№4
октябрь 2016

MSK IX

Интернет изнутри

Критическая инфраструктура

Согласованная Директива ЕС по кибербезопасности
Введение в рамках Европейского Союза специальных законов, регулирующих эту область, представляется очень важным.

Содержание:

Иформационный сборник «Интернет изнутри»

По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №4, дата выхода: октябрь 2016 г.

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Дизайн:
Чернега Наталья

Телефон, телеграф, мосты...

главный редактор,
Андрей Робачевский

Дорогой читатель!

Этот номер посвящен критической инфраструктуре Интернета. Эта тема содержит много ловушек, связанных с субъективностью понятия и неясностью терминологии. Насколько "критичен" тот или иной элемент? В чем различие критической информационной инфраструктуры и информационной инфраструктуры, поддерживающей критические отрасли?

Тем не менее, ясно, что Интернет все более плотно вплетается в нашу жизнь, что безотказность информационных услуг все более значима, что всеобщая связность открывает фантастические возможности, но создает критические зависимости.

Телефон, телеграф, железнодорожные станции, мосты... Когда мы говорим о критической информационной инфраструктуре, выделить эти компоненты гораздо сложнее. Во-первых, из-за зависимостей, порой неочевидных на первый взгляд. Например, доступность корпоративного DNS-резолвера может быть более значимой, чем доступность корневого сервера. Во-вторых, устойчивость и отсутствие критических элементов, представляющих единые точки отказа, заложена в саму архитектуру Интернета.

Мы пригласили ведущих российских и зарубежных экспертов поделиться своими взглядами на эти вопросы. В качестве формата обсуждения мы выбрали "круглый стол", виртуальный, разумеется, в духе нашего издания.

На протяжении нескольких лет Европейское агентство по сетевой и информационной безопасности ENISA ведет работу по сбору передового опыта и национальных практик для определения и защиты критических элементов информационной инфраструктуры. С некоторыми результатами этой работы мы познакомим вас в этом номере. Здесь вы также найдете анализ европейской Директивы по сетевой и информационной безопасности (NIS), недавно одобренной Европарламентом.

Чтобы номер не получился совсем нетехническим, мы оставили место и для технологических вопросов. В следующем году в Интернете произойдет весьма критическое изменение - замена основного ключа корневой зоны DNS. О том, как произойдет замена и какие проблемы предстоит решить - в статье Джеффа Хьюстона "Замена в корневой зоне".

А в качестве десерта мы предлагаем ставшие традиционными разделы "Путевые заметки" и "Ученые шутят", где вы сможете познакомиться с миром встреч и конференций глазами Ольги Александровой-Мясиной и порадоваться поучительной басне Леонида Тодорова.

Итак, перед вами четвертый выпуск. Надеемся, что он вам покажется полезным и интересным. Расскажите нам, что вам понравилось, а что – нет, о чем бы вы хотели прочитать в следующих номерах. Как всегда, ждем ваших отзывов и предложений по адресу info@internetinside.ru.

Проблемы правового обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Стрельцов А.А.

(Заместитель директора Института проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова, доктор технических наук, доктор юридических наук , профессор)

Обеспечение безопасности критической информационной инфраструктуры (КИИ) является одним из важных условий удовлетворения законных интересов граждан, устойчивого функционирования всех сфер жизни современного общества, обороноспособности страны и безопасности государства[1]. Существенная роль в формировании данного условия принадлежит нормативному правовому регулированию общественных отношений в области противодействия угрозам нарушения безопасности КИИ посредством злонамеренного использования против объектов КИИ информационно-коммуникационных технологий (ИКТ).

Исследованию способов и методов использования права для противодействия угрозам безопасности инфраструктуры общества, в том числе и КИИ, посвящено значительное количество работ как отечественных, так и зарубежных специалистов[2]. В Российской Федерации совершенствование нормативного правового обеспечения безопасности КИИ осуществляется в рамках реализации целей и задач государственной политики[3].

В настоящей статье обсуждается ряд проблем развития правового обеспечения безопасности КИИ как важного фактора обеспечения безопасности России[4].

