ядерной энергетики, электроэнергетики и электросвязи, научных работников и приглашенных региональных и международных наблюдателей.

Еще одним примером ГЧП являются группы CERT/CSIRT/CIRT. Благодаря им, государственные учреждения и частный сектор имеют возможность объединить усилия для урегулирования инцидентов, связанных с кибербезопасностью. В то же время для поддержания эффективности таких групп необходимы взаимодействие и доверительные отношения.

2.6 Меры/инициативы по усилению потенциала

2.6.1 Создание учебных заведений по вопросам кибербезопасности

Осознав, что для борьбы с растущими проблемами в области кибербезопасности необходимо инвестировать средства в подготовку кадров и образование в области кибербезопасности, многие правительства создали учебные учреждения для подготовки следующего поколения специалистов по вопросам кибербезопасности. Авторы нескольких вкладов, полученных от Государств – Членов МСЭ в рамках исследовательского периода, признали необходимость принятия соответствующих мер, в том числе путем укрепления отношений между государственными заинтересованными сторонами, университетами и научно-исследовательскими центрами.

Так, в 2015 году в Чаде была создана Национальная высшая школа информационных и коммуникационных технологий (ENASTIC), что стало наглядной демонстрацией наличия у высших органов власти страны

[47] Документ 2/168 ИК2 МСЭ-D, Республика Корея.
[48] Документ SG2RGQ/214 ИК2 МСЭ-D, Бразилия.

политической воли к созданию основы для обеспечения повышения квалификации в области ИКТ (в том числе путем предоставления степеней в области кибербезопасности, сетей, электросвязи и т. д.)[49].

Аналогичным образом, в Сенегале была создана ориентированная на региональный уровень Национальная школа кибербезопасности (ENC), цель которой заключается в наращивании потенциала и повышении уровня осведомленности лиц, ответственных за принятие решений, старших офицеров министерства обороны и других лиц, участвующих в функционировании цифровой экосистемы региона[50].

Перед школой стоят, в том числе, следующие ключевые задачи:

– подготовка и повышение уровня осведомленности государственных должностных лиц, сенегальских и иностранных сотрудников и студентов, а также лиц, работающих в государственном и частном секторах кибербезопасности, в целях улучшения понимания рисков и угроз;

– регулярное обучение специализированных сотрудников CERT/CSIRT, с тем чтобы помочь им реагировать на самые изощренные кибератаки;

– периодическая подготовка сотрудников государственных и субрегиональных учреждений, с тем чтобы предоставить им возможность и знания, необходимые для подготовки к инцидентам, защиты от них, реагирования на них и восстановления после них.

2.6.2 Прочие инициативы по созданию потенциала

В течение всего исследовательского периода координатор Бюро развития электросвязи (БРЭ) по вопросам кибербезопасности регулярно предоставлял обновленную информацию о программе работы БРЭ, в том числе о его различных инициативах в сфере создания потенциала. Взаимодействуя с различными организациями и лицами, БРЭ обеспечило подготовку кадров по вопросам создания потенциала в интересах развивающихся стран, включая проведение тренировочных занятий по кибербезопасности, оказание помощи в развитии CSIRT и проведение учебных занятий. Данные усилия были также отмечены во вкладах, предоставленных Государствами-Членами и Членами Секторов. Для ознакомления с дополнительной информацией см. **Приложение 1**.

[49] Документ 2/136 ИК2 МСЭ-D, Чад.
[50] Документ SG2RGQ/146 ИК2 МСЭ-D, Сенегал.

Глава 3 – Защита ребенка в онлайновой среде

3.1 Обзор

Современный интернет – это уже нечто большее, чем просто банк знаний, "огромная библиотека с беспорядочно сваленными материалами", как это было в эпоху Web 1.0. Она стала коммуникационной платформой, которой пользуются все, в том числе и дети. По данным Детского фонда Организации Объединенных Наций (ЮНИСЕФ), на долю детей приходится треть населения мира, пользующегося интернетом[51].

Характер онлайновых угроз, с которыми сталкиваются дети, изменился. Если раньше они были исключительно информационными, что предполагало, например, доступ к информации о наркотиках, порнографии или экстремистских движениях, то в настоящее время они также носят поведенческий характер, что предполагает, например, дессоциализацию, пристрастие к азартным играм, неконтролируемые расходы, виртуальное запугивание, разглашение персональных данных и опасные знакомства.

В течение последних 10 лет технологическое сообщество активно работает над поиском способов защиты детей от веб-сайтов, содержащих информацию неприемлемого характера, однако разработчики и родители теперь столкнулись с новой проблемой – как правильно познакомить юных пользователей с цифровым пространством и как оперативно контролировать и корректировать виртуальное поведение. Ввиду стремительного развития интернет-технологий проблема защиты детей, в необходимости решения которой в мире не возникает сомнений, естественно, охватила и киберпространство. Его безопасность имеет первостепенное значение, когда речь заходит о знакомстве детей с цифровыми устройствами и интернетом.

Декларация Буэнос-Айреса, принятая ВКРЭ-17, гласит, "*что возможности, предоставляемые электросвязью/ИКТ, следует использовать в полной мере, чтобы обеспечить справедливый доступ к электросвязи/ИКТ и инновациям, которые способствуют устойчивому социально-экономическому развитию, уменьшению масштабов нищеты, созданию рабочих мест, установлению гендерного равенства, защите ребенка в онлайновой среде, развитию предпринимательства, а также охвату цифровыми технологиями и расширению прав и возможностей для всех*"[52].

В Резолюции 179 (Пересм. Дубай, 2018 г.) Полномочной конференции (МСЭ) и Резолюции 67 (Пересм. Буэнос-Айрес, 2017 г.) ВКРЭ определена роль, которую МСЭ и МСЭ-D должны играть в обеспечении защиты ребенка в онлайновой среде.

Как показала пандемия COVID-19, модели поведения злоумышленников и преступных сетей постоянно эволюционируют; кроме того, преступники пользуются тем, что многие дети проводят намного больше времени в онлайновой среде, чем обычно. В связи с этим публикация Руководящих указаний по защите ребенка в онлайновой среде 2020 года, которые призваны обеспечить благополучие, неприкосновенность и безопасность детей, является своевременной[53].

Данные руководящие указания были разработаны МСЭ совместно с рабочей группой авторов из ведущих учреждений, занимающихся вопросами ИКТ, защиты ребенка (в онлайновой среде) и их правами. Это комплекс рекомендаций, предназначенный для всех соответствующих заинтересованных сторон и посвященный тому, как способствовать созданию безопасной онлайновой среды, расширяющей права и возможности детей и молодежи. Цель руководящих указаний – повысить уровень осведомленности о сфере защиты ребенка в онлайновой среде и предоставить ресурсы и инструменты, с помощью которых дети и их семьи могут развивать цифровые навыки, а предприятия и заинтересованные стороны из государственного сектора – разработать корпоративную и национальную политику и стратегию защиты ребенка в онлайновой среде. Предназначенные для детей, родителей, педагогов, представителей предприятий и лиц, ответственных за разработку политики, данные руководящие указания призваны стать образцом для подражания, который можно адаптировать к обычаям и законам национального или местного значения.

---

51 ЮНИСЕФ, Положение детей в мире, 2017 год, декабрь 2017 г.

52 Всемирная конференция по развитию электросвязи (Буэнос-Айрес, 2017 г.), Декларация Буэнос-Айреса.

53 МСЭ, Руководящие указания по защите ребенка в онлайновой среде.

Согласно Стратегическому плану МСЭ, изложенному в Резолюции 71 (Пересм. Дубай, 2018 г.) Полномочной конференции МСЭ, одна из задач МСЭ-D заключается в том, чтобы "*содействовать развитию и использованию электросвязи/ИКТ и приложений с целью расширения возможностей людей и общества для устойчивого развития" (п. D.4). В частности, МСЭ-D должен предоставить "продукты и услуги по охвату девушек и женщин и лиц с особыми потребностями (включая пожилых людей, молодежь, детей и коренные народы) цифровыми технологиями, такими как повышение информированности о стратегиях, политике и практике охвата цифровыми услугами, развитие цифровых навыков, комплекты материалов и руководящие указания, а также дискуссионные форумы для обмена опытом и совместного использования стратегий*", в том числе, в целях защиты ребенка в онлайновой среде (п. D.4-3).

Меры, предпринимаемые МСЭ-D и его членами для защиты ребенка в онлайновой среде, изложены в пункте d) Раздела 2 круга ведения по Вопросу 3/2:

d) продолжать собирать примеры национального опыта, относящегося к кибербезопасности и защите ребенка в онлайновой среде, в Государствах-Членах, а также выявлять и изучать общие темы в рамках этого опыта, готовя на основе этой информации материалы для руководящих указаний, которые помогут Государствам-Членам в разработке эффективных механизмов обеспечения безопасности в цифровой среде.

3.2 Примеры передового опыта и общие тенденции Государств – Членов МСЭ

В рамках исследовательского цикла основные мероприятия по защите ребенка в онлайновой среде, проведенные Государствами-Членами, были направлены на повышение уровня осведомленности, разработку норм регулирования и проведение тематических обследований.

Повышение осведомленности

Защита ребенка в киберпространстве имеет множество аспектов и предусматривает обязательное наличие не только инструментов и платформы, но и соответствующих данных. Для распространения таких ресурсов в обществе необходимо задействовать культурные программы.

Так, Иранская организация по информационным технологиям разработала проект "Дети и интернет" (KOVA), направленный на защиту детей в киберпространстве, который стал одним из победителей конкурса на соискание наград Всемирной встречи на высшем уровне по вопросам информационного общества в 2018 году.

Ввиду стремительного развития инфраструктуры интернета в последние годы и большого количества юных пользователей интернета, включая детей, в 2016 году иранское правительство приступило к реализации национальной программы по защите детей в интернете. В рамках программы Министерство ИКТ запустило проект KOVA, направленный на повышение уровня осведомленности детей и их родителей о рисках, связанных с интернетом, и способах защиты детей от них. Основные цели проекта заключаются в следующем:

- выявлять наиболее значимые угрозы для детей в киберпространстве, предлагать связанные с ними решения и услуги правовой защиты от них;
- повышать осведомленность учащихся начальной и старшей школы, а также учителей и родителей о различных угрозах, которым подвергаются дети в разном возрасте;
- помогать детям и подросткам обеспечить свою безопасность и защиту при использовании социальных сетей и интернета;
- отвечать на вопросы детей, подростков, педагогов и родителей о проблемах обеспечения безопасности и защиты в киберпространстве.

В рамках достижения предусмотренных проектом целей были использованы различные инструменты и методы (такие как театральные постановки, фильмы и анимация) для обучения детей обеспечению безопасности в онлайновой среде. На первом этапе реализации проекта обучение прошли свыше 200 000 учащихся 900 школ; на втором этапе планируется охватить 4000 школ[54].

[54] Документ 2/82 ИК2 МСЭ-D, Иранский научно-технологический университет (Исламская Республика Иран).

В Бутане за период начиная с 2016 года число пользователей интернета увеличилось более чем на 28% в результате облегчения доступа, повышения степени приемлемости установления соединений в ценовом отношении и увеличения доступности более дешевых смартфонов. Большинство школьников имеют доступ к смартфонам, что повышает риск возникновения инцидентов, связанных с безопасностью. В Бутане пока нет школьной программы по кибербезопасности, поскольку тенденция к увеличению использования интернета и мобильных устройств наблюдается лишь в последнее время. Тем не менее крайне необходимо, чтобы государственные органы включили вопрос обеспечения кибербезопасности в школьную программу, чтобы адаптироваться к изменениям времени. Частные колледжи Бутана уже рассматривают различные варианты внедрения соответствующих образовательных программ, особенно в области кибербезопасности. Школьники должны знать о таких рисках, поскольку они более подвержены фишинговым атакам и атакам в рамках онлайновых игр[55].

С учетом этих соображений, изучая привычки и поведение детей в онлайновой среде, Бутан разрабатывает анимационные видеоматериалы на такие темы, как торговля детьми, киберзапугивание, конфиденциальность и безопасность онлайновых игр, которые будут транслироваться по национальному телевидению. Кроме того, разрабатываются предназначенные для учащихся плакаты и брошюры, содержащие информацию о передовом опыте в области кибербезопасности, которые будут распространены для использования в школах страны. Для разработки соответствующих руководящих указаний по защите ребенка в онлайновой среде Бутан создает целевую группу национального уровня, в состав которой войдут представители различных заинтересованных сторон[56].

В Китае на общенациональном уровне проводится ежегодная неделя популяризации идеи обеспечения безопасности сетей, направленная на повышение уровня осведомленности населения в целом о кибербезопасности и его навыков защиты в онлайновой среде путем организации экспозиций, форумов, конкурсов, лекций, тематических дней и других мероприятий. В частности, проводятся лекции по сетевой безопасности для обмена знаниями и навыками в соответствии с потребностями различных групп, таких как учащиеся начальной и средней школы, престарелые лица и лица с особыми потребностями (например, лица с ограниченными возможностями), в зависимости от уровня их навыков в области информационных технологий[57].

В Соединенных Штатах родителям и преподавателям предоставляется информация о методах взаимодействия с детьми и подростками, в том числе о разъяснении следующих принципов: "То, что ты публикуешь в Сети может остаться там на всю жизнь!", "Отдавай себе отчет в том, какую информацию ты выкладываешь в Сеть!", "Следи за тем, чтобы не выложить в Сеть слишком много информации о себе!", "Публикуй в Сети о других только то, что тебе хотелось бы, чтобы они публиковали о тебе!", "Управляй своим присутствием в Сети, ограничивая круг тех, кто может видеть информацию и обмениваться информацией!", "Знай, какие данные собираются!"[58].

Регулирование

Учитывая широкую доступность информационных технологий, правительства принимают серьезные нормативные меры для обеспечения безопасности всех граждан, имеющих доступ к интернету, особенно несовершеннолетних. Хотя законодательство в области кибербезопасности несколько отличается в разных странах мира, факторы, лежащие в основе существующей проблемы, остаются неизменными.

Одной из основных причин появления соответствующих нормативных актов является особая уязвимость детей дошкольного и младшего школьного возраста в онлайновой среде, которые легко становятся жертвами интернет-хищников (лиц, совершающих сексуальные домогательства в отношении несовершеннолетних в интернете), унижений и онлайнового груминга (когда незнакомец завоевывает доверие ребенка в собственных целях), а также неправомерного использования персональных данных.

Постепенно дети превратились в группу населения, подвергающуюся наибольшему риску разглашения информации о частной жизни и кражи идентичности. Поэтому вопрос о необходимости защиты персональных данных детей стоит крайне остро.

---

55 Документ SG2RGQ/79 ИК2 МСЭ-D, Бутан.
56 Документ 2/385 ИК2 МСЭ-D, Бутан.
57 Документ 2/286 ИК2 МСЭ-D, Китай.
58 Документ 2/400 ИК2 МСЭ-D, Соединенные Штаты Америки.

В Китае, например, принято специальное положение о киберзащите персональных данных детей, которым регулируется весь цикл сбора, хранения, использования, передачи и раскрытия персональных данных детей[59]. Положение предусматривает специальные меры защиты, четкие принципы и совместное управление с целью создания благоприятной онлайновой среды для здорового развития детей. Специальные меры защиты включают, среди прочего, права на удаление и неразглашение персональных данных детей; при этом принципы охватывают вопросы законной необходимости, информированного согласия, четкой цели, безопасности и законного использования. Данное положение применяется, прежде всего, для защиты персональных данных детей в возрасте до 14 лет.

В декабре 2010 года Российской Федерацией был принят закон о защите детей от информации, причиняющей вред их здоровью и развитию, который гарантирует информационную безопасность несовершеннолетних и устанавливает условия и порядок распространения информации среди детей[60].

Кроме того, положениями Закона о СМИ Российской Федерации запрещается распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях (таких как интернет) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая:

- фамилию, имя, отчество;
- фото- и видеоизображение такого несовершеннолетнего, его (ее) родителей и иных законных представителей;
- дату рождения такого несовершеннолетнего;
- аудиозапись его (ее) голоса;
- место его (ее) жительства или место временного пребывания;
- место его (ее) учебы или работы;
- иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего[61].

Тематические обследования

МСЭ оказал техническую помощь Бутану в рамках продолжающейся разработки национальной стратегии кибербезопасности[62]. В ходе этого процесса было проведено обследование среди 126 учащихся (средний возраст которых составил 16 лет) для оценки использования интернета, инцидентов, связанных с безопасностью, таких как киберзапугивание, и распространенности компьютерных вирусов или правонарушений, совершаемых учащимися; при этом использовались вопросы с несколькими вариантами ответов.

Обследование показало, что учащиеся активно пользуются интернетом. Почти все учащиеся, принявшие участие в обследовании, пользовались интернетом, а свыше 40% делали это свыше двух часов в день. Проблема обеспечения кибербезопасности оказалась острой для учащихся: несмотря на то, что почти 40% из них столкнулись с заражением вредоносными программными средствами, лишь около 10% сообщили об использовании антивирусных программ.

Что касается осведомленности в вопросах кибербезопасности, школа остается важным источником знаний для учащихся. Почти 40% учащихся сообщили, что они узнали о кибербезопасности в школе.

Учащиеся также подвергались киберпреступлениям и другим видам вредоносной деятельности. Помимо компьютерных вирусов, свыше 10% опрошенных учащихся стали жертвами киберзапугивания, а 25% сказали, что в онлайновой среде с ними контактировало незнакомое лицо. Кроме того, согласно одному из разделов вопросника, посвященного незаконным или ненадлежащим действиям, около 35% учащихся посылали злонамеренные или вредоносные сообщения, которые можно было бы считать киберзапугиванием. Примерно столько же учащихся пытались взломать или взломали защищенную беспроводную сеть.

---

59 Документ SG2RGQ/179 ИК2 МСЭ-D, Китай.
60 Документ 2/264 ИК2 МСЭ-D, Российская Федерация.
61 См. Статью 4 Федерального закона № 2124, https://digital.gov.ru/ru/documents/6406/ (на русском языке); Документ 2/264 ИК2 МСЭ-D, Российская Федерация.
62 Документ SG2RGQ/135 ИК2 МСЭ-D, Бутан.

Вследствие того, что первоначальное обследование было ограниченным, Бутан провел еще одно обследование по безопасности и защите ребенка в онлайновой среде на национальном уровне. Обследование проводилось в рамках проекта "Цифровые дети Азиатско-Тихоокеанского региона" (DKAP), инициированного Бюро Организации Объединенных Наций по вопросам образования, науки и культуры ЮНЕСКО в Бангкоке (ЮНЕСКО Бангкок) при поддержке Корейского целевого фонда (KFIT). Обследование охватило 2381 учащегося в возрасте от 12 до 17 лет из 45 школ по всей стране, которым было задано 112 вопросов, для того чтобы определить уровень осведомленности о кибербезопасности, угрозы, а также профилактические меры. По данным обследования, большинство студентов (81%) имеют доступ к смартфонам дома. Большая часть студентов, как правило, проводит в интернете в среднем 1–2 часа в день. Помимо этого, 54% студентов не знают, как отделить достоверную информацию от недостоверной. Около 49% учащихся опасаются, что кто-то злоупотребляет их личными данными.

Небольшая доля учащихся (10%) обходят ограничения по возрасту, давая ложную информацию, участвуют в травле других людей и входят в чужие учетные записи. Кроме того, 85% учащихся готовы заводить новых друзей в интернете, а 68% не против общения с людьми из других мест или из других кругов общения. Обследование вызвало обеспокоенность в связи с тем фактом, что 51% студентов встречались с незнакомыми людьми, с которыми познакомились онлайн, а также что 22,8% студентов готовы рассматривать возможность встречи с незнакомыми людьми, при этом доля учащихся женского пола среди тех, кто встречается с незнакомыми людьми, выше чем доля учащихся мужского поля[63].

В Кот-д'Ивуаре PLCC провела обследование среди 200 молодых людей из трех средних школ Абиджана, с тем чтобы проанализировать поведение детей в онлайновой среде, выявить риски и предложить эффективные способы обеспечения безопасности для борьбы со злоупотреблениями в онлайновой среде[64].

В общей сложности 83% респондентов обследования сообщили об использовании интернета. Основная причина, по которой оставшиеся респонденты не пользовались интернетом, заключалась в стоимости смартфонов и терминалов. Среди детей в возрасте 15–18 лет телевидение оказалось на втором месте по уровню использования, а 86,3% детей имели учетную запись в социальных сетях. Предпочитаемым средством доступа в интернет среди представителей данной возрастной группы оказались смартфоны. Изображения и фильмы со сценами насилия были названы в качестве основного источника негативного опыта в онлайновой среде; затем идут пиратство и, наконец, оскорбления и угрозы. В меньшей степени респонденты сообщали о негативном опыте с сексуальной коннотацией. По словам ряда респондентов, их шантажировали с помощью видеоматериалов откровенно сексуального характера.

Потенциально наиболее пагубным опытом, с которым столкнулись дети, согласно результатам обследования, были:

- вирусы, ошибки, спам или хакерство (24%);
- видеоматериалы сексуального характера (7,5%);
- изображения или видеоматериалы со сценами насилия (28,6%);
- использование фотографий без предварительного согласования (7,5%);
- оскорбления, злонамеренные действия или угрозы (19,5%);
- кража идентичности (6,7%);
- контакт с незнакомцем (4,51%);
- мошенничество (0,75%);
- шантаж (0,75%).

Поддержка, оказываемая МСЭ Государствам-Членам в области защиты ребенка в онлайновой среде

В период с 4 по 6 апреля 2018 года в Одессе, Украина, в сотрудничестве с Одесской национальной академией связи им. А.С. Попова МСЭ провел региональный семинар-практикум для стран Европы и Содружества

[63] Документ 2/385 ИК2 МСЭ-D, Бутан.
[64] Документ 2/201 ИК2 МСЭ-D, Кот-д'Ивуар.

Независимых Государств (СНГ) по вопросам кибербезопасности и защиты ребенка в онлайновой среде[65]. Окончательные варианты всех документов (включая повестку дня, доклады, выводы и рекомендации, список участников, презентации и фотографии) были опубликованы на веб-сайтах академии[66] и МСЭ[67]. Участники семинара, представлявшие 14 Государств-Членов, пришли к выводу, что странам Европы и СНГ необходимо расширять сотрудничество в целях оптимизации использования имеющихся ресурсов и достижения практических результатов, в том числе путем перевода учебных материалов по вопросам кибербезопасности и защиты ребенка в онлайновой среде. Выводы и рекомендации, разработанные участниками семинара-практикума, представлены в итоговом документе[68].

Защита ребенка в онлайновой среде – это одно из ключевых направлений региональной инициативы МСЭ для стран Европы по укреплению доверия и обеспечению безопасности при использовании электросвязи/ИКТ. В ответ на обращения членов с просьбой разработать дорожные карты реализации инициатив по защите ребенка в онлайновой среде МСЭ провел обследование среди правительств стран, охваченных региональной инициативой, с тем чтобы рассмотреть широкий круг вопросов, связанных с существующей политикой и практикой использования детьми и молодыми людьми всевозможных технологических платформ в цифровом пространстве. Обследование было проведено впервые в 2009 году и охватило все Государства-Члены, а в 2016 году его пересмотренная версия была реализована среди Государств-Членов из Центральной и Восточной Европы, Балтии и Балканского региона.

На основе ответов, полученных в ходе обследования, в 2017 году БРЭ опубликовало региональный обзор национальных мероприятий по защите ребенка в онлайновой среде в Европе, показав, на каком этапе находятся страны-участницы с точки зрения разработки, принятия, осуществления и мониторинга политики в отношении защиты ребенка в онлайновой среде[69]. В нем также были приведены примеры существующей практики в Албании, Болгарии, Боснии и Герцеговине, Венгрии, Греции, Кипре, Латвии, Литве, Лихтенштейне, Северной Македонии, Монако, Польше, Словакии, Румынии, Сербии, Словении, Турции, Финляндии, Хорватии, Черногории, Чешской Республике и Эстонии.

Рабочая группа Совета МСЭ по защите ребенка в онлайновой среде (РГС-СОР) осуществляет свою деятельность в соответствии с Резолюцией 1306 Совета МСЭ (2009 г.), а также Резолюцией 179 (Пересм. Дубай, 2018 г.), в которой Полномочная конференция постановила, что МСЭ в сотрудничестве с компетентными заинтересованными сторонами необходимо продолжить реализацию инициативы по защите ребенка в онлайновой среде, используя ее как платформу для повышения уровня осведомленности о проблемах обеспечения безопасности ребенка в онлайновой среде, продолжить оказывать помощь и поддержку Государствам-Членам, особенно развивающимся странам, в разработке и осуществлении дорожных карт реализации данной инициативы, а также продолжить координировать осуществление этой инициативы[70].

Для целях рассмотрения Вопроса 3/2 была предоставлена информация о 15-м, 16-м и 17-м собраниях РГС-СОР, состоявшихся 26 сентября 2019 года, 4 февраля 2020 года и 26 января 2021 года, соответственно, в Женеве и дистанционно[71],[72].

Следующие документы были представлены в ходе собраний:

– обновленная информация по Руководящим указаниям МСЭ по защите ребенка в онлайновой среде[73];

– презентация на тему "Результаты онлайновых консультаций с участием молодежи"[74];

---

65 Документ 2/75 ИК2 МСЭ-D, Одесская национальная академия связи им. А.С. Попова (Украина).

66 Одесская национальная академия связи им. А.С. Попова, Региональный семинар-практикум для стран СНГ и Европы "Кибербезопасность и защита ребенка в онлайновой среде", Одесса, Украина, 4–6 апреля 2018 года.

67 МСЭ, Региональный семинар-практикум для стран СНГ и Европы "Кибербезопасность и защита ребенка в онлайновой среде", Одесса, Украина, 4–6 апреля 2018 года.

68 МСЭ, Выводы и рекомендации, Региональный семинар-практикум МСЭ для стран Европы и СНГ по вопросам кибербезопасности и защиты ребенка в онлайновой среде, Одесса, Украина, 4–6 апреля 2018 года.

69 МСЭ-D, Региональный обзор национальных мероприятий по защите ребенка в онлайновой среде в Европе, 2017 год.

70 Полномочная конференция МСЭ, Резолюция 179 (Пересм. Дубай, 2018 г.) "Роль МСЭ в защите ребенка в онлайновой среде".

71 Документ SG2RGQ/242 ИК2 МСЭ-D, Рабочая группа Совета по защите ребенка в онлайновой среде (РГС-СОР).

72 Вклады, полученные от членов и внешних экспертов, доступны по следующим ссылкам: 15-е собрание, 16-е собрание, 17-е собрание.

73 РГС-СОР МСЭ, Документ CWG-COP-14/2 "Обновленная информация об инициативе МСЭ по защите ребенка в онлайновой среде (СОР)".

74 РГС-СОР МСЭ, Документ CWG-COP-15/INF/3 "Онлайновые консультации с участием молодежи".

- презентация на тему "Работа и деятельность МСЭ в области защиты ребенка в онлайновой среде"[75];
- презентация на тему "Процесс рассмотрения Руководящих указаний по СОР 2019–2020 годов"[76];
- презентация на тему "Инициатива МСЭ по защите ребенка в онлайновой среде и внедрение Руководящих указаний по СОР 2019–2020 годов"[77];

Одним из основных результатов собраний стало признание необходимости выработки рекомендаций по увеличению числа ответов со стороны молодых людей, а также по активизации и расширению участия заинтересованных сторон в работе РГС-СОР, учитывая важность оценки эффективности программ.

В 2020 году МСЭ провел серию тематических форумов[78] для обмена опытом в области защиты ребенка в онлайновой среде между различными заинтересованными сторонами, а также для популяризации Руководящих принципов по защите ребенка в онлайновой среде и содействия их популяризации, адаптации и контекстуализации на национальном и региональном уровнях:

- Африка: 30 октября 2020 года[79];
- Северная и Южная Америка: 19 октября 2020 года[80];
- Арабские государства: 23 ноября 2020 года[81];
- Азиатско-Тихоокеанский регион: 3 ноября 2020 года[82];
- Содружество Независимых Государств: 27 октября 2020 года[83];
- Европа: 26–27 ноября 2020 года[84].

3.3 Извлеченные уроки, дальнейшие шаги, действия и выводы

Необходимость обеспечить защиту ребенка в онлайновой среде стала особенно острой во время пандемии COVID-19.

На основе деятельности Государств-Членов можно извлечь ряд уроков, касающихся вопросов защиты ребенка в онлайновой среде. В частности:

- каждая страна должна признать свою ответственность за обеспечение безопасности интернета и связанных с ним технологий для детей и молодых людей;
- страны все чаще включают вопрос повышения осведомленности об онлайновых рисках в повестку дня по защите и воспитанию детей в целом;
- несмотря на укореняющееся мнение о том, что интернет может, в том числе, способствовать формированию гражданской ответственности и получению новых знаний, во многих случаях нехватка ресурсов и опыта на местном уровне, по-видимому, тормозит дальнейшее развитие в данном направлении;
- во многих странах законодательная база в целом соответствует международным и региональным правовым документам, однако чрезвычайно важно, чтобы в каждой стране правовые меры и законодательство отвечали технологическому прогрессу и изменению поведения;

---

75 РГС-СОР МСЭ, Документ CWG-COP-16/5 "Работа и деятельность МСЭ в области защиты ребенка в онлайновой среде".
76 РГС-СОР МСЭ, Документ CWG-COP-16/4 "Инициатива МСЭ по защите ребенка в онлайновой среде: процесс рассмотрения Руководящих указаний по СОР 2019–2020 годов".
77 РГС-СОР МСЭ, Документ CWG-COP-17/2(Rev.1) "СОР МСЭ, 2020 год, защита и расширение прав и возможностей ребенка в онлайновой среде".
78 МСЭ, Региональные выпуски: Руководящие указания по СОР 2020 года.
79 МСЭ-D, Региональный выпуск пересмотренных руководящих указаний по СОР для Африки, 30 октября 2020 года.
80 МСЭ-D, Руководящие указания по СОР для Северной и Южной Америки, 19 октября 2020 года.
81 МСЭ-D, Онлайновый региональный диалог "Руководящие указания МСЭ по СОР 2020 года и возможности для реализации в Арабском регионе", 23 ноября 2020 года.
82 МСЭ-D, Региональный форум МСЭ по вопросам развития для стран Азиатско-Тихоокеанского региона (РФР-АТР). Сессия по кибербезопасности после форума – выпуск Руководящих указаний по защите ребенка в онлайновой среде 2020 года для Азиатско-Тихоокеанского региона, 3 ноября 2020 года.
83 МСЭ-D, Форум МСЭ – ИИТО ЮНЕСКО по защите ребенка в онлайновой среде для Региона СНГ, 27 октября 2020 года.
84 МСЭ-D, Форум МСЭ по защите ребенка в онлайновой среде для Региона Европы, 26–27 ноября 2020 года.

– поскольку национальные координационные центры являются одним из ключевых элементов эффективной защиты в онлайновой среде, каждая страна должна располагать таким центром для участия в региональных и международных инициативах, обеспечив его необходимыми ресурсами в полном объеме[85].

Существует также ряд областей, в которых Государства-Члены могли бы активизировать усилия по содействию защите ребенка в онлайновой среде, в частности путем:

– повышения информированности и обучения цифровой грамотности как специалистов по кибербезопасности, так и детей, родителей и учителей;

– разработки законов и нормативных актов, направленных на защиту ребенка в онлайновой среде;

– проведения репрезентативных обследований для повышения степени учета соответствующих потребностей при внедрении существующей политики, инициатив и мер, направленных на защиту ребенка в онлайновой среде.

Некоммерческие и общественные организации могут предпринять меры для повышения уровня осведомленности и развития навыков у детей, с тем чтобы помочь им повысить эффективность безопасного использования интернета, в том числе путем:

– предотвращение драматизации, которая в противном случае будет может способствовать чувству страха у родителей в отношении использования интернета их детьми, тем самым избегая подхода, способного усилить тревогу родителей, и без того обеспокоенных технологией, которую они плохо понимают, что заставляет их саботировать использование нетрадиционного инструмента для обучения, каковым является интернет;

– популяризации учебных программ, способствующих развитию передовых методов управления контентом, а также повышения уровня осведомленности детей о том, как ответственно пользоваться интернетом;

– создания интернет-портала в качестве образовательной базы для детей, подростков, родителей и учителей;

– привлечения всех заинтересованных сторон, включая государственные учреждения, частный интернет-сектор, неправительственные организации, местные группы и представителей население в целом, к повышению осведомленности на местном уровне[86].

В целом можно сделать вывод, что:

– международное сотрудничество и государственная поддержка играют ключевую роль в обеспечении кибербезопасности и защиты ребенка в онлайновой среде;

– для разработки стратегий кибербезопасности развивающимся странам следует использовать инструменты национальной политики;

– государственно-частные партнерства имеют важное значение для повышения эффективности организационных и технических средств обеспечения кибербезопасности;

– разработка новых стратегических и регуляторных механизмов для защиты ребенка в онлайновой среде и оценка существующих механизмов достигли своего пика;

– необходимо привлечь учебные учреждения и частные компании к реализации проектов по созданию организационно-технических средств для защиты ребенка в онлайновой среде, в том числе в рамках региональных инициатив МСЭ;

– необходимо разработать учебные программы и инструменты для защиты ребенка в онлайновой среде, которые учитывали бы потребности детей с ограниченными возможностями;

– Государствам-Членам следует проанализировать выполнение своих обязательств на основе Глобального индекса кибербезопасности (GCI) и приступить к принятию дальнейших мер;

– необходимо привлечь учебные заведения, субъекты частного сектора и неправительственные организации к деятельности МСЭ-D, в том числе к работе исследовательских комиссий МСЭ и

---

[85] Документ SG2RGQ/47 ИК2 МСЭ-D, Координатор БРЭ по Вопросу 3/2.
[86] Документ 2/201 ИК2 МСЭ-D, Кот-д'Ивуар.

центров профессионального мастерства, которые организовывают учебные курсы по вопросам кибербезопасности.

Для разработки более эффективных решений крайне важно обеспечить обмен информацией между всеми заинтересованными сторонами об имеющихся инструментах в области кибербезопасности и защиты ребенка в онлайновой среде ввиду ее растущего значения во всем мире и необходимости объединения усилий в этом направлении, особенно в рамках деятельности МСЭ-D[87].

[87] Документ 2/75 ИК2 МСЭ-D, Одесская национальная академия связи им. А.С. Попова (Украина).

Глава 4 – Проблемы в области кибербезопасности, с которыми сталкиваются лица с ограниченными возможностями

4.1 Введение

Для тех, кто совершает кибератаки, табу не существует. Нельзя допускать, чтобы люди с ограниченными возможностями были подвержены повышенному киберриску лишь по той причине, что они не располагают информацией или не осведомлены по тому или иному вопросу.

В рамках исследовательского периода 2014–2017 годов 2-я Исследовательская комиссия МСЭ-D провела обследование по вопросам осведомленности о кибербезопасности, результаты которого были опубликованы в заключительном отчете[88]. Полученные данные свидетельствуют о том, что пожилые лица и лица с ограниченными возможностями в наименьшей степени охвачены кампаниями по повышению осведомленности о кибербезопасности. Кроме того, 69% Государств-Членов, принявших участие в обследовании, не включили лиц с ограниченными возможностями в свои целевые группы по повышению осведомленности о кибербезопасности.

Результаты однозначно показывают, что в данном направлении необходимо предпринять дополнительные усилия. Для повышения уровня осведомленности об особых потребностях лиц с ограниченными возможностями и других заинтересованных сторон, включая правительства и частные организации, в области кибербезопасности Группа Докладчика по Вопросу 3/2 продолжила изучение специфических факторов безопасности и киберуязвимостей на основе сценариев использования. Сценарии использования, извлеченные уроки и другие полезные сведения приведены в настоящей главе.

4.2 Сценарии использования

4.2.1 Спамеры и фишеры, выбирающие в качестве своих мишеней лиц с ограниченными возможностями

Обзор

Действия спамеров и "угонщиков", захватывающих адреса электронной почты, приобретают все более изощренный характер, так как мошенники научились определять, есть ли у потенциальной жертвы инвалидность, с тем чтобы выдать себя за жертву. Кроме того, лица с ограниченными возможностями сталкиваются с трудностями при обращении за помощью в отдел безопасности или отдел борьбы с мошенничеством организаций, предоставляющих им услуги электронной почты.