Основные составляющие правового обеспечения безопасности КИИ

Понятие «КИИ» появилось сравнительно недавно и в Российской Федерации раскрывается как «совокупность автоматизированных систем управления производственными и технологическими процессами (АСУ) критически важных объектов инфраструктуры (КВО) Российской Федерации и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей (ИКС), предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий»[5].

В составе КИИ можно выделить информационную и телекоммуникационную среды.

- Информационная среда КИИ представляет собой совокупность вычислительных и информационных ресурсов, образующих АСУ КВО. При этом вычислительные ресурсы образуются совокупностью локальных вычислительных сетей, иных средств вычислительной техники и программных средств, описывающих методы и способы автоматизации обработки информации, и могут быть использованы для организации распределенных вычислений (например, для дешифровки зашифрованного кода, моделирования сложных социальных и физических процессов).

- Телекоммуникационная среда КИИ образуется совокупностью телекоммуникационных устройств; линий связи и каналообразующего оборудования; систем открытых протоколов обмена информацией между телекоммуникационными устройствами; глобальной системы цифровых адресов и доменных имен (цифровых идентификаторов); программного обеспечения, реализующего методы, алгоритмы и процессы телекоммуникационной связи на базе протоколов взаимодействия локальных вычислительных сетей и предоставляющего доступ к локальным вычислительным сетям и иным средствам автоматизированной обработки информации.

Основу телекоммуникационной составляющей КИИ составляют национальные сети электросвязи и сеть Интернет.

Сети электросвязи являются технологической системой, включающей в себя средства связи и линии связи[6]. Сети электросвязи для оказания услуг связи используют радиочастотный спектр и ресурс нумерации единой сети электросвязи, регулирование которых является исключительным правом Российской Федерации[7].

Сеть Интернет может рассматриваться в качестве технологической надстройки над сетью электросвязи, обеспечивающей оказание ус-

луг передачи и обработки информации (например, электронная почта, телеконференции, передача файлов, доступ к вычислительным и информационным ресурсам (системам) в локальных вычислительных сетях). Оказание услуг передачи и обработки информации, иных информационных услуг в сети Интернет осуществляется в пространстве цифровых адресов или доменных имен (разновидности «электронных» (цифровых) идентификаторов объектов коммуникации). Регулирование отношений в области распределения цифровых идентификаторов и поддержания их в актуальном состоянии осуществляется вне территории Российской Федерации. Соответственно, использование цифровых идентификаторов объектов сети Интернет, а также обеспечение безопасности процесса их использования осуществляется на основе международного правового регулирования.

Исходя из того, что основную угрозу безопасности АСУ КВО и ИКС составляют целенаправленные воздействия на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, правовое обеспечение безопасности КИИ должно включать две основные составляющие – национальную и международную[8].

Национальная составляющая правового обеспечения безопасности КИИ образуется совокупностью принципов, правовых институтов и норм, закрепленных национальным законодательством и регулирующих в рамках национальной юрисдикции отношения в области противодействия угрозам безопасности АСУ КВО и ИКС.

Международная составляющая правового обеспечения безопасности КИИ образуется совокупностью принципов и норм, закреплённых в признаваемых Российской Федерацией международных договорах и регулирующих вопросы международного сотрудничества государств в рассматриваемой области.

Национальная составляющая правового обеспечения безопасности КИИ

Общественные отношения в области обеспечения безопасности АСУ КВО и ИКС, обеспечивающих взаимодействие этих объектов, регулируются, прежде всего, отраслевым федеральным законодательством.

Так, в федеральных законах, регулирующих отношения в области защиты населения и территорий от чрезвычайных ситуаций, в том числе технологического характера[9], обеспечения безопасности использования объектов атомной энергетики[10], гидротехнических сооружений[11], объектов промышленности[12], объектов транспортной инфраструктуры[13], объектов топливно-энергетического комплекса[14] , сетей связи[15], ИКТ и информационных систем и ответственности операторов информационных систем за несоблюдение правил обеспечения их безопасности[16], предупреждения создания опасных информационных технологий и преодоления средств защиты информации[17], закреплено понятие «критически важный объект», а также принципы и нормы, регулирующие отношения в области обеспечения безопасности КВО.