Они становятся мишенью для спамеров и "угонщиков", которые выдают себя за жертву, используя инвалидность человека в качестве опознавательной характеристики. В одном из случаев был взломан адрес электронной почты глухого человека, использовавшего язык жестов. Учетная запись жертвы принадлежала Gmail, однако она могла принадлежать и любому другому поставщику услуг электронной почты. К сожалению, служба поддержки Gmail не оказала практически никакой помощи. После того как жертва нажала на фишинговую ссылку и ее учетная запись была взломана, спамер смог получить доступ к адресной книге жертвы и, возможно, к другим файлам на ее компьютере.

В службе поддержки жертве сказали, что единственное решение – это сменить поставщика услуг электронной почты и адрес электронной почты. В данном примере инвалидность заключалась в глухоте, однако не исключено, что для данного вида кражи идентичности может быть использована любая другая форма инвалидности.

Пользователям электронной почты, включая лиц с ограниченными возможностями, необходимо осознать, что перед тем как нажать на полученную ссылку, они должны проверить ее, даже если они получили ее

[88] МСЭ, Заключительный отчет по Вопросу 3/2 2-й Исследовательской комиссии МСЭ-D в исследовательском периоде 2014–2017 годов, Защищенность сетей информации и связи: передовой опыт по созданию культуры кибербезопасности, МСЭ, 2017 год.

от друзей. Служба поддержки поставщиков услуг электронной почты также должна проявлять активный интерес к данной форме злоупотреблений, особенно когда жертвами становятся представители уязвимых групп населения. В приведенном примере жертва связалась со службой поддержки по телефону через друга или через службу ретрансляции по телефону для глухих лиц; поставщики услуг должны серьезнее относиться к таким обращениям или предоставлять специальный номер телефона людей, с которыми глухие пользователи могут напрямую связаться с помощью телетайпа. Еще лучше, если поставщики услуг наймут персонал службы поддержки, который свободно владеет языком жестов. В Соединенных Штатах Америки, например, Amazon предприняла шаги для предоставления такой услуги.

Примеры сообщений электронной почты

Ниже приведены два примера сообщений электронной почты, которые спамер в указанном выше случае отправил адресатам в списке контактов жертвы. В результате жертва сменила поставщика услуг электронной почты, сообщив о взломе лицам в своем списке контактов.

Пример 1: спамер выдает себя за человека с ограниченными возможностями.

От: Лицо с ограниченными возможностями: лицосограниченнымивозможностями@gmail.com

Отправлено: 23 марта 2018 г. 13:00

Тема: УХ ТЫ!!! В стране X РАЗМЕР ЕЖЕМЕСЯЧНОГО ПОСОБИЯ ДЛЯ ГЛУХИХ УВЕЛИЧЕН НА 70%

Ух ты!!! Страна X побеспокоилась обо всех глухих и слабослышащих людях, и Лидер страны X решил увеличить размер пособия по социальному страхованию, дополнительного гарантированного дохода и социального пособия по нетрудоспособности на 70%, и это Хорошая Новость для всех глухих и слабослышащих в стране X.

Чтобы ознакомиться с дополнительной информацией и узнать, насколько увеличился размер Вашего пособия по социальному страхованию, дополнительного гарантированного дохода и социального пособия по нетрудоспособности,

перейдите по ссылке: http://noisecancel.net/js/gggg/G/G/us/index.php

[Примечание: первоначальная фишинговая ссылка была изменена.]

И осуществите Вход в систему, используя адрес своей Электронной почты, а также убедитесь, что все правильно

Новости для глухих

Пример 2: от жертвы, сообщившей своим знакомым, что его почту взломали.

Всем привет!

Как я уже говорил ранее, в результате того, что три недели назад меня втянули в просмотр видео на АЯЖ, мою СТАРУЮ почту взломали!

[Примечание: АЯЖ – американский язык жестов.]

Хакер продолжает отправлять ФЕЙКОВЫЕ сообщения, используя мою учетную запись gmail. Что пугает, так это то, что их содержание кажется настоящим и связанным с моей деятельностью как глухого человека.

Потратив нескольких часов на поиски в роботизированной сети Google, я нашел номер телефона человека, с которым можно связаться: (855) 836-3987.

И знаете, что? Вместо того, чтобы попытаться помочь мне, они сказали: "очень плохо".

С Вашей учетной записью в Gmail все хорошо?

А пока удалите ВСЕ сообщения электронной почты.

<от лицасограниченнымивозможностями@gmail.com>

Приношу свои извинения,

Лицо с ограниченными возможностями

Извлеченные уроки и предлагаемые примеры передовой практики

- Сообщество лиц с ограниченными возможностями необходимо проинформировать об известных проблемах в области спама и вредоносных программных средств.
- Поставщикам услуг необходимо обеспечить наличие подготовленного персонала для обработки обращений клиентов-представителей сообщества лиц с ограниченными возможностями.
- Пользователям услуг электронной почты не следует нажимать на какие-либо веб-адреса, если источник не был проверен.
- Жертвам взлома электронной почты следует:
  - проинформировать своего поставщика услуг электронной почты;
  - переслать подозрительное сообщение электронной почты в отдел по борьбе с мошенничеством поставщика услуг электронной почты;
  - потребовать, чтобы взломанный адрес электронной почты был заблокирован;
  - изменить адрес электронной почты;
  - сообщить всем лицам в списке контактов, что адрес электронной почты был взломан, и предоставить им новый адрес.

4.2.2 Киберриски, связанные с ассистивными технологиями на основе IoT

Базовая информация

По данным Всемирной организации здравоохранения (ВОЗ), более 2 миллиардов человек имеют инвалидность, что составляет 37,5% от общей численности населения мира[89]. Как отмечает Департамент по экономическим и социальным вопросам Организации Объединенных Наций, ввиду отсутствия

[89] ВОЗ, Всемирный доклад об инвалидности, 2011 год, ВОЗ, 2011 год.

единого определения термина "лица с ограниченными возможностями" страны внедрили различную классификацию и пороговые значения[90]. В соответствии с международно признанным определением ВОЗ лицо с ограниченными возможностями – это лицо, столкнувшееся с нарушением функционирования или структуры тела, ограничением действий или трудностями при выполнении действий или задач[91].

Как следует из этого определения, существует множество видов инвалидности, каждый из которых представляет собой барьер, влияющий на жизнь человека. В то же время важную роль в преодолении этих барьеров и содействии повышению качества жизни лиц с ограниченными возможностями играют технологии.

В настоящее время они получили широкое распространение, оказывая влияние как на повседневную жизнь отдельных людей, так и на общество в целом. За последнее десятилетие IoT продемонстрировал наличие потенциала, необходимого для того, чтобы изменить жизнь лиц с ограниченными возможностями к лучшему[92]. Поэтому для преодоления ограничений, обусловленных инвалидностью, все чаще используются ассистивные технологии на основе IoT[93].

В Конвенции о правах инвалидов ИКТ определены как один из важнейших элементов оказания помощи лицам с ограниченными возможностями. В частности, в Статье 9, посвященной вопросу доступности, подчеркивается роль ИКТ в содействии обеспечению независимости и всестороннего участия лиц с ограниченными возможностями в различных сферах деятельности, а также содержится положение, уполномочивающее государства-участники сознательно предпринимать совместные усилия для расширения доступа к ИКТ[94].

И ИКТ, и IoT позволяют повысить безопасность, мобильность и независимость; многие устройства и услуги IoT, от протезов, подключенных к интернету, до "умной" обуви, передающей владельцу направление движения при помощи вибрации, предназначены для повышения качества жизни и снижения зависимости лиц с ограниченными возможностями от других людей[95]. Например, слепые или слабовидящие лица могут использовать технологии, помогающие им ориентироваться в окружающем их мире и получать доступ к письменной информации. Кроме того, технологии "умного" дома позволяют людям управлять находящимися у них дома бытовыми приборами и другими предметами, доступ к которым может быть затруднен, такими как осветительные приборы, дверные замки и системы безопасности.

Технологии: две стороны одной медали

Несмотря на то, что ассистивные технологии на основе IoT создают множество преимуществ, они также экспоненциально повышают подверженность пользователей киберрискам. Учитывая растущую зависимость от ассистивных технологий, любое нарушение функционирования или изменение таких технологий может привести к повышению степени уязвимости.

Для устройств и услуг на основе IoT зачастую характерен уровень безопасности ниже оптимального. Так, они могут не использовать надлежащее шифрование для передачи данных, что может привести к неправомерному раскрытию и утечке данных. Для лиц с ограниченными возможностями, например, персональные данные могут иметь конфиденциальный характер и предполагать раскрытие подробной информации о состоянии здоровья человека.

Учитывая значимость ассистивных технологий для лиц с ограниченными возможностями, негативное воздействие киберрисков может иметь катастрофические последствия. В частности, некоторые люди с ограниченными физическими возможностями полагаются на биомеханические протезы для восстановления способности передвигаться в полной или частичной мере. В таких протезах используются специальные датчики для считывания и анализа параметров сокращения мышц, что позволяет воспроизвести движения с помощью соответствующих устройств (например, перемещение пальцев протеза руки). Протезы регулярно посылают данные в "облако" для анализа результатов проведенных

---

90 Департамент Организации Объединенных Наций по экономическим и социальным вопросам (ДЭСВ ООН), Disability and Development Report: Realizing the Sustainable Development Goals by, for and with persons with disabilities. United Nations, New York, 2018.

91 ВОЗ, там же, Глава 1.

92 Future of Privacy Forum, The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions, January 2019.

93 ВОЗ, Вопросы здравоохранения, Ассистивные технологии.

94 ДЭСВ ООН, Конвенция о правах инвалидов, Статья 9 "Доступность".

95 Future of Privacy Forum, там же

вычислений и повышения своей эффективности. Возможность установления соединений делает такие устройства уязвимыми для атак, направленных на получение доступа к данным, хранящимся в "облаке", манипулирование ими или удаление таких данных, а также на получение доступа к персональным данным пользователей. Более того, злоумышленники могут получить дистанционный контроль над управлением тем или иным протезом. Причем последствия могут быть еще хуже, если протез подключен к имплантату головного мозга[96].

В качестве другого примера можно привести кохлеарные имплантаты, которые используют некоторые люди с нарушениями слуха и которые имеют более инвазивный характер, чем традиционные слуховые аппараты. В основе данной технологии лежат три основных компонента, в частности микрофон, речевой процессор и имплантированный приемник-стимулятор. Некоторые современные кохлеарные имплантаты применяются вместе с устройствами дистанционного управления, которые позволяют пользователям управлять настройками имплантата с помощью мобильного приложения. На базовом уровне злоумышленники могут попытаться отключить имплантат, сделав жертву глухой. Более изощренные атаки могут помешать речевому процессору получить входящий сигнал от микрофона или могут перенастроить приемник для передачи звуков, генерируемых злоумышленником. Выявить такие более изощренные атаки может оказаться сложнее, особенно если у пользователей кохлеарных имплантатов нет другого способа проверить, что они слышат.

Помимо атак, ориентированных на использование ассистивных технологий, злоумышленники могут также делать своей мишенью технологии, которые традиционно используют лица с ограниченными возможностями. Так, лица с нарушением зрения могут лишиться всех надежных средств навигации, если используемые ими GPS-инструменты окажутся неисправными или умышленно взломанными злоумышленниками. При совершении спуфинг-атак на основе GPS радиопередатчик, расположенный рядом с целью, используется для создания помех производимому на законных основаниях сигналу GPS[97]. В этом случае злоумышленник может передать неточные координаты или прервать передачу данных, что может привести к нанесению материального ущерба и другим существенным последствиям.

Хотя это лишь несколько примеров возможных кибератак, направленных на использование цифровых ассистивных технологий, они подтверждают значимую роль кибербезопасности в обеспечении безопасности лиц с ограниченными возможностями, которые используют такие технологии.

Дальнейшие действия, которые следует рассмотреть

Интернет и IoT могут способствовать участию лиц с ограниченными возможностями в социальной, экономической и гражданской жизнедеятельности. Хотя потенциал таких технологий очевиден, для обеспечения согласованности социальных, законодательных, личностных и инфраструктурных факторов в рамках экосистемы IoT с акцентом на безопасности устройств IoT необходимо предпринимать усилия непрерывно. Правительства могли бы принять конкретные меры для повышения безопасности и, следовательно, надежности ассистивных технологий.

Они также могли бы принять меры для усовершенствования законодательства и политики в отношении доступности и безопасности IoT и разработать механизмы, которые помогли бы стимулировать и обеспечить их соблюдение. Внедрение такой концепции следует начинать с оценки потребностей лиц с ограниченными возможностями; при этом сама концепция должна предусматривать четкое распределение функций и обязанностей. Поскольку к решению данного вопроса, скорее всего, будут привлечены представители различных сфер государственного сектора (например, технологии и электросвязь, благосостояние и медицина), установление и поддержание сотрудничества будет иметь ключевое значение и требовать содействия в рамках работы над каждой инициативой.

Отдельные инициативы можно внедрить. Например, правительства могли бы разработать механизмы сертификации ассистивных технологий с точки зрения обеспечения кибербезопасности, что могло бы предусматривать проведение проверки и тестирования безопасности на периодической основе, а также взятие на себя обязательства регулярно обновлять систему с учетом развития технологий. Кроме того, правительства могли бы поддерживать производителей, создавая для них те или иные стимулы, содействуя партнерству между государственным и частным секторами и предлагая начальное финансирование и гранты для выполнения научно-исследовательской и опытно-конструкторской работы.

---

[96] Vladimir Dashchenko. How to Attack and Defend a Prosthetic Arm. Securelist (Kaspersky), 26 February 2019

[97] Maria Korolov, What is GPS spoofing? And how you can defend against it, *CSO website*, International Data Group (IDG), 7 May 2019.

Аналогичным образом, необходимо содействовать формированию культуры безопасности с возможностью реагирования на риски, связанные с соответствующими технологиями. Правительствам необходимо объединить усилия с частным сектором для проведения кампаний по повышению уровня осведомленности населения о кибербезопасности.

В заключение следует отметить, что, хотя ассистивные технологии на основе IoT являются одним из ключевых элементов поддержки лиц с ограниченными возможностями, они также могут создать и ряд рисков, которые при ненадлежащем решении вопроса могут иметь серьезные последствия. Поэтому ассистивные технологии должны отвечать самым высоким стандартам безопасности и учитывать технологический прогресс.

Извлеченные уроки и предлагаемые примеры передовой практики

Как указывалось выше, для повышения доступности информационно-коммуникационных услуг необходимо принимать меры по обеспечению кибербезопасности в интересах лиц с ограниченными возможностями, особенно лиц с нарушениями слуха, в частности таких, которые требуют использования услуг электросвязи по ретрансляции и дистанционного ввода субтитров.

4.2.3 Учет факторов безопасности при предоставлении услуг по обеспечению доступности ИКТ

Введение

Услуги по обеспечению доступности ИКТ, такие как услуги электросвязи по ретрансляции и дистанционный ввод субтитров, позволяют лицам с ограниченными возможностями общаться и получать доступ к информации. Такие услуги, безусловно, требуют принятия мер безопасности для защиты и обеспечения неприкосновенности частной жизни лиц с ограниченными возможностями и снижения киберуязвимости этих и других групп населения с особыми потребностями, таких как дети и пожилые лица.

Аспекты безопасности дистанционного ввода субтитров

Дистанционный ввод субтитров – это услуга, при которой слова, произнесенные на собрании или конференции, транскрибируются в другом месте, отличном от того, в котором проходило такое собрание[98]. Услуги на основе ИКТ, как, например, услуги с использованием стационарных и сотовых телефонов, а также компьютерного микрофона, предназначены для передачи голоса оратора специалисту по субтитрам, который транскрибирует голосовые данные в текст. Затем транскрибированный текст в режиме реального времени возвращается в место проведения собрания, где его можно прочитать. Текст с дистанционно введенными субтитрами часто отображается на экране или мониторе общего доступа в конференц-зале или на персональном мониторе. Услуги дистанционного ввода субтитров имеют жизненно важное значение для глухих или слабослышащих лиц, позволяя им участвовать в тех или иных собраниях; при этом они также несут пользу лицам, чей родной язык отличается от языка, используемого на собрании, и помогают в ситуациях, когда участие в работе различных групп принимают ораторы с разным голосом и акцентом (например, на работе, в классе или в общественном центре). Лицо, осуществляющее транскрибирование для дистанционного ввода субтитров, именуется специалистом по субтитрам и должно иметь квалификацию стенографиста. Часто специалист по субтитрам также известен как специалист по преобразованию речи в текст.

Необходимость предоставления услуг дистанционного ввода субтитров предусмотрена положениями различных норм и правил национального или местного значения. Поставщик услуг должен принять все разумные меры предосторожности для обеспечения конфиденциальности собрания, так как оно может содержать конфиденциальную информацию.

Виды конфиденциальной информации

Ниже приводится неполный перечень видов потенциально конфиденциальной информации:

– конфиденциальная информация, рассматриваемая в ходе собраний и/или конференций;

---

[98] Сектор стандартизации электросвязи МСЭ (МСЭ-Т), Технический документ FSTP-ACC-RCS, "Обзор служб дистанционного ввода субтитров", 17 октября 2019 года.

– медицинские данные пациентов;
– юридическая информация об отдельных лицах;
– консультации;
– информация о соблюдении требований в отношении защиты данных.

Поставщики услуг дистанционного ввода субтитров должны соблюдать действующие нормативно-правовые положения о конфиденциальности и защите данных, в частности такие, которые установлены Европейским союзом[99].

Шифрование текста с субтитрами

Текст, поступающий на дисплей или персональный терминал, должен быть защищен паролем. Поставщик услуг дистанционного ввода субтитров несет ответственность за безопасность скрипта и обязан соблюдать соответствующие требования по защите данных. Рекомендуется шифровать текст и, если необходимо, URL источника текста с помощью протокола безопасных соединений или другой соответствующей технологии.

Шифрование звука

Оригинальные звуковые данные мероприятия должны быть надежно защищены.

Вопросы безопасности при предоставлении услуг электросвязи по ретрансляции

Функциональная эквивалентность

Функциональная эквивалентность определяется как "*способность лиц с различными возможностями (в частности, лица с ограниченными возможностями и лица с особыми потребностями) пользоваться услугой или системой связи с таким же комплексом предлагаемых функций и с такой же степенью удобства использования, которые предлагается более широкой группе пользователей в составе населения [...] Это касается как технических, так и экономических факторов, а также предусматривает, что пользователи услуг ретрансляции не должны подвергаться какой-либо финансовой дискриминации*"[100].

Функциональная эквивалентность включает в себя обязательства, связанные с обеспечением безопасности, которые применяются к поставщикам услуг связи в той или иной юрисдикции. Функциональная эквивалентность подразумевает, что к пользователям услуг ретрансляции должны применяться те же условия, которые применяются к другим пользователям в рамках соответствующего сообщества, особенно в отношении типов вызовов, предусмотренных услугами ретрансляции, что может сказаться на обеспечении безопасности.

Требования безопасности в отношении обеспечения функциональной эквивалентности

Для достижения функциональной эквивалентности необходимо обеспечить конфиденциальность, неприкосновенность частной жизни и безопасность услуг ретрансляции по телефону, технологий, используемых для предоставления таких услуг, а также людей, задействованных в предоставлении таких услуг в качестве операторов связи.

Требования к услугам ретрансляции по телефону с точки зрения обеспечения конфиденциальности и безопасности вызовов, включая шифрование, должны согласовываться с требованиями, применимыми к услугам электросвязи в целом в соответствующей стране или регионе.

Факторы киберуязвимости лиц с особыми потребностями

Обеспечение безопасного пользования интернетом особенно важно для лиц и групп с особыми потребностями, таких как пожилые лица и дети. Снижение уровня киберуязвимости этих групп – это неотложный и важный вопрос, требующий разработки и соблюдения руководящих указаний.

---

[99] Европейский союз, регламент Regulation (EU) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент защиты данных).

[100] Сектор стандартизации электросвязи МСЭ, Рекомендация МСЭ-Т F.930 "Мультимедийные услуги электросвязи по ретрансляции".

4.3 Полезная информация

Вопрос 7/1 1-й Исследовательской комиссии МСЭ-D "Доступ к услугам электросвязи/ИКТ лиц с ограниченными возможностями и особыми потребностями", в рамках которого рассматриваются различные темы этой области[101]. Форум Future of Privacy Forum (Неприкосновенность частной жизни в будущем) публикует доклад, озаглавленный "Интернет вещей (IoT) и лица с ограниченными возможностями: изучение преимуществ, вызовов и противоречий в области обеспечения неприкосновенности частной жизни"[102].

В этих источниках содержится дополнительная информация.

[101] Вопрос 7/1 1-й Исследовательской комиссии МСЭ-D.
[102] Future of Privacy Forum. Op. cit, там же.

Глава 5 – Состояние проблем в области кибербезопасности, в том числе тех, которые стоят на пути появляющихся технологий, таких как интернет вещей и облачные вычисления

5.1 Введение

Экспоненциальный рост технологического потенциала привел к тому, что степень цифровизации мира, его подключения к интернету и его взаимосвязанности неуклонно увеличивается. По данным Всемирного экономического форума, эпоха, известная как "Глобализация 4.0", в которой цифровые активы и услуги составляют основу экономики и экспорта, уже началась[103].

Под действием инновационных решений меняется ход технологического развития, что обусловлено необходимостью удовлетворения новых производственных нужд и практических потребностей. Наряду с технологией 5G устройства IoT получает все большее распространение: по оценкам, к 2025 году в мире будет насчитываться 41,6 миллиарда подключенных устройств[104]. Роль облачных решений в осуществлении тех или иных операций приобрела жизненно важное значение, в связи с чем их применяют 94% предприятий по всему миру[105]. Учитывая растущую доступность и точность данных, ИИ также продолжает находить более широкое применение.

В то же время появление новых технологий усиливает необходимость обеспечения кибербезопасности. Цифровые инновации привели к увеличению числа продуктов и их значительному усложнению, в результате чего выросла вероятность использования различных уязвимостей и недостатков.

Число киберугроз непрерывно увеличивается. В 2018 году ежедневно совершалось 80 000 кибератак, что составляло свыше 30 миллионов атак в год[106]. В 2019 году ежедневно регистрировалось более 90 миллиардов попыток похищения конфиденциальной информации[107]. Киберугрозы также становятся все более изощренными, угрожая целому миру и экономике, ориентированным на цифровые технологии, включая киберфизические системы в домах, "умных" городах, транспортных средствах, производственных системах и объектах важнейшей инфраструктуры. Эксперты доказали, что можно взломать даже медицинские устройства, имплантированные в человеческий организм, такие как кардиостимуляторы и дозаторы инсулина[108].

Такой рост числа атак обусловлен также распространением в даркнете хакерства как услуги, которая зачастую предоставляется по приемлемой цене. Киберпреступность все больше коммерциализируется, превратившись в крупный сектор, где хакеры продают широкий спектр вредоносных инструментов и услуг, начиная от кражи паролей невысокой сложности и заканчивая сложными наборами эксплойтов и технологиями совершения атак, такими как DDoS, вредоносные программы, программы-вымогатели и программы-шпионы[109]. Кроме того, новые технологии, которые часто применяются для усовершенствования киберзащиты, могут использоваться злоумышленниками в целях повышения эффективности и расширения сферы применения инструментов взлома[110]. ИИ, автоматизированные бот-сети, IoT и "облачные" решения все чаще используются в крупномасштабных кибератаках, а применение новых методов взлома, таких как инструменты для автоматизированного фишинга, вместе с новыми технологиями расширило спектр киберрисков.

---

103 Klaus Schwab, Globalization 4.0- What Does It Mean? *World Economic Forum*, 5 November 2018.

104 Business Wire, The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast, 18 June 2019.

105 Kim Weins, Cloud Computing Trends: 2019 State of the Cloud Report, *Flexera Blog*, 21 May 2020.

106 PurpleSec, 2019 Cyber Security Statistics Trends & Data: The Ultimate List of Cyber Security Stats, *PurpleSec* (блог), accessed 27 April 2020.

107 Check Point, Prepare for a New Cyber Cold War in 2020, Warns Check Point, пресс-релиз, 24 October 2019.

108 Lily Hay Newman, These Hackers Made an App That Kills to Prove a Point, *Wired*, 16 July 2019; Dan Goodin. Insulin Pump hack delivers fatal dosage over the air, *The Register*, 27 October 2011.

109 Armor, The Dark Market Report: The New Economy, 28 September 2020.

110 Deloitte, Protecting against the changing cybersecurity risk landscape, Future of risk in the digital era, Deloitte & Touche LLC, 2019.

Серьезной проблемой кибербезопасности является общая нехватка профессиональных навыков и недостаточная осведомленность сотрудников. По мере того как киберугрозы становятся все более изощренными, организации с трудом набирают квалифицированных экспертов в области кибербезопасности, способных обеспечить защиту их систем[111]. В 2017 году 82% работодателей сообщили о том, что их сотрудники не обладают достаточными навыками в области кибербезопасности. К 2021 году 4 миллиона профессиональных должностей в сфере кибербезопасности останутся незанятыми[112]. Кроме того, персонал общего назначения демонстрирует слабый уровень знаний о киберугрозах. Человеческий фактор играет ключевую роль в обеспечении кибербезопасности и, как оказалось, несет значительную долю ответственности за допущенные инциденты. По результатам одного из исследований, в 2018 году 99% цифровых инцидентов были непреднамеренно инициированы сотрудниками, ставшими жертвами социальной инженерии; при этом лишь 1% таких инцидентов был вызван исключительно технологическими сбоями или эксплуатацией оборудования[113].

Кибербезопасность – это динамично развивающаяся сфера, и организации должны осуществлять непрерывную проверку применяемых ими средств кибербезопасности для защиты от возникающих угроз. Для создания более безопасной среды необходимо привлечь заинтересованные стороны к обсуждению вопросов кибербезопасности и управления рисками, связанными с неприкосновенностью частной жизни, обеспечить проверку, расширение и совершенствование существующих процессов управления рисками в области кибербезопасности и неприкосновенности частной жизни, а также определить ключевые факторы кибербезопасности и неприкосновенности частной жизни, которые могут быть характерны для тех или иных технологических решений и условий. В настоящей главе рассматривается множество угроз кибербезопасности, связанных с появляющимися технологиями, включая IoT, облачные вычисления, 5G, ИИ и четвертую промышленную революцию (называемую "Промышленная революция 4.0"). В ней также изложены существующие тенденции, проблемы и возможные решения, направленные на устранение угроз, которые могут свести на нет успехи, достигнутые благодаря внедрению цифровых инноваций.

5.2 Угрозы кибербезопасности, ее субъекты и их мотивы

Цель киберугроз заключается в том, чтобы подорвать три традиционные задачи кибербезопасности, а именно обеспечение конфиденциальности, целостности и доступности. Конфиденциальность защищает информацию от всех, кроме тех, кто имеет к ней доступ. Целостность обеспечивает точность и достоверность информации и предотвращает несанкционированное изменение данных. Доступность означает возможность доступа к данным и информации, когда это необходимо.

Ландшафт киберугроз – это неоднородная среда, в которой существуют различные субъекты, преследующие разные цели и располагающие разными возможностями. Ниже приведена возможная классификация, в целом, злоумышленников.

- ***Инсайдеры***: согласно последним данным, около 40% инцидентов совершаются внутренним персоналом, зачастую недовольными сотрудниками, которые стремятся отомстить своим работодателям[114]. Инсайдеры могут быть особенно опасны, поскольку они имеют прямой доступ к данным, информации и цифровым активам.
- ***Хактивисты***: это люди, действия которых обусловлены политическими и социальными мотивами. Как правило, они крадут и распространяют конфиденциальную информацию, с тем чтобы поставить в неловкое положение политических лидеров или знаменитостей, а также раскрывают проприетарные и секретные данные во имя свободы слова. Кроме того, они часто искажают веб-сайты и совершают атаки типа DDoS на определенные службы или веб-сайты[115].
- ***Киберпреступники***: это преступники, мотивированные финансовыми выгодами. Их цель – завладеть информацией об отдельных лицах, компаниях или организациях для получения денежной выгоды. Как правило, они шантажируют своих жертв, совершают эксфильтрацию и продажу данных и объектов прав интеллектуальной собственности на черном рынке, а также совершают атаки с

---

111 William Crumpler and James Lewis, The Cybersecurity Workforce Gap, Center for Strategic and International Studies, 29 January 2019.

112 Rob Saunders, 134 Cybersecurity Statistics and Trends for 2021, Varonis. Updated 16 March 2021.

113 Proofpoint, Proofpoint's Annual Human Factor Report Details Top Cybercriminal Trends: More than 99 Percent of Cyberattacks Need Humans to Click, 9 September 2019.

114 Verizon, 2019 Data Breach Investigations Report, Verizon, 2019.

115 Lillian Ablon, Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data, RAND Corporation, 2018.

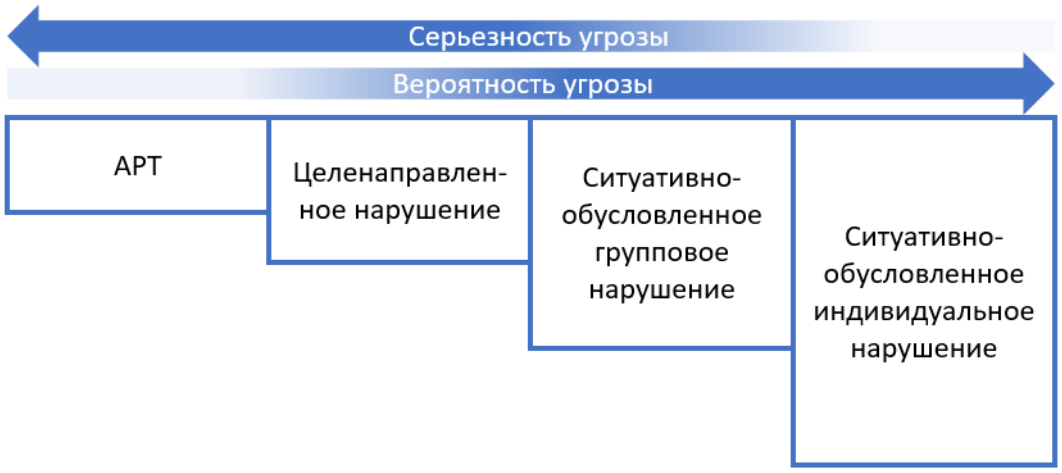
помощью программ-вымогателей. Как уже говорилось выше, киберпреступления превратились в услугу, в рамках которой различные группы продают причиняющие вред товары и услуги, начиная с системных эксплойтов и заканчивая полноценными атаками.

– ***Устойчивые угрозы нового уровня*** **(APT)**: согласно определению Национального института стандартов и технологий (NIST) Соединенных Штатов Америки, такие угрозы исходят от весьма изощренных и находчивых нарушителей, способных закрепиться в сети жертвы для достижения таких целей, как эксфильтрация информации, саботаж или препятствование осуществлению жизненно важных аспектов поставленной жертвой цели или причинение ущерба цифровым активам жертвы[116]. Устойчивые угрозы нового уровня адаптируются к системам защиты жертв благодаря тому, что атака совершается сразу по нескольким векторам; при этом выполнение предусмотренной такой атакой задачи может осуществляться в скрытном режиме в течение длительного периода времени. Такие нарушители являются наиболее сложными с точки зрения необходимых для этого технических навыков, финансирования и организационных ресурсов, поэтому их деятельность часто спонсируют государства для обеспечения своих геополитических интересов.

Несмотря на то, что все злоумышленники выбирают своей целью нарушение конфиденциальности, целостности и доступности информации и активов, вторжение в сеть может иметь широкий спектр последствий. Универсальный термин "кибератака" охватывает целый ряд действий, начиная с таких нарушений, как искажение веб-сайта или атака типа DoS, и заканчивая уничтожением важнейших данных и систем путем совершения атак с применением "оружия".

Злоумышленники и их атаки отличаются степенью изощренности и вредоносности, а также продолжительностью. Несмотря на то, что защититься от всех угроз не представляется возможным, организации могут распознавать соответствующие угрозы по их характеристикам, а также связанным с ними рискам и контексту, используя для этих целей модель угроз. На **Рисунке** 1 приведена общая модель киберугроз, показывающая, что большинство организаций, как правило, сталкиваются с ситуативно-обусловленными и менее изощренными угрозами, которые не требуют использования сложных средств защиты.

Рисунок 1: Модель угрозы



Напротив, крупные предприятия, организации, осуществляющие свою деятельность в жизненно важных и стратегических секторах, а также субъекты, управляющие ценной информацией и активами, с большей вероятностью подвергнутся атакам, исходящим от целенаправленных угроз или устойчивых угроз нового уровня.

В настоящем разделе представлен общий обзор существующих в киберпространстве угроз. В оставшейся части главы содержится информация о том, как такие угрозы применяются в отношении появляющихся технологий и какие доступны действенные стратегии, концепции и решения для защиты от них.

---

[116] NIST, Joint Task Force Transformation Initiative. NIST Special Publication 800-39: Managing Information Security Risk- Organization, Mission, and Information System View, March 2011.

5.2.1 Угрозы с технологической точки зрения

Появляющиеся технологии позволяют собирать, обмениваться, хранить и анализировать огромные объемы данных, зачастую с беспрецедентной скоростью. Вместе с тем некоторые факторы, в частности расширение возможностей для установления соединений и усложнение среды взаимодействия данных инструментов, могут породить ряд технологических и организационных проблем в области безопасности.

Виртуализация

Виртуализация является ключевым компонентом современной технологической среды, позволяя разработчикам настраивать инфраструктуру в соответствии с потребностями сетевых приложений и осуществлять разработку новых архитектур и протоколов в идеальных условиях[117]. В то же время совместное использование каналов связи и маршрутизаторов в многоарендной архитектуре сопряжено с рядом рисков для обеспечения безопасности[118].

– Риск несанкционированного раскрытия данных, как преднамеренного, так и непреднамеренного характера, усугубляется в виртуальной среде, где физические ресурсы совместно используются несколькими клиентами или пользователями. Вредоносные действия, такие как перехват и сбор "мусора" (поиск остатков данных в сети для получения информации), легче осуществить, если система позволяет проводить перекрестную проверку различных пользователей.

– Многоарендная архитектура может увеличить риски, обусловленные наличием цепочки поставок, что затрудняет защиту от вторжений. Злоумышленники могут получить привилегии и вторгнуться в сеть жертвы, используя в качестве вектора вторжения ресурсы на том же физическом уровне, но с более низкой степенью защиты.

– В виртуализированной среде результаты обработки персональных данных имеют особенно сложный характер ввиду высокой иерархичности систем администрирования привилегий. Такие особенности открывают злоумышленникам возможности для совершения мошеннических действий с персональными данными и повышения уровня привилегий.

– Совместное использование ресурсов может также увеличить риск злонамеренных или непреднамеренных сбоев в работе системы, которые могут негативно сказаться на предоставлении услуг. В частности, перегрузка физических ресурсов может снизить производительность виртуальных сетей с последующим нарушением связи.

Безопасность облачных вычислений

В облачных решениях предоставление услуг и ресурсов на основе ИТ, включая связанные с ними функции и обязанности по обеспечению безопасности, осуществляется с привлечением поставщика облачных услуг. Благодаря этому появляется возможность оперативно расширить масштаб внедрения новых технологий и повысить их безопасность, так как поставщик, применяя принцип экономии за счет масштаба, потенциально может предложить более высокий уровень защиты и контроля. В то же время облачные уязвимости могут оказаться привлекательными для киберзлоумышленников ввиду того, что один-единственный успешный взлом может дать несанкционированный доступ ко множеству клиентов. Облачные решения включают в себя нескольких уровней абстракции (а именно: приложение, операционная система, архитектура и сеть), что позволяет злоумышленникам атаковать их по нескольким направлениям.

– Уязвимостями программного обеспечения можно воспользоваться путем внедрения кода на языке структурированных запросов и применения других механизмов для совершения атак. В этом сценарии потребителям облачных услуг важно понимать, кто отвечает за внесение тех или иных исправлений (в частности поставщик облачных решений – за решения в отношении программного обеспечения как услуги, а потребитель – за решения в отношении инфраструктуры как услуги и платформы как услуги).

– Поставщики облачных решений предлагают широкий спектр услуг и подключенных к интернету интерфейсов прикладного программирования, что позволяет их клиентам администрировать и контролировать свои активы. Такая возможность установления соединений делает облачные

---

117 Leonardo Richter Bays et al., Virtual network security: threats, countermeasures, and challenges, *Journal of Internet Services and Applications* 6, article no. 1 (2015).

118 Агентство Европейского союза по кибербезопасности (ENISA), Security aspects of virtualization, 10 February 2017.