В то же время реализация положений государственной политики в области обеспечения безопасности КИИ требует дальнейшего развития правовых принципов и норм, регулирующих соответствующие общественные отношения, т.е. национальной составляющей правового обеспечения безопасности КИИ.

В этой связи приоритетного внимания заслуживают следующие сложные проблемы:

- установление разрешительного порядка (лицензирование) деятельности в области обеспечения безопасности АСУ и КВО ИКС;
- развитие системы сертификации устройств и систем, составляющих КИИ;
- организация взаимодействия субъектов системы обеспечения безопасности КИИ в рамках государственной системы обнаружения и предупреждения компьютерных атак на объектах КИИ;
- расширение участия государства в оперативном управлении сетями связи общего пользования в целях минимизации последствий атак на ИКС КИИ.

Установление лицензирования деятельности в области обеспечения безопасности АСУ КВО и ИКС потребует определенного развития отраслевого законодательства.

Законодательством в области связи установлено, что деятельность юридических лиц и индивидуальных предпринимателей по возмездному оказанию услуг связи, с использованием сетей электросвязи, в том числе применяемых в ИКС, осуществляется только на основании лицензии.

Предусмотрена возможность предъявления требований к сетям связи по построению, управлению или нумерации, применяемым средствам связи, организационно-техническому обеспечению устойчивого функционирования сетей связи, в том числе в чрезвычайных ситуациях, защиты сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации[18].

С этой точки зрения для выполнения положений государственной политики содержание лицензий по оказанию операторами сетей связи общего пользования услуг связи, связанных с обеспечением функционирования ИКС для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, может быть несколько расширено.

В меньшей степени урегулированы правом отношения в области лицензирования деятельности субъектов обеспечения безопасности АСУ КВО.

В настоящее время лицензирование деятельности в области обеспечения безопасности КВО используется в ограниченных масштабах.

Так, в области использования атомной энергии предусмотрено, что органы государственного регулирования в области безопасности выдают эксплуатирующим организациям, а также организациям, выполняющим работы и предоставляющим услуги в данной области, разрешения (лицензии) на право ведения работ в области использования атомной энергии[19], а также в области обеспечения промышленной безопасности[20].

В остальных случаях обеспечение безопасности КВО осуществляется посредством установления критериев отнесения объектов инфраструктуры к КВО, определения порядка формирования и утверждения перечня таких объектов, разработки паспорта безопасности таких объектов, а также обязательных для выполнения требований

к КВО в области защиты населения и территорий от чрезвычайных ситуаций. В целях предупреждения возникновения и развития чрезвычайных ситуаций, снижения размеров ущерба и потерь от чрезвычайных ситуаций, организации ликвидации чрезвычайных ситуаций право выполнения перечисленных функций предоставлено правительству Российской Федерации[21].

Создание системы лицензирования деятельности в области обеспечения безопасности АСУ КВО потребует введения существенных правовых новаций, включая раскрытие понятия «автоматизированная система управления производственными и технологическими процессами» как самостоятельного объекта правовых отношений, порядка определения ее структуры и состава, отношения к КВО, определения содержания деятельности по обеспечению безопасности АСУ, требований к физическим и юридическим лицам, допускаемым к ее осуществлению. Необходимо будет установить порядок предоставления лицензии, определения срока ее действия, отказа в выдаче лицензии, ее переоформления, внесения дополнений и изменений, приостановления и возобновления деятельности, аннулирования лицензии, формирования и ведения реестра лицензий.

Весьма широкая трактовка понятия КИИ делает важным аспектом проблемы развития правового обеспечения безопасности данной инфраструктуры закрепление правового механизма идентификации объектов, систем и устройств, относящихся к КИИ.

Сертификация устройств и систем, составляющих АСУ КВО и ИКС, рассматривается в качестве важного средства снижения опасности проявления угроз безопасности КИИ. Законодательством о связи для обеспечения целостности, устойчивости функционирования и безопасности установлено обязательное подтверждение соответствия установленным требованиям средств связи сети связи общего пользования[22]. Подтверждение соответствия средств связи осуществляется на соответствие техническому регламенту и требованиям, предусмотренным нормативными правовыми актами федерального органа исполнительной власти в области связи. Подтверждение может осуществляться посредством обязательной сертификации или принятия декларации о соответствии. Для проведения обязательной сертификации средства связи предоставляются изготовителем или продавцом.