решения потенциальной мишенью для сетевых атак, таких как выслеживание/прослушивание сетевого трафика, атаки типа DoS и атаки через посредника.

- Если злоумышленнику удается незаконно получить учетные данные пользователей, он может получить доступ к интерфейсу управления, используемому администраторами для управления большим количеством активов. Учитывая это, необходимо создать надежные механизмы аутентификации и авторизации, особенно для высокопривилегированных сотрудников.
- Многоарендная архитектура увеличивает риск нарушения сохранности или утечки данных в случае сбоя или взлома системы раздельного управления (нарушение изолированности).
- При переходе на облачные решения клиенты, как правило, теряют с точки зрения прозрачности и контроля над своими данными и активами. Это увеличивает риски, связанные с безопасным удалением данных, хранящихся на нескольких устройствах инфраструктуры поставщика облачных решений. Поэтому необходимо убедиться, что данные были надежно и тщательно удалены. Данная проблема усугубляется при применении многооблачных решений.
- Привязка к поставщику, в результате которой клиенты сталкиваются с трудностями при переходе к другому поставщику облачных решений, может представлять серьезные риски для безопасности. Пользователям необходимо предусмотреть планы в отношении смены поставщика при разработке стратегий обеспечения непрерывности бизнес-процессов, а также хранить все данные в стандартном формате, позволяющем без труда осуществить их передачу.
- По данным Регуляторного органа связи Намибии, хранение данных клиентов в центрах обработки данных поставщиков облачных услуг, расположенных за пределами границ государства, представляет собой острую проблему. Юрисдикция органов регулирования не распространяется на страны, где размещены серверы данных, поэтому на их территории они практически не могут осуществлять надзор за обеспечением защиты клиентов и кибербезопасности в случае совершения кибератак, что приводит к краже идентичности, утечке персональных данных и, в некоторых случаях, потере потенциального дохода. Кроме того, законодательство таких стран может отличаться в том, что касается доступа к информации, защиты данных и законного мониторинга, в результате чего клиенты могут подвергаться несанкционированному доступу к персональным данным[119].

Интернет вещей

Поскольку культура безопасности, закладываемой на этапе проектирования, еще только начинает получать распространение, одной из наиболее тревожных тенденций с точки зрения рисков является расширение возможностей для установления соединений, которое создает значительные проблемы в области безопасности[120].

- "Умные" объекты, начиная с камер, дверей и холодильных установок и заканчивая системами кондиционирования воздуха и носимыми устройствами, собирают огромное количество информации (как данных, так и метаданных). Подслушивая данные, получаемые "умными" объектами своей жертвы, злоумышленники могут многое узнать о ее жизни.
- Новой угрозой для IoT являются программы-вымогатели. "Умные" устройства создают заманчивые возможности для вымогательства со стороны злоумышленников, и это обусловлено не только широким выбором "легкой" добычи, но и тем, что атаки такого рода могут нарушить функциональность устройств, тем самым причиняя жертве неудобства и заставляя ее платить выкуп[121].
- Устройства IoT особенно уязвимы для атак типа DoS и DDoS, поскольку большинство из них имеют ограниченные технические возможности (память, хранение, центральный процессор и т. д.). Злоумышленники могут без труда перегрузить их ограниченные ресурсы, вызвав сбои в функционировании.

---

119 Документ SG2RGQ/75 ИК2 МСЭ-D, Намибия.

120 Amit Ashbel, The rise of IoT and the associated security risks, 7 July 2016.

121 Syed Rameem Zahra and Mohammad Ahsan Chishti, RansomWare and Internet of Things: A New Security Nightmare, *Proceedings of the 9th International Conference on Cloud Computing, Data Science Engineering (Confluence),* Uttar Pradesh, India, 10-11 January 2019.

– Ограниченность ресурсов в устройствах IoT создает очень существенную проблему, если возникает необходимость предусмотреть в них возможность принятия мер по обеспечению безопасности, поскольку последние могут требовать большого объема вычислительной работы[122].

– Ключевым фактором обеспечения безопасности IoT является уровень сложности. В устройствах применены различные технологии, такие как виртуализация, облачные вычисления, датчики и сети, которые имеют свои собственные уязвимости. Обеспечить безопасность IoT означает обеспечить безопасность всей цепочки таких компонентов. Аналогичным образом, IoT применяется в нескольких областях (бытовая автоматика, здравоохранение, предметы одежды и т. д.), в которых существуют различные потребности в отношении обеспечения безопасности и которые подвержены различным угрозам.

– Несмотря на то, что наиболее распространенными являются интернет-атаки, устройства IoT также могут стать объектом физических атак. В местах, где наблюдение совсем или практически не ведется, злоумышленники могут без труда получить доступ к устройствам IoT и взломать их.

– Устройства IoT также могут использоваться в качестве векторов для совершения атак типа DDoS. Так, в 2016 году известный поставщик систем доменных имен стал жертвой атаки типа DDoS, которая исходила от десятков миллионов IP-адресов, причем большая часть вредоносного трафика поступала с устройств IoT, таких как принтеры, маршрутизаторы и камеры[123].

5G

Технологии связи пятого поколения, известные как 5G, повысят надежность и качество соединений за счет высокой скорости и малого времени задержки, что позволит получить максимальную отдачу от применения приложений на основе появляющихся технологий в таких областях, как энергетика, здравоохранение и производство. Соответствующие активы привлекают и злоумышленников, а присущие им уязвимости делают задачу по обеспечению кибербезопасности особенно сложной. Кроме того, поскольку решения на основе 5G все еще находятся на этапе экспериментального внедрения, существующих данных и информации о случаях совершения кибератак недостаточно, что еще больше усложняет понимание потенциальной угрозы[124].

– Ландшафт угроз, связанных с 5G, широк и неоднороден; сочетая в себе различные технологии, он также наследует сопряженные с ними уязвимости и угрозы. В частности, сети и активы 5G могут подвергаться атакам вследствие использования унаследованных уязвимостей технологий второго, третьего и четвертого поколений, а также традиционных IP-уязвимостей и уязвимостей технологии виртуализации. Злоумышленники также могут нацелиться на активы, характерные для 5G, такие как ядро, точка доступа и граничные элементы.

– Атаки на технологии 5G могут включать в себя попытки кражи или уничтожения данных, манипулирования ими, перехвата сообщений или нарушения функционирования средств связи, повреждения физических активов или нарушения предоставления услуг. 5G соединит широкий спектр секторов и вертикалей, что, скорее всего, изменит условия кибербезопасности и, таким образом, вызовет появление новых уязвимостей.

– Критический фактор угрозы исходит от цепочки поставок, в частности от подвергшихся атаке поставщиков товаров и услуг. Риск заключается в том, что поставщик может злонамеренно оставить в своей продукции скрытые обходные пути, недоработки программного обеспечения или критические ошибки. Внедрение автоматических (и неконтролируемых) обновлений и манипулирование функциональными возможностями также создают проблемы для обеспечения безопасности. Взаимосвязь между 5G и национальной безопасностью очевидна, поэтому к отбору поставщиков необходимо подойти серьезно, применив ориентированный на риски подход.

---

122 Ammar Rayes and Samer Salam, Internet of Things From Hype to Reality: The Road to Digitization, Springer International Publishing, 2019.

123 Nicole Perlroth, Hackers Used New Weapons to Disrupt Major Websites Across U.S, *The New York Times*, 21 October 2016.

124 ENISA, ENISA threat landscape for 5G Networks, November 2019.

Искусственный интеллект

Распространение решений на основе ИИ в различных сферах жизнедеятельности общества будет влиять на условия обеспечения кибербезопасности по нескольким направлениям. Такие активы могут стать мишенью для злоумышленников или использоваться ими и теми, кто им противостоит.

– Активами на основе ИИ можно манипулировать, изменяя автоматизированные решения и поведение, в частности, путем искажения данных, фальсификации моделей классификации и использования обходных путей[125]. Все эти методы используют возможности для обучения системы, с тем чтобы оказать отрицательное воздействие на результат, введя в систему ошибочные данные и информацию[126].

– Хакеры прибегают к решениям на основе ИИ, с тем чтобы расширить охват своих действий и возможности. ИИ можно использовать для создания вредоносных программ, способных обходить меры защиты в автономном режиме, адаптируя применяемые методы на основе полученных положительных результатов и непрерывно совершенствуя свои действия.

– ИИ также является важным оборонительным ресурсом. Он может значительно повысить устойчивость системы путем усиления типичных мер защиты, таких как обнаружение угроз и аномалий, реагирование на инциденты и анализ угроз.

5.2.2 Угрозы через призму Промышленной революции 4.0

Парадигма Промышленной революции 4.0 предполагает применение автоматизации наряду с IoT, решениями в области виртуализации, аналитикой и ИИ в различных вертикалях. Указанные технологии позволяют собирать, хранить, совместно использовать и интерпретировать огромные объемы данных и могут способствовать достижению существенного прогресса с точки зрения скорости, действенности, экономической эффективности и предоставления услуг. Предусмотренные Промышленной революцией 4.0 принципы применимы в различных отраслях, каждая из которых подвержена характерным для нее угрозам и рискам для безопасности.

"Умные" дома

"Умные" дома – это одна из множества вертикалей, где можно применить принципы, предусмотренные Промышленной революцией 4.0, в частности в области "умного" энергопотребления, освещения и отопления. "Умные" дома включают в себя широкий спектр "умных" объектов, которые используют датчики и исполнительные механизмы и управляются дистанционно через интернет[127]. Подключение устройств к интернету создает ряд рисков для безопасности.

– "Умные" дома генерируют огромные объемы данных, которые уязвимы для атак. Как отмечено Министерством почты и новых информационно-коммуникационных технологий Чада, объекты, подключенные к интернету (включая "умные" телевизоры), не защищены от угроз безопасности информационной системы. Так, использование подключенных телевизоров может способствовать доступу к персональным данным через интернет не имеющих таких прав лиц или упростить кражу идентичности через сеть. Подключенные объекты так же уязвимы, как и личный компьютер, подключенный к компьютерной сети. Аналогичным образом, они подвергаются угрозе со стороны вредоносных программных средств[128].

– "Умные" устройства имеют слабую защиту, и их можно без труда взломать. Злоумышленники, получившие контроль над устройством, могут перемещаться в боковом направлении в пределах внутренней сети, чтобы взять под контроль другие узлы.

– "Умные" устройства, как правило, обладают ограниченными вычислительными ресурсами, что делает их особенно уязвимыми для атак типа DoS и DDoS, в результате которых устройство или сеть становятся временно недоступными для предполагаемого пользователя.

---

125 Battista Biggio and Fabio Roli, Wild patterns: Ten years after the rise of adversarial machine learning, *Pattern Recognition*, Vol. 84, December 2018, pp. 317-31.

126 Matthew Jagielski et al., Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning, *IEEE Symposium on Security and Privacy (SP)*, 2018.

127 Ado Adamou Abba Ari et al. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics*, 31 July 2020.

128 Документ 2/140 ИК2 МСЭ-D, Чад.

"Умные" города

Инфраструктура "умных" городов построена на сочетании появляющихся технологий с технологиями интеграции данных и автоматизации задач, что позволяет оптимизировать организацию городов и предложить услуги более высокого качества. В основе функционирования "умных" городов лежит обмен обширными массивами данных между важнейшими службами, такими как транспорт, энергоснабжение и здравоохранение, взаимосвязь которых неуклонно растет. Масштабы производимых данных и роль, которую эти данные играют в функционировании "умных" городов, обуславливают острую потребность в обеспечении кибербезопасности для защиты конфиденциальной информации и целостности цифровых активов от различных угроз безопасности.

– ***Электронное здравоохранение***: поскольку зависимость от технологий и объем данных в сфере здравоохранения растут, поставщики медицинских услуг должны защитить конфиденциальную информацию и обеспечить предоставление услуг. Несмотря на то, что информация о каких-либо имевших место инцидентах отсутствует, результаты моделирования подтвердили возможность беспроводного отключения имплантируемых кардиодефибрилляторов[129], взлома дозаторов инсулина в целях введения летальной дозы[130] и даже проникновения в системы мониторинга здоровья пациента для изменения основных показателей состояния его организма в режиме реального времени[131].

– ***"Умные" электросети***: это ключевой компонент "умных" городов. В них используются двунаправленные устройства, такие как датчики, исполнительные механизмы и счетчики, которые позволяют поддерживать потоки энергии, идущие от производителей к потребителям, на одинаковом уровне и осуществлять контроль над ними[132]. Поскольку "умные" электросети используют протоколы ИКТ и подключение к интернету, они уязвимы для кибератак[133]. Хотя "умные" электросети представляют собой заманчивую мишень для совершения атак, они имеют сложную архитектуру, вследствие чего нанесение крупномасштабного ущерба требует технических и организационных ресурсов высокого уровня. На сегодняшний день известно лишь о двух случаях серьезных перебоев в электроснабжении, вызванных кибератаками, – BlackEnergy3 и Crashoverride, за которыми, как полагают, стояли государственные субъекты[134].

– ***"Умный" транспорт***: цифровые активы, физические системы, сети связи и автоматизация могут использоваться в сфере транспортной инфраструктуры для оптимизации качества и эффективности. Изменяя данные и информацию, злоумышленники могут препятствовать трафику и даже вызывать инциденты. Кроме того, "умные" транспортные системы предполагают значительный поток персональной и конфиденциальной информации, которую необходимо защищать.

Промышленный интернет вещей

Промышленный интернет вещей (IIoT) адаптирует парадигму IoT к условиям промышленности. В сочетании с робототехникой и автоматизацией это может дать промышленным предприятиям важное преимущество, в том числе за счет повышения качества, экономической эффективности и поддержания производственного процесса на должном уровне. Такие киберфизические системы имеют особые характеристики и требования, ввиду чего преобразование традиционных мер обеспечения кибербезопасности становится особенно проблематичным.

Киберфизическая система – это существующая в режиме реального времени материальная среда с высоким уровнем обусловленности и взаимосвязанности, в которой доступность данных имеет выраженный характер по сравнению с целостностью и конфиденциальностью данных[135]. В таких системах цифровые компоненты взаимодействуют с физическими процессами, такими как движение объектов, химические реакции, выделение веществ и процессы охлаждения, а потоки данных служат в качестве

---

129 Daniel Halperin et al., Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, *IEEE Symposium on Security and Privacy (SP)*, 2008.

130 Arundhati Parmar, Hacker shows off vulnerabilities of wireless insulin pumps. *MedCityNews*, 1 March 2012; David Klonoff, Cybersecurity for Connected Diabetes Devices, *Journal of Diabetes Science and Technology* 9, Vol. 9, No. 5, 16 April 2015.

131 Douglas McKee, 80 to 0 in Under 5 Seconds: Falsifying a Medical Patient's Vitals, McAfee, 11 August 2018.

132 Lindah Kotut and Luay A. Wahsheh, Survey of Cyber Security Challenges and Solutions in Smart Grids, 2016 *Cybersecurity Symposium* (CYBERSEC).

133 Muhammed Zekeriya Gunduz and Resul Das., Cyber-security on smart grid: Threats and potential solutions, *Computer Networks*, Vol. 169, 14 March 2020.

134 Dragos, Inc., CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids, 12 June 2017.

135 Roberto Setola et al., Cyber threats for operational technologies. *International Journal of System of Systems Engineering*, Vol. 10, No. 2, 2020.

ресурсов, необходимых для выполнения задач. В таких условиях внедрение общих средств обеспечения безопасности, таких как антивирусное программное обеспечение, шифрование или брандмауэры, может замедлить поток данных и нарушить ход выполнения действий, что приведет к задержкам, которые могут существенно повлиять на осуществление деятельности, несмотря на то, что они не являются значимыми с количественной точки зрения[136].

Кроме того, большая часть оборудования в киберфизических системах не может справиться с осуществлением сложных мер безопасности и внедрением обновлений, что приводит к тому, что подключенные к интернету активы оказываются потенциально уязвимыми. Кибератаки на промышленные киберфизические системы могут нанести серьезный экономический ущерб, нарушив их функционирование и, как следствие, производственный процесс на заводе.

В то же время ключевая проблема заключается в том, что, манипулируя потоком данных, злоумышленники, совершающие кибератаки, могут изменять функционирование системы до тех пор, пока не произойдет ее механическое разрушение, что приведет к кинетическому воздействию и может иметь серьезные последствия для безопасности населения. Так, если злоумышленник введет в систему измененные данные, которые покажут диспетчеру, что температура снижается слишком быстро, диспетчер автоматически примет меры для компенсации такого снижения, увеличив температуру нагрева, что приведет к скрытому перегреву[137]. В 2014 году, например, злоумышленники взломали систему немецкого сталелитейного завода и не позволили печи выключиться надлежащим образом, чем могли нанести серьезный физический ущерб важнейшим компонентам[138].

Злонамеренные кибердействия, способные оказать физическое воздействие, имеют крайне сложный характер и требуют не только хорошего понимания используемых цифровых активов, но и обширных знаний целевого физического процесса, а также подробных сведений о различных переменных. Таким образом, располагать техническими и организационными ресурсами, необходимыми для осуществления операций такого рода, по всей видимости, могут злоумышленники, стоящие за устойчивыми угрозами нового уровня, и спонсируемые государствами посредники.

5.3 Существующие и появляющиеся решения

Значительная часть устройств IoT не имеет встроенных базовых функций по обеспечению кибербезопасности. В октябре 2018 года, после 18 месяцев взаимодействия с представителями отрасли и экспертами Национального центра кибербезопасности, Министерство цифровых технологий, культуры, средств массовой информации и спорта Соединенного Королевства опубликовало Кодекс практики по безопасности потребительских устройств IoT[139]. В кодексе содержатся 13 добровольных руководящих указаний, которые являются базовыми для устройств IoT и которые производители должны учитывать при разработке своей продукции, чтобы обеспечить ее "проектируемая безопасность". Кодекс способствовал разработке первого применимого на глобальном уровне стандарта безопасности IoT – ETSI TS 103 645[140].

Algérie Télécom также отметил необходимость предоставления руководящих указаний и рекомендаций по обеспечению безопасности появляющихся технологий, таких как облачные вычисления и IoT, которые должны стать основной движущей силой развития информационной системы и цифровой экономики[141].

В **Таблице 1** и **Таблице 2** приведен перечень Рекомендаций МСЭ-Т, которые имеют отношение к защите облачных вычислений и IoT, соответственно, с точки зрения инфраструктуры, приложений, данных и конфиденциальности.

---

136 Roberto Setola et al., An overview of Cyber Attack to Industrial Control System, *Chemical Engineering Transactions*, Vol. 77, 2019.

137 Stephen McLaughlin et al., The Cybersecurity Landscape in Industrial Control Systems, *Proceedings of the IEEE*, Vol. 104, issue 5, May 2016.

138 Robert Lee et al., German Steel Mill Cyber Attack, Industrial Control Systems Defense Use Case Dec 30, 2014.

139 Министерство цифровых технологий, культуры, средств массовой информации и спорта Соединенного Королевства, Code of Practice for Consumer IoT Security. October 2018.

140 ETSI, ETSI TS 103 645 V1.1.1 (2019-02), Cyber Security for Consumer Internet of Things.

141 Документ 2/66 ИК2 МСЭ-D, Algérie Télécom SPA (Алжир).

Таблица 1: Архитектура безопасности для защиты инфраструктуры, приложений и данных, а также обеспечения конфиденциальности в сфере облачных вычислений

Название	Тема	Учреждение	Ссылка
Обзор безопасности облачных вычислений			
МСЭ-Т X.1601	Основы безопасности облачных вычислений	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12613
Проектирование безопасности облачных вычислений			
МСЭ-Т X.1602	Требования по безопасности прикладной среды программного обеспечения как услуги	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12615
МСЭ-Т X.1603	Требования к безопасности данных для услуги мониторинга облачных вычислений	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13406
МСЭ-Т X.1604	Требования к безопасности сети как услуге (NaaS) в среде облачных вычислений	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14093
МСЭ-Т X.1605	Требования к безопасности открытой инфраструктуре как услуге (IaaS) в среде облачных вычислений	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14094
МСЭ-Т X.1631	Информационные технологии – Методы обеспечения безопасности – Свод правил для управления информационной безопасностью, в основе которого лежит стандарт ISO/IEC 27002 для облачных услуг	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12490
Передовой опыт и руководящие указания в сфере облачных вычислений			
МСЭ-Т X.1641	Руководящие указания по безопасности данных потребителей облачных услуг	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12853
МСЭ-Т X.1642	Руководящие указания по эксплуатационной безопасности облачных вычислений	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=12616

Таблица 2: Архитектура безопасности для защиты инфраструктуры, приложений и данных, а также обеспечения конфиденциальности в сфере IoT

Название	Тема	Учреждение	Ссылка
Безопасность интернета вещей (IoT)			
МСЭ-Т X.1361	Структура безопасности интернета вещей на основе модели с использованием шлюза	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13607
МСЭ-Т X.1362	Простая процедура шифрования для среды интернета вещей (IoT)	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13196
МСЭ-Т X.1364	Требования безопасности и структура безопасности узкополосного интернета вещей	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14088
МСЭ-Т X.1365	Методика обеспечения безопасности при использовании криптографии на основе идентичности в поддержку услуг интернета вещей (IoT) в сетях электросвязи	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14089
МСЭ-Т серия X, Доб. 31	МСЭ-Т X.660 – Добавление "Руководящие указания по использованию идентификаторов объектов для интернета вещей"	МСЭ	https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13411

Прочие появляющиеся методы и системы обеспечения безопасности

– Приложения ИИ, в том числе машинного и глубокого обучения, могут значительно повысить действенность и экономическую эффективность стратегий обеспечения кибербезопасности. С помощью регрессии, классификации и кластеризации эти решения выявляют аномалии, определяют различные типологии атак и разрабатывают возможные ответные меры для устранения их последствий. Системы на основе ИИ также могут усилить эффект от мер реагирования на инциденты, предложив конкретные меры в ответ на те или иные инциденты. Кроме того, они могут повысить уровень управления рисками путем присвоения новым уязвимостям и ошибкам конфигурации значений показателей риска в автоматическом режиме на основе их описания, а также самостоятельно предупреждать атаки, значительно ускоряя извлечение, обработку и применение данных об угрозах, исполнителях, атаках, вредоносных программных средствах, уязвимостях и индикаторах компрометации[142].

– Особенности технологии распределенного реестра (DLT) также являются перспективными с точки зрения использования приложений по обеспечению безопасности[143]. Во-первых, хранение данных с помощью DLT осуществляется децентрализовано, что значительно снижает риск обширной утечки данных, поскольку злоумышленники больше не могут получить доступ ко всем хранящимся данным через одну-единственную точку доступа. Аналогичным образом, децентрализация приносит существенные преимущества в области безопасности сетям IoT, организация которых традиционно построена на логике "клиент-серверная модель", предусматривающей управление данными и устройствами в сети центральным органом. С помощью DLT-приложений устройства IoT могут выявлять аномалии и изолировать узлы, которые ведут себя странным образом. Кроме того, DLT может способствовать формированию доверия к сетям IoT, обеспечивая непрерывную доступность, контролируемость, подотчетность, целостность и конфиденциальность подлежащих обмену данных[144].

– Метод оркестровки, автоматизации и реагирования на угрозы безопасности (SOAR) включает в себя решения, предусматривающие установление соединений между инструментами и системами

[142] Padmavathi Ganapathi and D. Shanmugapriya, Handbook of Research on Machine and Deep Learning Applications for Cyber Security. *IGI Global*, 2019; and Dave Shackleford, Who's Using Cyberthreat Intelligence and How?. *SANS*, 12 February 2015.

[143] Nir Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, *Telecommunications Policy*, Vol.41, issue 10, November 2017.

[144] Ben Cole, The 'supply chain of trust' inherent to IoT data security, *IoT Agenda*, 28 November 2016.

безопасности для обеспечения комплексности и органичности действий, таких как управление уязвимостями, реагирование на инциденты и автоматизация операций по обеспечению безопасности. Автоматизация процессов по обеспечению безопасности позволяет системе осуществлять мероприятия по устранению нарушений и проведению регламентных работ (сканирование уязвимостей, мониторинг доступа и ведение журнала регистрации) без вмешательства со стороны человека.

– Еще один вариант предусматривает использование модели нулевого доверия, в которой внутренняя сегментация сетевой среды и администрирование доступа осуществляются по принципу наименьших привилегий. Иными словами, каждый модуль, включая пользователей, устройства, интерфейсы прикладного программирования и устройства IoT, имеет доступ только к тем ресурсам, данным и активам, которые необходимы для их правомерного функционирования. Модели нулевого доверия значительно повышают уровень внутренней безопасности, затрудняя боковое перемещение злоумышленников и повышение ими своих привилегий благодаря тому, что заставляют их атаковать сразу несколько устройств для получения доступа ко всей сети.

– "Брокеры" безопасности облачного доступа – это точки применения правил, функционирующие на уровне между пользователями и поставщиками облачных услуг. В частности, принудительное применение правил безопасности может включать в себя аутентификацию, однократную регистрацию входа, авторизацию, сопоставление регистрационных данных, составление профилей устройств, шифрование, токенизацию, ведение журнала регистрации, оповещение, а также обнаружение/предупреждение применения вредоносных программных средств[145].

– Управление привилегированным доступом – это мониторинг и защита привилегированных учетных записей, таких как учетные записи администратора, используемые для доступа к важнейшим активам, данным и ресурсам, с помощью комплекса инструментов и решений. Такие решения изолируют важнейшие учетные записи в безопасном и контролируемом репозитории, тем самым снижая риск кражи регистрационных данных.

– Организациям следует перейти от подхода, ориентированного на разработку и эксплуатацию (DevOps), к подходу, ориентированному на разработку, обеспечение безопасности и эксплуатацию (DevSecOps), согласно которому функция обеспечения безопасности является неотъемлемой частью разработки и эксплуатации. В системах и инструментах DevSecOps обеспечение безопасности не привязывается к созданию конечного продукта (такого как программное обеспечение и приложения), а рассматривается как неотъемлемая и существенная функция, начиная с самого раннего этапа разработки. Такой подход повышает надежность мер по обеспечению безопасности, снижает риски и сокращает расходы на обеспечение соответствия нормативным требованиям.

– Разработанная Гартнером Адаптивная система непрерывной оценки риска и доверия (CARTA) предлагает адаптивный подход к обеспечению безопасности, в котором принятие решений осуществляется исходя из рисков и эффективности[146]. CARTA предполагает три этапа действий: "выполнение", в рамках которого основные усилия направлены на анализ основных угроз; "построение", который относится к угрозам и уязвимостям, выявленным в ходе разработки продуктов и их эксплуатации; и "планирование", в рамках которого используются аналитические методы для определения рисков безопасности и оценки того, не окажет ли их снижение негативного влияния на производительность[147].

Экономически эффективные решения

– По данным Министерства цифровых технологий, культуры, средств массовой информации и спорта Соединенного Королевства, начать борьбу с последствиями кибератак в широких масштабах и получить при этом значительные выгоды на глобальном уровне можно путем воздействия на окупаемость инвестиций в совершение наиболее типичных и менее усложненных атак. Программа активной киберзащиты (ACD) была разработана для снижения окупаемости соответствующих инвестиций преступников вследствие повышения стоимости и рисков совершения кибератак на товары Соединенного Королевства[148]. В 2018 году программа обеспечила наибольший эффект от своей реализации благодаря своей ликвидационной службе, отвечающей за выявление

---

145 Gartner, Gartner Glossary. Cloud Access Security Brokers (CASBs).
146 Gartner, The Gartner IT Security Approach for the Digital Age, 12 June 2017.
147 Gartner, Gartner Keynote: Leverage Automation for Modern Security, 17 June 2019.
148 Ian Levy and Maddy S. Active Cyber Defence (ACD)- The Second Year, United Kingdom National Cyber Security Centre. 15 July 2019.

вредоносных веб-сайтов (те, которые непосредственно участвуют в совершении атак или обеспечивают инфраструктурную поддержку их совершения) и уведомление их владельца или лица, предоставляющего услуги хостинга, о необходимости удаления таких веб-сайтов из интернета: таким образом было ликвидировано в общей сложности 192 256 мошеннических веб-сайтов; причем 64% этих веб-сайтов были ликвидированы в течение 24 часов. Кроме того, были ликвидированы 22 133 фишинговых кампании, размещавшихся в переданном Соединенному Королевству IP-пространстве (в общей сложности 142 203 индивидуальных атаки), а также 14 124 связанных с правительством фишинговых веб-сайта[149].

– По мнению литовской компании NRD Cyber Security, для достижения значительных положительных результатов с точки зрения обеспечения безопасности национальной цифровой среды национальные и отраслевые группы CSIRT должны не только выполнять функции контактных лиц, аналитиков и координаторов мер реагирования на инциденты, но и вдохновлять на развитие и способствовать формированию дополнительного независимого потенциала в области кибербезопасности на уровне отраслей, профессиональных сообществ, образовательных центров, исследований, мероприятий, собраний, конференций, а также частных и ведомственных CSIRT[150].

– По мнению эстонской компании Guardtime, киберучения имеют первостепенное значение для обеспечения киберустойчивости в долгосрочной перспективе, так как они помогают группам понять, какие процессы необходимы для смягчения последствий киберкризиса. Эстония рекомендует разработать программу управления киберустойчивостью, предусматривающую принятие соответствующих мер в области образования, проведения профессиональной подготовки и организации киберучений, включая как мероприятия местного значения, так и национальные учения, разработанные с учетом конкретных потребностей и проводимые на регулярной основе. Такие программы должны учитывать различные аспекты национальной организационной структуры и социально-экономической ситуации, функции и обязанности различных заинтересованных сторон, национальную нормативно-правовую базу, региональные и международные партнерские связи страны, а также различные риски, с которыми сталкивается страна в условиях меняющегося ландшафта киберугроз[151].

149 Документ SG2RGQ/175 ИК2 МСЭ-D, Соединенное Королевство.
150 Документ 2/172 ИК2 МСЭ-D, NRD Cyber Security (CS) (Литва).
151 Документ SG2RGQ/32 ИК2 МСЭ-D, Guardtime AS (Эстония).

Глава 6 – Как кибербезопасность может способствовать защите персональных данных

6.1 Введение

С развитием новых информационных технологий появляются все новые и все более удобные услуги для использования в повседневной жизни. В то же время появление новых информационных технологий также приводит к тому, что риски, с которыми сталкиваются отдельные лица в контексте обеспечения конфиденциальности и защиты данных, изменяются на двусторонней основе. Персональные данные подвергаются все новым и новым угрозам, однако есть несколько способов, как минимизировать такие риски или избежать их. Для этого необходимо уделять больше внимания кибербезопасности и технологиям, которые направлены на усиление конфиденциальности и могут помочь защитить персональные данные, таким как псевдонимизация и "проектируемая конфиденциальность".

Псевдонимизация – это процедура управления данными и деидентификации данных, с помощью которой поля персональной идентификационной информации в записи данных заменяются одним или несколькими искусственными идентификаторами или "псевдонимами". Использование одного псевдонима вместо каждого замененного поля или целого ряда замененных полей снижает вероятность идентификации лица по такой записи данных; при этом оставшаяся часть записи данных остается пригодной для анализа и обработки данных[152]. Псевдонимизация может способствовать защите персональных идентификационных данных и уменьшить нагрузку на организации, которые собирают и хранят такие данные.

При применении принципа "проектируемая конфиденциальность", для того чтобы принять меры по обеспечению безопасности, не ожидается совершение нарушения. Напротив, разработчики прогнозируют или предугадывают угрозу конфиденциальности, или предотвращают ее возникновение с помощью превентивных мер, таких как планирование или проектирование услуг[153]. Разница между двумя указанными выше подходами заключается в том, что псевдонимизация требует принятия определенных технических мер, в то время как принцип "проектируемая конфиденциальность" предоставляет операторам персональных данных свободу определения того, какие дополнительные технические меры могут наилучшим образом обеспечить безопасность и конфиденциальность данных.

6.2 Правовая база и передовой опыт Государств-Членов

В Бразилии в недавно принятом Общем законе о защите данных содержится определение различных типов персональных и текущих данных, определены правовые основания для обработки данных на внутреннем и международном уровнях и основные права субъектов данных, а также предусмотрено создание национального органа по защите данных[154]. Законом установлены принципы минимизации данных, предотвращения их утечки и обеспечения их безопасности, а также конкретные правила, регулирующие деятельность в соответствующих сферах. Закон также предусматривает применение принципа "проектируемая безопасность", в соответствии с которым меры безопасности, необходимые для защиты персональных данных, применяются, начиная с этапа разработки продукции или услуг и заканчивая их предоставлением.

В 2017 году Китай официально представил комплекс национальных стандартов по техническим характеристикам безопасности персональных данных на основе технологии информационной безопасности, которые дополняют требования по безопасности персональных данных, изложенные в Законе о кибербезопасности. Стандарты содержат руководящие указания и инструкции по эксплуатации. Китай продолжает исследования и разработку стандартов в области защиты персональных данных[155].

В Китае местные компании, осуществляющие деятельность по обеспечению безопасности данных, также активно исследуют и разрабатывают продукты и услуги в области безопасности, в том числе в области

---

152 Wikipedia, https://en.wikipedia.org/wiki/Pseudonymization.

153 Принцип "проектируемая конфиденциальность" использовался в существующей архитектуре, однако эта концепция носила вторичный характер. Широкое распространение этот принцип получил после того, как в середине 1990-х годов к нему обратилась д-р Анна Кавукян, Комиссар по вопросам информации и конфиденциальности провинции Онтарио (Канада).

154 Документ SG2RGQ/143 ИК2 МСЭ-D, Бразилия.

155 Документ 2/156 ИК2 МСЭ-D, Китай.

предотвращения потери данных, аудита безопасности баз данных, сканирования баз данных на предмет утечки данных, шифрования баз данных и маскирования данных, в целях предоставления технической поддержки в сфере защиты персональных данных.

Республика Корея внесла существенную поправку в свой Закон о защите персональных данных, которая предусматривает принятие технических мер для защиты персональных данных[156]. Данная поправка включала в себя изменения, направленные на упорядочение нормативного надзора и введение понятия "псевдонимизированных данных", что позволяет диспетчерам и операторам обработки данных осуществлять обработку данных более безопасным образом, сводя при этом к минимуму риск ненадлежащего использования и утечки данных за счет принятия других технологических и организационных мер, таких как "проектируемая защита персональных данных" и "защита персональных данных по умолчанию".

Кроме того, правительство Республики Корея опубликовало руководящие указания для защиты персональных данных при их автоматической обработке. Несмотря на то, что новые технологии, такие как анализ больших данных на основе применения ИИ и датчики, используемые в устройствах IoT для сбора данных, делают предоставление инновационных услуг возможным, понимание потока обработки персональных данных сталкивается с определенными трудностями, а принятие последующих мер реагирования – с определенными ограничениями. Согласно руководящим указаниям, при автоматической обработке персональных данных, полученных с устройств IoT, рекомендуется применять принцип "проектируемая конфиденциальность", в соответствие с которым возможность утечки персональных данных тщательно учитывается на протяжении всего жизненного цикла данных, начиная с самых первых действий на этапе планирования.

Этими руководящими указаниями предусмотрены следующие десять правил защиты персональных данных при их автоматической обработке:

- Этап планирования
  - Правило 1: подтверждение персональных данных, необходимых для предоставления услуг
  - Правило 2: подтверждение соблюдения правовых норм при сборе персональных данных
- Этап проектирования
  - Правило 3: минимизация данных и обработка только необходимых персональных данных
  - Правило 4: применение соответствующих мер безопасности на каждом этапе обработки персональных данных
  - Правило 5: прозрачное внедрение процедур и методов обработки персональных данных
  - Правило 6: установление гарантий того, что субъекты данных могут легко реализовывать свои права
  - Правило 7: четкие инструкции субъектам данных по предоставлению и передаче персональных данных третьим лицам
  - Правило 8: уничтожение персональных данных и предотвращение их дальнейшего сбора по окончании предоставление услуг субъектом данных
  - Правило 9: планы по гарантированию прав субъектов данных при прекращении бизнес-деятельности
- Этап оценки
  - Правило 10: изучение факторов риска, связанных с утечкой персональных данных до начала предоставления услуг.

Ввиду недавно возникшей необходимости отслеживать подтвержденные случаи COVID-19 по всему миру Республика Корея приняла различные институциональные и технические меры для защиты персональных данных. Помимо обеспечения правовой основы для отслеживания пациентов с подтвержденным диагнозом путем пересмотра соответствующих нормативных актов, принимаются технические меры по разделению данных и управлению идентификационной информацией в целях предотвращения возможной

[156] Документ 2/342 ИК2 МСЭ-D, Республика Корея.