Сертификация других средств и устройств АСУ КВО и ИКС законодательством об информационных технологиях[23] и отраслевым законодательством не предусмотрена. Для формирования системы сертификации таких систем и устройств потребуется определение признаков их отнесения к АСУ КВО и ИКС, принятие технических регламентов, устанавливающих требования по безопасности использования рассматриваемых средств и устройств, а также создание системы сертифицирующих организаций.

Регулирование отношений в области взаимодействия субъектов системы обеспечения безопасности КИИ в рамках государственной системы обнаружения и предупреждения компьютерных атак на объектах КИИ в настоящее время урегулированы президентом Российской Федерации в части, касающейся задач данной системы и функций Федеральной службы безопасности Российской Федерации[24].

Определено, что данная государственная система представляет собой централизованную, иерархическую, территориально распределенную структуру, включающую силы и средства обнаружения и предупреждения компьютерных атак, а также органы управления различных уровней, в полномочия которых входят вопросы обеспечения безопасности автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры.

В рамках развития правового обеспечения включения элементов КИИ в государственную систему обнаружения и предупреждения компьютерных атак должны быть закреплены механизмы формирования перечней объектов КИИ, структуры и полномочий указанных органов управления, порядок развертывания средств обнаружения и предупреждения компьютерных атак и источники финансирования данных работ, а также взаимодействия между уполномоченным федеральным органом исполнительной власти в области безопасности и другими субъектами сил обнаружения, предупреждения и ликвидации последствий компьютерных атак на элементы КИИ и компьютерных инцидентов. Взаимодействие субъектов сил обнаружения, предупреждения и ликвидации последствий компьютерных атак может базироваться на принципе сочетания интересов и взаимной ответственности государства, граждан, а также организаций, участвующих в разработке, создании и эксплуатации автоматизированных систем управления КВО[25].

Представляется важным сформировать механизм установления и поддержания баланса интересов уполномоченных федеральных органов исполнительной власти и частного сектора, гражданского общества, представленного, прежде всего, экспертным сообществом, в решении проблем обеспечения безопасности КИИ, выработке и реализации рекомендаций по противодействию угрозам безопасности объектов информационной инфраструктуры.

Кроме того, важно законодательно уточнить понятие «компьютерный инцидент». Раскрытие данного понятия как «факт нарушения штатного режима функционирования элемента критической информационной инфраструктуры или критической информационной инфраструктуры в целом» недостаточно для осуществления эффективной правоприменительной практики в данной области. Для этого, как минимум, должны быть закреплены юридические факты, порождающие, изменяющие или прекращающие правоотношения в области обнаружения и предупреждения компьютерных атак, мониторинга уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов. Исходя из того, что нарушения штатного режима функционирования АСУ КВО могут быть следствием как ошибок в работе ее систем и устройств, так и целенаправленного воздействия на АСУ, важно учитывать причины возникновения нарушений.

Отношения в области участия государства в оперативном управлении сетями связи общего пользования в целях минимизации последствий атак на КИИ в основном урегулированы законодательством в области связи. Предусмотрено, что такое управление со стороны федерального органа исполнительной власти в области связи может осуществляться в чрезвычайных ситуациях во взаимодействии с центрами управления сетями связи специального назначения и имеющими присоединение к сетям связи общего пользования

и технологическим сетям связи.

Других случаев участия государства в оперативном управлении сетями связи общего пользования не предусмотрено.

С другой стороны, без такого участия представляется весьма затруднительным обеспечить «создание правовых оснований и определение порядка применения мер принудительного изменения информационного обмена с объектами информатизации, являющимися источниками компьютерных атак, вплоть до его полного прекращения»[26].

Для устранения данного пробела в законодательстве необходимо обеспечить дальнейшее развитие механизмов взаимодействия уполномоченных федеральных органов исполнительной власти и операторов связи.

Международная составляющая правового обеспечения безопасности КИИ

С учетом основных задач развития системы международной информационной безопасности, определенных президентом Российской Федерации[27], можно выделить следующие основные группы международных отношений, требующих нормативного правового регулирования в рамках правового обеспечения безопасности КИИ:

- определение границ национальной КИИ в глобальной информационно-коммуникационной инфраструктуре;
- закрепление признаков компьютерных инцидентов в автоматизированных системах управления КВО;
- международное сотрудничество в области ликвидации последствий компьютерных инцидентов в КВО.