утечки персональных данных. Отдельные данные используются для эпидемиологических исследований исключительно в случае подтверждения того или иного случая; при этом информация о пользователях и посетителях обрабатывается таким образом, который позволяет обеспечить ее безопасность, например путем автоматического уничтожения через четыре недели после того, как был проведен ее сбор[157].

Итальянская компания разработала и запатентовала методологию, которую организации могут без труда использовать для составления перечня технических мероприятий по приведению облачной инфраструктуры (частной, общественной или гибридной) в соответствие с нормами конфиденциальности[158]. Данная методология, в том числе, предполагает разработку общих руководящих указаний, на основе которых Государства-Члены могли бы создать национальных конфигураторов для обеспечения более эффективной и приемлемой в ценовом отношении стандартизации с участием нескольких стран, используя технологию облачных вычислений в качестве мощной платформы для содействия стремительному развитию цифровой экономики.

Еще один пример передового опыта – это Статья 25 о "проектируемой защите персональных данных" и "защите персональных данных по умолчанию" GDPR, согласно которой "проектируемая конфиденциальность" признается как наиболее подходящий способ предупреждения рисков для защиты персональных данных, связанных с устройствами IoT, большими данными, ИИ и другими новыми технологиями. Принцип "проектируемая конфиденциальность" подразумевает принятие соответствующих организационных и технических мер для обеспечения безопасности и конфиденциальности персональных данных на протяжении всего жизненного цикла продуктов, услуг, приложений, а также бизнес-процедур и технических процедур организации. Технические меры могут включать, в частности, псевдонимизацию и минимизацию данных[159].

Управление Европейского союза по кибербезопасности (ENISA) представило восемь ключевых принципов содействия применению предприятиями принципа "проектируемая конфиденциальность" в целях изучения различных методов, стратегий и технических факторов защиты персональных данных[160].

---

157 Документ SG2RGQ/268 ИК2 МСЭ-D, Республика Корея.

158 Документ SG2RGQ/25 ИК2 МСЭ-D, Proge-Software (Италия).

159 Европейский союз, регламент Regulation (EU) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент защиты данных).

160 ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014.

Таблица 3: Восемь ключевых принципов применение принципа "проектируемая конфиденциальность"

	Принцип	Содержание
1	Минимизировать	Минимизация количества обрабатываемых персональных данных за счет обработки в соответствии с четко поставленными целями, направленными на снижение вероятности нарушения требований конфиденциальности
2	Скрыть	Скрыть передачу открытого текста при обработке персональных данных для предотвращения доступа извне
3	Разделить	Разделить и хранить отдельно различные персональные данные для предупреждения дискриминации отдельного лица в базе данных
4	Агрегировать	Агрегировать большие объемы обрабатываемых персональных данных, с тем чтобы свести к минимуму дискриминацию отдельных лиц, а также распределить результаты обработки данных по категориям, с тем чтобы сделать дискриминацию невозможной
5	Проинформировать	Информировать субъектов данных обо всем процессе обработки персональных данных, с тем чтобы обеспечить четкое понимание целей использования данных
6	Установить контроль	Установить контроль за использованием персональных данных. Субъекты данных должны понимать весь процесс обработки персональных данных и иметь возможность реализовать свои права в отношении неправомерного использования их персональных данных или уровней безопасности в соответствии с пятым принципом – "Проинформировать"
7	Обеспечить соблюдение	Внутренняя политика защиты персональных данных должна отражать правовые и систематические обязанности и должна быть реализована на практике
8	Продемонстрировать	Продемонстрировать выполнение правовых обязательств, в частности в отношении обеспечения эффективного внедрения политики защиты персональных данных и безотлагательного принятия мер в ответ на инциденты, связанные с утечкой данных

ENISA также внесло предложения о проведении различными заинтересованными сторонами мероприятий, направленных на обеспечение конфиденциальности и защиту данных. Управлением рекомендует лицам, ответственным за разработку политики, содействовать и поддерживать разработку новых стимулов для усовершенствования услуг по защите персональных данных, а также группам, занимающимся научно-исследовательской и опытно-конструкторской деятельностью, исследовать технические методы защиты персональных данных на основе междисциплинарного подхода и распространить результаты исследований через лиц, ответственных за разработку политики, и средства массовой информации. Наконец, управление рекомендует разработчикам программного обеспечения создать технологию, которая могла бы на интуитивном уровне осуществлять обновление свойств конфиденциальности и позволяла бы обеспечить защиту персональных данных в рамках общедоступных и совместно разработанных инфраструктурных проектов.

Федеральная торговая комиссия Соединенных Штатов Америки (FTC) придает особое значение практическим и процессуальным принципам обеспечения конфиденциальности, таким как "проектируемая конфиденциальность" и упрощенный выбор потребителя, а также материально-правовым и процессуальным принципам, таким как гарантированная прозрачность. Комиссия также делает акцент на защите конфиденциальности потребителей в контексте деятельности коммерческого предприятия, продукции и всех этапов развития услуг[161].

Управление по защите данных Испании (AEPD) опубликовало руководство по применению принципа "проектируемая конфиденциальность", в котором подчеркивается необходимость учитывать фактор конфиденциальности и принципы защиты данных с самого начала обработки каких бы то ни было данных. В руководстве также представлены основные принципы и стратегии обработки персональных данных[162].

---

161 FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy-makers, March 2012.

162 *Agencia Española Protección Datos (AEPD)*, A Guide to Privacy by Design, October 2019.

Таблица 4: Взаимосвязь между целями обеспечения конфиденциальности и принципами проектирования конфиденциальности

Цели обеспечения конфиденциальности	Принципы обеспечения конфиденциальности, ориентированные на данные	Принципы обеспечения конфиденциальности, ориентированные на процесс
Невозможность установления связи	Минимизировать, извлечь, разделить, скрыть	
Установить контроль		Установить контроль, обеспечить соблюдение, продемонстрировать
Прозрачность		Проинформировать

6.3 Извлеченные уроки и дальнейшие действия

Скорость кибератак, утечки данных и несанкционированного использования персональных данных растет в геометрической прогрессии. Сейчас как никогда важно понять права и обязанности отдельных лиц и организаций в отношении персональных данных; особенно это касается организаций, которые работают с информацией, позволяющей установить личность.

В этой главе представлен обзор правовых изменений и технических мер обеспечения кибербезопасности, которые были внедрены на территории Государств-Членов для защиты персональных данных. В ней также приведены примеры передовой практики, с тем чтобы помочь Государствам-Членам выполнять меняющиеся требования в отношении конфиденциальности данных, а также изложена роль технологий кибербезопасности в снижении рисков и содействии соблюдению установленных требований.

Изучив различные технологии кибербезопасности и передовой опыт, применяемые Государствами-Членами для защиты персональных данных, можно извлечь следующие уроки:

– институциональные механизмы псевдонимизации, применения принципа "проектируемая конфиденциальность" и принятия других технологических мер способствуют формированию более безопасной среды;

– предприятиям, которые собирают и используют персональные данные, необходимо предпринимать активные усилия по внедрению технических мер, направленных на обеспечение более основательной защиты персональных данных;

– различным заинтересованным сторонам, в том числе субъектам данных, гражданскому обществу, научно-педагогическому составу академических организаций и представителям промышленности, необходимо обсуждать использование технологий и прилагать усилия для повышения осведомленности и улучшения безопасности на коллективной основе.

Глава 7 – Будущее Вопроса

Кибербезопасность – это важный вопрос для всех заинтересованных сторон, включая правительства и потребителей. Проводимая МСЭ-D в этом отношении работа способствует повышению осведомленности о соответствующих рисках. Ввиду постоянного роста во всем мире масштабов установления соединений и использования интернета по-прежнему весьма важной является задача защиты потребителей и систем. Учитывая сохраняющуюся глобальную потребность в обмене информацией о методах обеспечения кибербезопасности, руководящий состав Группы Докладчика по Вопросу 3/2 2-й Исследовательской комиссии МСЭ-D считает, что Вопрос о кибербезопасности следует сохранить без изменений в следующем исследовательском цикле. Темы, рассмотренные в ходе данного исследовательского периода, не утратили своей актуальности и должны стать основой для дальнейших вкладов и работы в течение следующего исследовательского периода. Таким образом, общую структуру Вопроса следует сохранить без изменений: поскольку проблемы безопасности касаются всех технологий, Вопрос 3/2 по-прежнему применим ко всем новым и появляющимся технологиям, так как эти проблемы, в силу их характера, следует учитывать на этапе проектирования.

Annexes

Annex 1: List of contributions and liaison statements received on Question 3/2

Contributions on Question 3/2

Web	Received	Source	Title
2/407	2021-03-03	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/400	2021-03-01	United States	Update on Cyber Awareness Campaigns
2/385	2021-01-28	Bhutan	Survey findings on National Child Online Safety and Protection
RGQ2/278	2020-09-22	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs
RGQ2/268	2020-09-22	Republic of Korea	Protecting personal data in responding COVID-19 pandemic (Korea's experience)
RGQ2/261	2020-08-19	Togo	Draft text for Chapter 1 of the Final Report for Question 3/2- Update on the status of spam and malware, including mitigation responses
RGQ2/241	2020-08-26	United Kingdom	Updated case study on securing consumer Internet of Things (IoT) devices in UK
RGQ2/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme
RGQ2/234	2020-08-20	United Kingdom	UK case study- reporting service for phishing emails
RGQ2/216	2020-07-27	Brazil	Brazilian National Cybersecurity Strategy (E-Ciber)
RGQ2/215	2020-07-27	Brazil	#SafeConnection (#ConexãoSegura) Awareness Campaigns
RGQ2/214	2020-07-27	Brazil	Brazilian National Cyberdrill- Cyber Guardian Exercise
2/344	2020-02-11	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/342	2020-02-11	Republic of Korea	Korea's major amendment to data protection law and its implication
2/341	2020-02-11	Republic of Korea	Implementation plan for strengthening national cybersecurity of Korea
2/338	2020-02-11	Co-Rapporteur for Question 3/2	Draft table of contents (V1) for the Final Report of Q3/2
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility
2/328	2020-02-08	Deloitte (United States)	People with disabilities and the Internet of Things

(продолжение)

Web	Received	Source	Title
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo
2/322	2020-02-07	Welchman Keen (Singapore)	Enhancing capacity and capability for critical national infrastructure in the Pacific Island Nations
2/321	2020-01-08	Sudan	WSIS project for consideration by Question 3/2
2/305	2020-01-15	Mexico	Perception on security and trust from Mexican users on fixed and/or mobile Internet
2/287	2020-01-07	China	Forum on network security technology development and international cooperation
2/286	2020-01-07	China	National Network Security Publicity Week and network security industrial park
2/272	2020-01-02	Niger	Cybersecurity best practices: case study and recommendation
2/264	2019-12-27	Russian Federation	Protecting children from information harmful to their health and development. Experience of the Russian Federation
RGQ2/TD/13 + Ann.1 (Rev.1)	2019-10-08	Forum of Incident Response and Security Teams (FIRST)	Introduction to incident response for policy makers
RGQ2/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills
RGQ2/179	2019-09-23	China	China's practice in protecting children's personal information
RGQ2/175	2019-09-19	United Kingdom	Follow up to "case study for the use of Active Cyber Defence on UK Government networks"
RGQ2/156 + Ann.1-3	2019-09-04	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
RGQ2/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK
RGQ2/153 + Ann.1-2	2019-08-22	United States	Enhancing the resilience of the Internet and communications ecosystem against botnets and other automated, distributed threats
RGQ2/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1
RGQ2/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus
RGQ2/143	2019-08-23	Brazil	The adoption of the Brazilian General Data Protection Law
RGQ2/135	2019-07-30	Bhutan	Cybersecurity initiatives in Bhutan
RGQ2/134	2019-07-29	State of Palestine, which participates in ITU under Resolution 99 (Rev. Dubai, 2018)	Government Data Exchange

(продолжение)

Web	Received	Source	Title
RGQ2/118	2019-06-21	Democratic Republic of the Congo	Securing information and communication networks: Best practices for developing a culture of cybersecurity
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire
2/199 (Rev.1)	2019-03-06	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combatting Cybercrime (PLCC)
2/172	2019-02-07	NRD Cyber Security (Lithuania)	National and sectorial CSIRT developments as means to strengthen cybersecurity environments, 2019 update
2/168	2019-02-07	Republic of Korea	2019 Comprehensive Cybersecurity Plan for the private sector
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies
2/165	2019-02-06	Mexico	Fixed and/or mobile Internet users' perception of cybersecurity
2/156	2019-02-05	China	Work experiences in personal information protection
2/155	2019-02-05	China	Design of evaluation index for network security capability
2/154	2019-02-05	China	Experience of Internet governance with the coordinated participation of the whole of society
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin
2/141	2019-01-15	Chad	Digital dividend
2/140	2019-01-15	Chad	Vulnerability of connected TVs
2/136	2019-01-15	Chad	Status of cybersecurity in the Republic of Chad
RGQ2/TD/1	2018-09-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for ITU members
RGQ2/79	2018-09-18	Bhutan	Challenges, issues and recommendations from Bhutan: developing country perspective
RGQ2/75	2018-09-18	Namibia	Enforcement of cyber security challenged by cloud services
RGQ2/55	2018-09-10	United Kingdom	Case study for the use of Active Cyber Defence on UK government networks
RGQ2/47	2018-08-31	BDT Focal Point for Question 3/2	Information on two publications issued in 2017: regional review of national activities on child online protection in Europe; and mobile identification: implementation, challenges, and opportunities
RGQ2/39 + Ann.1	2018-08-20	High-Tech Bridge SA (Switzerland)	Cybersecurity awareness and other educative activities to members

(продолжение)

Web	Received	Source	Title
RGQ2/32	2018-08-16	Guardtime AS (Estonia)	Towards cyber resilience- the role of national cyber exercises
RGQ2/30	2018-08-15	Brazil	Survey proposal
RGQ2/26	2018-08-14	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means of strengthen cybersecurity environments
RGQ2/25	2018-08-14	Proge-Software (Italy)	Data Privacy and Cloud.be compliant
2/91	2018-04-24	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States
2/84	2018-04-23	Japan	Proposal for workshops in 2018-2021 study period
2/82	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	KOVA Project: A best practice for COP implemented in Iran
2/75	2018-04-14	A.S. Popov Odessa National Academy of Telecommunications (Ukraine)	ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection. Conclusions and Recommendations
2/74	2018-04-13	Korea Telecom (Republic of Korea)	Study topics for Question 3/2 in the current study period
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities
2/66	2018-04-08	Algérie Télécom SPA (Algeria)	Proposals on the content of the (Question 3/2) final report
2/49	2018-03-15	Burundi	Current situation with regard to the Burundian Penal Code in relation to efforts to combat cybercrime
2/41	2018-02-28	Burundi	Cybersecurity, Internet Exchange point and e-commerce in Burundi

Incoming liaison statements for Question 3/2

Web	Received	Source	Title
RGQ2/242	2020-08-31	Council Working Group on Child Online Protection	Liaison statement from the Council Working Group on Child Online Protection (CWG-COP) to ITU-D SG2 on the outcome of the 15th and 16th Meetings of CWG-COP
RGQ2/174	2019-09-18	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on vulnerability of TVs
2/182 + Ann.1	2019-02-11	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D Study Group 2 Question 3/2 on Cybersecurity in Africa (overview and outlook), from Democratic Republic of Congo
RGQ2/62	2018-09-14	ITU-T Study Group 17	Liaison statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison representative with ITU-D Question 3/2
RGQ2/43	2018-08-27	ITU-T Study Group 13	Liaison statement from ITU-T SG13 to ITU-D SG1 Q3/1 and ITU-D SG2 Q3/2 on inter-sector coordination

(продолжение)

Web	Received	Source	Title
RGQ2/3	2018-05-11	ITU-T JCA-IMT2020	Liaison Statement from JCA-IMT2020 to ITU-D Study Groups 1 and 2 on invitation to update the information in the IMT2020 roadmap
2/73	2018-04-13	ITU-T JCA-AHF	Liaison Statement from ITU-T JCA-AHF to ITU-D Study Group 1 Q7/1 and Study Group 2 Q3/2 on JCA-AHF recent meeting reports
2/69	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on collaboration and liaison relationship with ITU-D Study Group 2 Question 3/2
2/68	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on best practices in Benin and Senegal
2/67 (Rev.1)	2018-04-09	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/62	2018-04-03	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on new work item X.framcdc "Framework of the creation and operation for a Cyber Defense Center"
2/46	2018-03-05	ITU-T JCA-IMT2020	Liaison Statement from ITU-T JCA-IMT2020 to ITU-D study groups on invitation to update the information in the IMT2020 roadmap
2/23	2017-11-24	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Question 3/2 on an ongoing work item on technical framework for countering telephone service scam
2/10	2017-11-22	ITU-T Study Group 20	Liaison Statement from ITU-T SG20 to ITU-D study groups on work on the combat of counterfeit ICT devices and mobile device theft

Annex 2: List of lessons learned received on Question 3/2

Web	Received	Source	Title
SG2RGQ/272	2020-09-22	United Kingdom	UK case study: Cyber resilience best practice for SMEs

The UK Government provides targeted support to small and medium-sized enterprises (SMEs) to help them navigate complicated standards to better understand how to mitigate cyberrisk. This support is designed specifically for organizations who are not aware of the cyberthreat and have limited resources, both financially and in terms of technical capability. Lessons learned include the following:

– Clear and consistent cyberrisk management messaging is crucial. Critically, **awareness campaigns** should not just explain *what* businesses need to do and *how* they can actually carry out the action by pointing to government advice, guidance and support, but should draw attention to ***why*** they should do it.

– **Advice and guidance** is most effective when it is non-technical, size-specific and easy to access. Government and law enforcement should use national, regional and local networks, and work in partnership with key industry bodies, to identify levers and business touchpoints that can be used to amplify messaging, and ensure advice and guidance reaching SMEs.

– The creation of a government-backed **certification scheme** can be an effective intervention to support SMEs to improve their cybersecurity. The certification scheme can:

  • be quickly and effectively delivered by a single supplier if the government can outline the technical controls and/or minimum standards that should be covered;

  • evolve to continue to meet the needs of SMEs and address the changing threat landscape;

  • better ensure organizations remain compliant through having a certification expiry date and requiring annual recertification.