Актуальность проблемы определения границ национального сегмента глобальной информационно-коммуникационной инфраструктуры обусловлена, с одной стороны, невозможностью установления устойчивой привязки цифровых идентификаторов объектов информационной инфраструктуры к национальной территории, а, с другой – необходимостью общепризнанного международного закрепления национальных пределов государственного суверенитета и, соответственно, государственной юрисдикции в пространстве объектов информационной инфраструктуры. Отсутствие общепризнанных пределов государственного суверенитета государств в этом пространстве является существенными препятствием для применения принципов и норм международного права к действиям государств в ИКТ-среде. В частности, это препятствует установлению границ ответственности государств за безопасность сегментов информационной инфраструктуры, за предотвращение их использования для распространения так называемого «информационного оружия», за организацию международного сотрудничества в области противодействия компьютерной преступности и территориям, а также решению некоторых других вопросов.

Как известно, выделение цифровых идентификаторов объектов сети Интернет национальным провайдерам, а также поддержание в актуальном состоянии соответствующих информационных систем IP-адресов и доменных имен осуществляется американской некоммерческой организацией ICANN и некоммерческими организациями RIR, зарегистрированными в разных государствах мира. Данные организации не являются субъектами международного права и не обладают международной правоспособностью, дееспособностью и деликтоспособностью. С этой точки зрения, они не могут гарантировать устойчивость выполнения выделенных функций в условиях значительной динамики международных отношений. Ни одно государство или международная организация не взяли на себя международных правовых обязательств по обеспечению устойчивости и безопасности функционирования системы цифровых идентификаторов глобальной информационной инфраструктуры. Все это вместе создает определенные риски нарушения устойчивости функционирования глобальной информационной инфраструктуры.

Делимитация национальных границ в ИКТ-среде не имеет целью осуществление дефрагментации этого пространства на совокупность изолированных национальных сегментов. Делимитация направлена на создание условий для реализации рекомендаций Группы правительственных экспертов ООН, направленных на предотвращение возникновения угроз международному миру и безопасности вследствие злонамеренного использования ИКТ. Эти рекомендации были рассмотрены и приняты к сведению Генеральной Ассамблеей ООН[28]. Так, Группа правительственных экспертов ООН полагает, что :

государственный суверенитет и государственная юрисдикция являются основой системы защиты национальных интересов, обеспечения национальной безопасности, противодействия угрозе злонамеренного и враждебного использования ИКТ против прав и свобод граждан, интересов общества и государства, нарушения международного мира и безопасности;

государства несут главную ответственность за обеспечение государственной безопасности и безопасности своих граждан, в том числе в ИКТ-среде.

Без установления пространственных пределов государственного суверенитета в ИКТ-среде вообще и в сети Интернет в частности, возложение такой ответственности на государства не представляется возможным.

Определение признаков компьютерных инцидентов в автоматизированных системах управления КВО международного характера является необходимым условием организации международного сотрудничества в области безопасности КИИ. Вообще говоря, в международном праве понятие «инцидент» применяется достаточно широко. Так, понятие «инцидент (международный инцидент)» обычно раскрывается как небольшие или ограниченные действия или авария, результатом которых стал широкий обмен мнениями между двумя или более национальными государствами.

Инцидент в киберпространстве, как правило, связан с нарушением функционирования составляющих киберпространства - электронной среды сбора и автоматизированной обработки информации,

ИКТ, определяющих процессы осуществления данных операций, а также информационных систем и систем автоматизированного управления.

Общий контекст «международного инцидента» в сфере ИКТ будет определяться, прежде всего, характером международных отношений между государствами, затронутыми «инцидентом». Данное событие может являться результатом непредвиденных действий государства в сфере ИКТ, наносящих ущерб интересам человека, государственных органов или вооруженных сил одного или более государств, или, наоборот, являться одним из многих преднамеренных, но незначительных провокаций, осуществляемых агентами одного государства против другого государства.

Учитывая, что международные отношения в области инцидентов в сфере ИКТ не регулируются международными договорами, основным и, по существу, единственным источником международного права в рассматриваемом случае служит международный обычай, однако его применение к сфере ИКТ сопряжено со значительными сложностями.

Международное сотрудничество в области ликвидации последствий компьютерных инцидентов на КВО. Как правило, сотрудничество государств в области ликвидации неблагоприятных последствий тех или иных событий обусловливается, прежде всего, гуманитарными соображениями.

В этом случае в соответствии с принципами международного права государства обязаны, независимо от различий в их политических, экономических и социальных системах, сотрудничать друг с другом в различных областях международных отношений с целью поддержания международного мира и безопасности и содействия международной экономической стабильности и прогрессу, общему благосостоянию народов и международному сотрудничеству, свободному от дискриминации, основанной на таких различиях.

В рамках международного сотрудничества в области ликвидации последствий компьютерных инцидентов на КВО государства могли бы взять на себя обязательства по оказанию помощи другим государствам в новой разновидности чрезвычайных ситуаций.

Заключение

Анализ проблемы совершенствования правового обеспечения безопасности КИИ позволяет сделать следующие основные выводы.

Во-первых, общественные отношения в области обеспечения безопасности КИИ в основном урегулированы законодательством (федеральные законы «О защите населения и территорий от чрезвычайных ситуаций...», «Об использовании атомной энергии», «О промышленной безопасности...», «О безопасности гидротехнических сооружений», «О транспортной безопасности», «О безопасности объектов топливно-энергетического комплекса» и некоторые другие).

Развитие правового обеспечения безопасности КИИ должно быть направлено на реализацию положений государственной политики Российской Федерации в данной области.

Правовое обеспечение безопасности КИИ включает национальную и международную составляющие.

Во-вторых, к числу важных проблем совершенствования национальной составляющей правового обеспечения безопасности КИИ относятся следующие:

- разрешительный порядок (лицензирование) деятельности в области обеспечения безопасности ИКС и АСУ КВО;
- сертификация устройств и систем, составляющих КИИ;

взаимодействие субъектов системы обеспечения безопасности КИИ в рамках государственной системы обнаружения и предупреждения компьютерных атак на объектах КИИ;