Web	Received	Source	Title
SG2RGQ/235	2020-08-20	United Kingdom	UK Government Digital Service (GDS) Global Digital Marketplace Programme

Challenges

A range of interconnected challenges face governments in relation to traditional approaches to public procurement of ICTs, which is typically:

- neither understanding nor meeting the needs of users
- task oriented, risk averse and inflexible
- isolated from what happens:
  - 'before' (strategic planning, investment appraisals, early market engagement)
  - 'after' (service delivery, monitoring and evaluation, supplier relationship management)
- hidden from public scrutiny due to the poor quality, inconsistency, incompleteness and poor availability of data.

User-centred design approaches

Since GDS was established in 2011, it has incubated, embedded and mainstreamed new standards-based approaches to government transformation.

These approaches were first conceptualized by the Government Design Principles,[163] published in April 2012.

Since then, GDS and the government and UK public sector more broadly have been incrementally applying these principles to redesign and improve services, organizational structures, governance approaches, etc. This includes public procurement.

Social Purpose Digital Commissioning

Focus on culture, mindset, collaboration and capability, by:

- understanding users' needs
- being clear about the problems you are trying to overcome (e.g. legacy ICT, system vulnerabilities, capability and capacity, governance and accountability, etc.) to meet users' needs
- being outcome-oriented (rather than solution-oriented), experimental and flexible, making small incremental investments to try out different approaches to address users' problems, learning quickly and iteratively
- being multidisciplinary and collaborative coalition builders, advocating for systemic change through communities of practice
- engaging throughout the end-to-end lifecycle of delivery- the 'before' and 'after' of procurement
- being open to public scrutiny through deliberative participation of civil society, enabled by structured, quality, consistent, complete and published open data.

[163] UK Government. Guidance. Government Design Principles. April 2012.

Web	Received	Source	Title
SG2RGQ/215	2020-07-27	Brazil	#ConexãoSegura (#SafeConnection) Awareness Campaigns

The campaign around personal data protection on the Internet reinforced the importance of telling consumers how to protect themselves in the digital environment. The interactions of consumers on digital media and on the website revealed that many of them have a number of doubts about what is fraud or scam- especially when it involves cash prizes, in addition to not knowing what to do when they are victims of these situations. It is also important to advise people not to post or publish personal data (surprisingly many people do not know what can happen). In the next initiative, it would be interesting to expand the dissemination of materials further in order to reach a wider audience.

Web	Received	Source	Title
SG2RGQ/214	2020-07-27	Brazil	Brazilian National Cyberdrill- Cyber Guardian Exercise

The exercise started with two national critical infrastructure (NCI) sectors and evolved in its second edition to a broader and more complex exercise process. The exercise continues to evolve, and for its third edition (cancelled due to the COVID-19 pandemic) it was planned to include six NCI sectors and to add an international cooperation component to the exercise.

Web	Received	Source	Title
2/325	2020-02-08	Democratic Republic of the Congo	La sécurité numérique en République Démocratique du Congo

Turn cybersecurity in the Democratic Republic of the Congo into a lever for integration, protection, good governance, economic growth and social progress.

This vision will make a significant contribution to building the country's capacity in its digital transformation (circulation of information, data economy, growth economy, transparency and traceability, interoperability of information systems, etc.). It will allow digitalization to become a key driver for modernizing the State, promoting economic growth and fostering social progress.

Web	Received	Source	Title
2/336	2020-02-11	United Kingdom	Case study of best practices for securing customer Internet of Things in the UK

A significant proportion of IoT devices do not have basic cybersecurity features built into them. Following 18 months of collaboration with industry and experts at the UK's National Cyber Security Centre (NCSC), the Department for Digital, Culture, Media and Sport (DCMS) published the Code of Practice (CoP) for Consumer IoT Security in October 2018. The 13 voluntary guidelines, as outlined in the 2018 CoP, provide a much-needed baseline for IoT devices that manufacturers should embed into their products to make them 'secure by design'.

These include:

- No default passwords
- Implement a vulnerability disclosure policy
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure personal data are protected
- Make systems resilient to outages
- Monitor system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data.

These guidelines are outcome-focused as opposed to being prescriptive, which gives companies the space to come up with innovative solutions and appropriate ways to secure their products. Some devices might require enhanced security that is not included on this list and, as such, retailers and manufacturers are encouraged to secure their devices accordingly and seek solutions beyond the 13 guidelines. Action on the first three guidelines will bring largest security benefits in the short term.

Web	Received	Source	Title
2/331	2020-02-11	Keio University (Japan)	Proposed text for consideration of security issues for ICT accessibility

This document describes the consideration and implementation of cybersecurity measures for persons with disabilities, especially those with hearing difficulties, such as telecommunication relay service and remote captioning, to enhance accessibility to information and communication services.

Web	Received	Source	Title
SG2RGQ/134	2019-07-29	State of Palestine	Government Data Exchange

The central server issues certificates to security servers and provides a list of authenticated certificates to the systems connected to the Government Data Exchange. In addition, the central security server maintains encrypted activity data (hash logs) from the security servers to enable a series of e-service uses to be built subsequently, if necessary. If one of the parties to the service denies sending or receiving certain information, the service provider and user logs are compared with the encrypted copy in the central server. This method allows the integrity of security server logs to be checked, as it is impossible to change the log without it subsequently being detected.

The terms of the data-sharing process are defined by a memorandum of understanding signed by the two parties sharing the data and the Ministry of Telecommunications and Information Technology (MTIT), as third-party system operator. The memorandum includes an annex on the obligations of the parties, an annex on controls, standards and the duties and rights of each party, and an annex on the data which the two parties agree to share.

The system allows a connected ministry to determine which other connected institutions may access and read its data and the level of data that may be accessed. This is done by means of a control window on the ministry's own security server, enabling it to grant access rights to any of its services to the institutions it wishes.

Encrypted data are shared directly through secure servers from one information system to another. They do not pass through the central system and cannot be displayed there. The central system only has statistical information on the data shared.

Using this approach, the system facilitates the secure sharing of data between institutions, enabling them to share data between one another. It has also made it easier for the public to access services currently available G2G, by only going to one institution where the service involves more than one. MTIT is currently working to develop this mechanism and to provide services to the public directly via applications being developed.

Web	Received	Source	Title
SG2RGQ/146	2019-08-21	Senegal	Overview of the National Cybersecurity School with a regional focus

- Enhancing international cooperation, particularly between developed and developing countries.
- The school's regional nature helps to enhance cooperation among African countries.
- Covering all aspects of cybersecurity in both initial and continuing training.
- As cybersecurity is a prerequisite for the Digital Senegal 2025 Strategy (SN2025), classes have begun at the offices of the National School of Administration (ENA) while construction of the school's own premises is being completed at Diamniadio, 20 km from Dakar.
- The school will be the final element in the system for information system security and cybersecurity already in place.
- Boosting the fight against cybercrime in Africa.

Web	Received	Source	Title
SG2RGQ/151	2019-08-22	United States	NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1

The recent update process to develop Version 1.1 of the Framework demonstrates an example of a good process for stakeholder engagement to ensure the Framework remains a useful tool for managing cybersecurity risk.

Web	Received	Source	Title
SG2RGQ/155	2019-08-23	United Kingdom	Case study of best practices for ransomware risk mitigation in the UK

A recent advisory on ransomware from the National Cyber Security Centre (NCSC) recommends the following risk-mitigation techniques:

- Keep devices and networks up to date (e.g. prompt updating and patching, and regular scans)
- Prevent and detect lateral movement in your enterprise network
- Segment networks
- Set up a security monitoring capability
- Whitelist applications
- Use antivirus
- Back up files.

The full advisory and detailed list of recommendations can be found at:
https://www.ncsc.gov.uk/news/ongoing-threat-organisations-ransomware

Protecting your organization from ransomware:
https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Mitigating malware:
https://www.ncsc.gov.uk/guidance/mitigating-malware

Unfortunately, it is not a question of 'if' but 'when' a cyberattack will occur. In the event an attack does take place, cooperation between the public and private sectors is key to understanding the threat and coordinating a quick and effective response to mitigate the impact of an attack. In the event of an attack, organizations are advised to contact the National Crime Agency, NCSC's Cyber Incident Response, or Cyber Security Information Sharing Partnership (CiSP). NCSC led the UK's response to the WannaCry attack and worked in collaboration with the National Crime Agency (NCA). Over the course of an incident, NCSC publishes statements and guidance for large organizations as well as home users and small businesses. Up-to-date information is announced via the NCSC Twitter account (@NCSC).

Web	Received	Source	Title
SG2RGQ/196	2019-09-24	Silensec Africa Limited (Kenya)	Using cloud-based cyber ranges and competence frameworks for the delivery of cyber drills

This contribution recommends the use of cyberrange technology (cloud-based – public or private cloud) and competency frameworks in the development and delivery of new generation cyberdrills.

Web	Received	Source	Title
2/201	2019-03-08	Côte d'Ivoire	Survey of online activities and Internet use by children in Côte d'Ivoire

- De-dramatize prevention by banishing the anxiety-provoking approach. Internet prevention can be part of a fear culture. However, this increases the anxiety of parents who are already worried about a technology they do not understand well, thereby undermining the extraordinary learning tool that is the Internet.
- Encourage educational programmes aimed at developing best practices in content management and raising children's awareness of responsible use of the Internet.
- Put an Internet portal online in order to provide children, adolescents, parents and teachers with an educational base.
- Involve all stakeholders in community-awareness activities: government agencies, the private Internet sector, NGOs, community groups and the general public.

Web	Received	Source	Title
2/174	2019-02-07	Côte d'Ivoire	Mapping of cybercrime threats in Côte d'Ivoire

Statistics should be collected on complaints and damages (financial, moral).

Web	Received	Source	Title
2/173	2019-02-07	Côte d'Ivoire	Presentation of Platform for Combating Cyber-crime (PLCC)

- Development of partnerships between bodies responsible for combating cybercrime and the police in developing countries
- Awareness-raising in schools
- Collaboration with equivalent organizations in other countries.

Web	Received	Source	Title
SG2RGQ/26 2/172	2018-08-14 2019-02-07	NRD Cyber Security (Lithuania)	National and sectoral CSIRT developments as means to strengthen cybersecurity environments (2018 + 2019 update)

For national digital security success, CSIRTs should focus substantial energy on broad facilitation for developing additional independent capabilities – in industries, professional communities, education centres, research, events, meet-ups and conferences, private and internal CSIRTs.

Web	Received	Source	Title
2/167	2019-02-07	Symantec Corporation (United States)	The importance of cyber threat intelligence in the definition of national cybersecurity strategies

- Establish and adopt situation awareness and threat intelligence policies.
- Develop incident analysis and response capabilities- establish CERTs.
- Develop collaboration with the private sector and information-sharing policies (public-private partnerships).

Web	Received	Source	Title
2/152	2019-02-01	Benin	Cybersecurity in the era of the digital economy in Benin

Benin calls on ITU-D Study Group 2 to support:

- the establishment of a national CERT in Benin to enhance the level of trust in cyberspace;
- the building up of a common African security and defence policy;
- the creation of a panel of eminent personalities to reflect on Africa's role in regard to security;
- the establishment of a CERT-AFR (for Africa) along the lines of CERT-EU (for the European Union);
- a coordinated effort to avoid disparities between the strategies adopted and means deployed by Member States in terms of military cyberdefence capabilities;
- regulators and ICT authorities as they seek to:
  - adopt measures designed to enhance the security of information systems and networks;
  - create reliable digital identities;
  - protect minors and vulnerable groups; and
  - foster transparency.

Web	Received	Source	Title
SG2RGQ/25	2018-08-14	Proge-Software [*SME pilot*] (Italy)	Data Privacy and Cloud- be compliant

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) (EU) 2016/679 governs data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying regulation within the EU. Superseding Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personally identifiable information (personal data) of individuals (formally called data subjects in the GDPR) inside the European Union, and applies to an enterprise that is established in the EU or – regardless of its location and the data subjects' citizenship – that is processing the personal data of people inside the EU. Controllers of personal data must put in place appropriate technical and organizational measures to implement the data-protection principles. Severe penalties are applied to violators.

Cloud computing

In computer science, cloud computing describes a type of outsourcing of computer services, similar to the way in which electricity supply is outsourced. Users can simply use it. They do not need to worry where the electricity is from, how it is made, or how it is transported. Periodically they pay for what they have consumed. The idea behind cloud computing is similar: The user can simply use storage, computing power or specially crafted development environments without having to worry how these work internally. Cloud computing is usually Internet-based computing. According to a paper published by IEEE Internet Computing in 2008, "*Cloud computing is a paradigm in which information is permanently stored in servers on the Internet and cached temporarily on clients that include computers, laptops, handhelds, sensors, etc.*".

Web	Received	Source	Title
SG2RGQ/32	2018-08-16	Guardtime AS [*SME pilot*] (Estonia)	Towards cyber resilience – the role of national cyber exercises

Cyberexercises are essential to achieving sustainable cyberresilience. Cyberexercises are different from training, and must be customized, realistic and engaging. Governments should consider developing a programme to govern cyberresilience, covering education, training and cyberexercises ranging from localized events to customized national-scale exercises conducted on a regular basis.

Web	Received	Source	Title
2/71	2018-04-11	G3ict	Spammers and phishers who target persons with disabilities

1 Contact the service provider to inform it of the highjacking of your e-mail address.

2 Try to give information on the spammer's/hacker's contact details with an example e-mail, e.g. by forwarding the suspect e-mail to its fraud section.

3 Ask to have your violated e-mail blocked.

4 Change your e-mail address.

5 Let your friends and contacts know you have been hacked and give them the new address.

6 Do not click on any web addresses unless you have verified it is in fact from a known source.

Web	Received	Source	Title
2/41	2018-02-28	Burundi	Cybersecurity, Internet exchange point and e-commerce in Burundi

Security of IT data and of communication networks in order to ensure high-quality services is the pillar of ICT-sector development. A legal and regulatory framework for cybersecurity in our country is an essential tool for implementing all aspects of data security. The introduction of an Internet exchange point facilitates local communications and reduces latency times and associated costs. Lastly, domain name management provides facilities for investors. Data security will thus enable us to ensure reliable e-transactions and retain our customers.

Канцелярия Директора
Международный союз электросвязи (МСЭ)
Бюро развития электросвязи (БРЭ)
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: bdtdirector@itu.int
Тел.: +41 22 730 5035/5435
Факс: +41 22 730 5484

Канцелярия заместителя Директора и региональное присутствие
Департамент координации операций на местах (DDR)
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: bdtdeputydir@itu.int
Тел.: +41 22 730 5131
Факс: +41 22 730 5484

Департамент цифровых сетей и цифрового общества (DNS)

Эл. почта: bdt-dns@itu.int
Тел.: +41 22 730 5421
Факс: +41 22 730 5484

Департамент центра цифровых знаний (DKH)

Эл. почта: bdt-dkh@itu.int
Тел.: +41 22 730 5900
Факс: +41 22 730 5484

Департамент партнерских отношений в интересах цифрового развития (PDD)

Эл. почта: bdt-pdd@itu.int
Тел.: +41 22 730 5447
Факс: +41 22 730 5484

Африка

Эфиопия

Региональное отделение МСЭ
Gambia Road
Leghar Ethio Telecom Bldg., 3rd floor
P.O. Box 60 005
Addis Ababa – Ethiopia

Эл. почта: itu-ro-africa@itu.int
Тел.: +251 11 551 4977
Тел.: +251 11 551 4855
Тел.: +251 11 551 8328
Факс: +251 11 551 7299

Камерун

Зональное отделение МСЭ
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Эл. почта: itu-yaounde@itu.int
Тел.: + 237 22 22 9292
Тел.: + 237 22 22 9291
Факс: + 237 22 22 9297

Сенегал

Зональное отделение МСЭ
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar – Yoff – Senegal

Эл. почта: itu-dakar@itu.int
Тел.: +221 33 859 7010
Тел.: +221 33 859 7021
Факс: +221 33 868 6386

Зимбабве

Зональное отделение МСЭ
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare – Zimbabwe

Эл. почта: itu-harare@itu.int
Тел.: +263 4 77 5939
Тел.: +263 4 77 5941
Факс: +263 4 77 1257

Северная и Южная Америка

Бразилия

Региональное отделение МСЭ
SAUS Quadra 6 Ed. Luis Eduardo
Magalhães
Bloco E, 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia – DF – Brazil

Эл. почта: itubrasilia@itu.int
Тел.: +55 61 2312 2730-1
Тел.: +55 61 2312 2733-5
Факс: +55 61 2312 2738

Барбадос

Зональное отделение МСЭ
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Эл. почта: itubridgetown@itu.int
Тел.: +1 246 431 0343
Факс: +1 246 437 7403

Чили

Зональное отделение МСЭ
Merced 753, Piso 4
Santiago de Chile – Chile

Эл. почта: itusantiago@itu.int
Тел.: +56 2 632 6134/6147
Факс: +56 2 632 6154

Гондурас

Зональное отделение МСЭ
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa – Honduras

Эл. почта: itutegucigalpa@itu.int
Тел.: +504 2235 5470
Факс: +504 2235 5471

Арабские государства

Египет

Региональное отделение МСЭ
Smart Village, Building B 147
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo – Egypt

Эл. почта: itu-ro-arabstates@itu.int
Тел.: +202 3537 1777
Факс: +202 3537 1888

Азиатско-Тихоокеанский регион

Таиланд

Региональное отделение МСЭ
Thailand Post Training Center
5th floor
111, Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

Эл. почта: ituasiapacificregion@itu.int
Тел.: +66 2 575 0055
Факс: +66 2 575 3507

Индонезия

Зональное отделение МСЭ
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110 – Indonesia

Эл. почта: ituasiapacificregion@itu.int
Тел.: +62 21 381 3572
Тел.: +62 21 380 2322/2324
Факс: +62 21 389 5521

СНГ

Российская Федерация

Региональное отделение МСЭ
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Эл. почта: itumoscow@itu.int
Тел.: +7 495 926 6070

Европа

Швейцария

Отделение для Европы МСЭ
Place des Nations
CH-1211 Geneva 20 – Switzerland

Эл. почта: eurregion@itu.int
Тел.: +41 22 730 5467
Факс: +41 22 730 5484

Международный союз электросвязи
Бюро развития электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-34104-6

Опубликовано в Швейцарии
Женева, 2021 г.