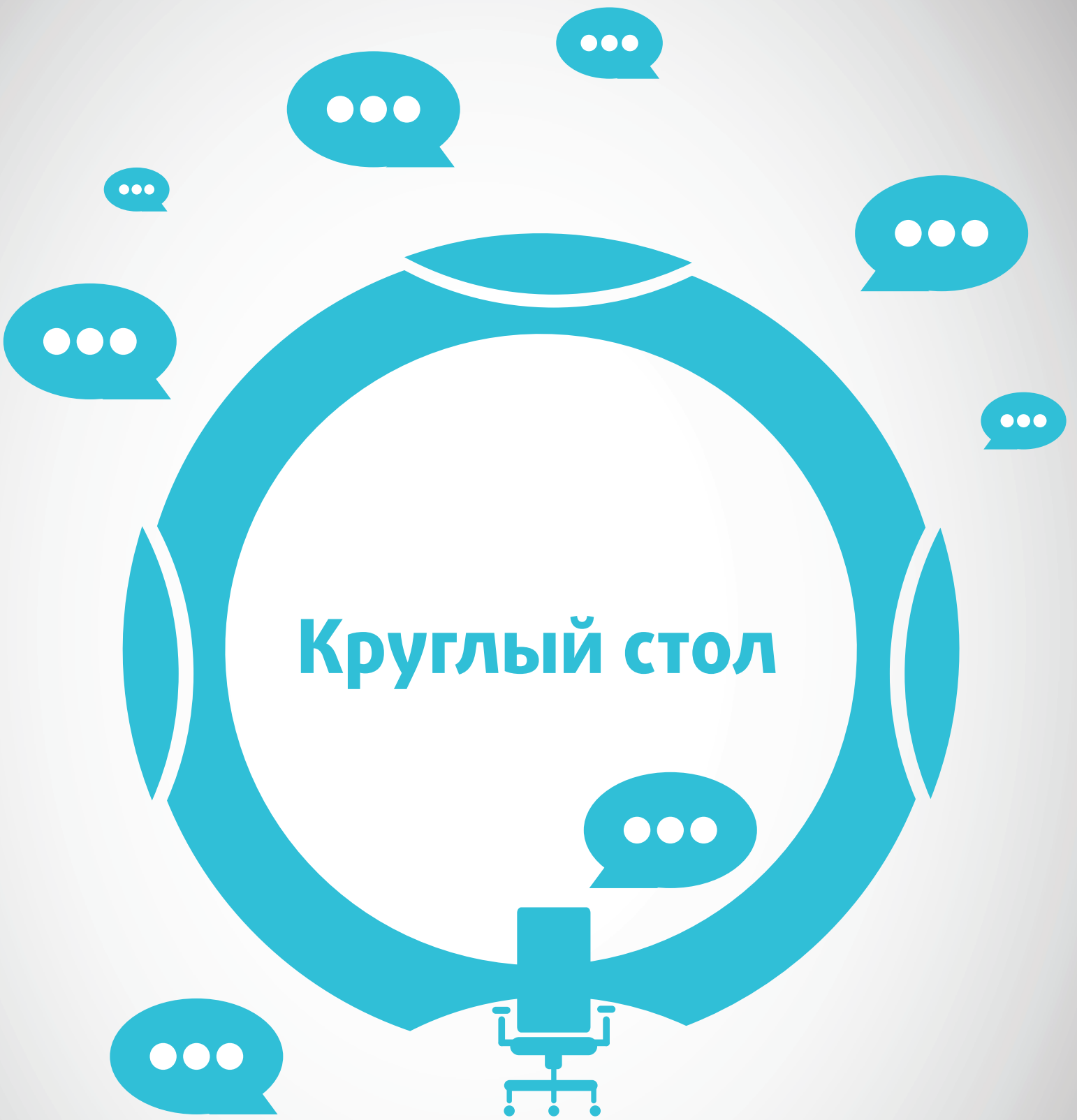
участие государства в оперативном управлении сетями связи общего пользования в целях минимизации последствий атак на ИКС КИИ.

В-третьих, важными проблемами совершенствования международной составляющей правового обеспечения безопасности КИИ являются следующие:

- определение границ национальной КИИ в глобальной информационно-коммуникационной инфраструктуре;
- закрепление признаков компьютерных инцидентов в автоматизированных системах управления КВО международного характера;
- международное сотрудничество в области ликвидации последствий компьютерных инцидентов в КВО.

В-четвертых, развитие правового обеспечения безопасности КИИ потребует введения значительного количества правовых новаций.

1. Стратегия национальной безопасности Российской Федерации. Утверждена указом президента Российской Федерации от 31.12.2015 № 683, доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности ООН. 22 июля 2015 г., A/70/174
2. Шинкарецкая Г. Г. Информационные технологии, война и гражданское население. Институт государства и права РАН. www.igpran/articles/3404/; Koh H. H., International Law in Cyberspace. Harvard International Law Journal. December 2012. v 54; Stauffacher D., Kavanagh C., Confidence building measures and International Cyber Security. ICT4 Peace Publishing, Geneva; Десятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности. 20-23 апреля 2015 г., Гармиш-Партенкирхен, Германия; Тиунов О. И., Авхадеев И. З. Об использовании информационно-коммуникационных технологий в вооруженных конфликтах и вопросы применимости международного права к их использованию государствами. В кн. Современное международное право. Теория и практика. Оригинал-макет. М., 2015 и другие.
3. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Утверждены указом президента Российской Федерации от 3 февраля 2012 г. № 803
4. Доктрина информационной безопасности Российской Федерации. Утверждена поручением президента Российской Федерации от 9 сентября 2000 года № 1895
5. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Утверждены указом президента Российской Федерации от 3 февраля 2012 г. № 803
6. Федеральный закон «О связи» от 7 июля 2003 года №126-ФЗ
7. Там же. Ст. 22, 24, 26.
8. Организационно-правовое обеспечение информационной безопасности. Под ред. Т. А. Поляковой и А. А. Стрельцова. М., Юрайт, 2016.
9. Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера». 21 декабря 1994 года № 68-ФЗ.
10. Федеральный закон «Об использовании атомной энергии» от 21 ноября 1995 года № 170-ФЗ.
11. Федеральный закон «О безопасности гидротехнических сооружений» от 21 июля 1997 года № 117-ФЗ.
12. Федеральный закон О промышленной безопасности опасных производственных объектов» от 21 июля 1997 года № 116-ФЗ.
13. Федеральный закон «О транспортной безопасности» от 9 февраля 2007 года № 16-ФЗ.
14. Федеральный закон «О безопасности объектов топливно-энергетического комплекса» от 21 июля 2011 года № 256-ФЗ.
15.Федеральный закон«О связи» от 7 июля 2003 года №126-ФЗ.
16. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ.
17. Уголовный кодекс Российской Федерации.
18. Федеральный закон «О связи», ст. 12.
19. Федеральный закон «Об использовании атомной энергии» от 21 ноября 1995 года, № 170-ФЗ.
20. Федеральный закон «О промышленной безопасности» опасных производственных объектов» от 21.07.1997 № 116-ФЗ.
21. Федеральный закон «О защите населения , ст. 10.
22. Федеральный закон «О связи», ст. 41.
23. Федеральный закон «Об информации, информационных технологиях и о защите информации».
24. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Указ президента Российской Федерации от 15 января 2013 года № 31с.
25. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Утверждены указом президента Российской Федерации от 3 февраля 2012 г. № 803.
26. Там же.
27. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утверждены президентом Российской Федерации 24 июля 2013 № Пр-1753.
28. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности ООН. 22 июля 2015 г., A/70/174.


Круглый стол

Критические информационные ресурсы и инфраструктура

Идентификация, обеспечение защиты и устойчивости

Мы пригласили ведущих российских и зарубежных экспертов поделиться своими взглядами на вопросы, связанные с критической инфраструктурой. В качестве формата обсуждения мы выбрали "круглый стол", виртуальный, разумеется, - в духе нашего издания.

Герман Клименко
советник президента РФ

Дмитрий Мариничев
Интернет-омбудсмен. Общественный представитель уполномоченного при Президенте РФ по защите прав предпринимателей по вопросам, связанным с нарушением прав предпринимателей при осуществлении регулирования и контроля функционирования и развития интернета

Участники круглого стола

Александр Ильин
технический директор MSK-IX

Марко Хохевонинг (Marco Hogewoning)
в прошлом сетевой инженер, теперь технический консультант группы внешних связей RIPE NCC

Михаил Кадер
инженер компании Cisco

Ваше определение критической инфраструктуры?

Есть несколько разных определений. Мне, как человеку много лет занимающемуся вопросами информационной безопасности, близко вот такое – из РД ФСТЭК: «Ключевая (критически важная) система информационной инфраструктуры (КСИИ) — информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан, и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями».

Если говорить об уровне отдельного государства, то критическая инфраструктура – это совокупность разного рода объектов и связей между ними, нарушение работы которой приводит к серьезным последствиям в жизнедеятельности общества, включая экономику, информационное пространство, уровень безопасности населения и т.д. Для конкретного государства таких систем можно выделить несколько – в частности, для их определения в случае нашей страны можно отталкиваться от распоряжения правительства РФ от 23 июня 2006 г. № 411-рс «Об утверждении Перечня критически важных объектов Российской Федерации».

Мне не очень нравится словосочетание «критическая инфраструктура», поскольку в любой технической системе присутствуют точки отказа – уязвимые компоненты, которые при выходе их строя затрудняют или делают невозможной работу всей системы. Обычно такие системы многократно резервируются и дублируются, но бывают элементы, которые продублировать нельзя (точно так же, как человеку нельзя вырастить второе сердце для резерва). Именно такие важные элементы и заслуживают наибольшего внимания и наибольшей защиты.

Если говорить в общем, то это совокупность технологических объектов и связей между ними, достаточных для функционирования управляемой системы. Рассматривая критичность инфраструктуры в аспекте общественной безопасности, можно сказать, что это инфраструктура, нарушение, отказ или разрушение которой могли бы оказать серьезное влияние на здоровье населения, общественные и политические дела, окружающую среду, безопасность и социально- экономическое благополучие. Но это лишь одно из определений – вопросами критической инфраструктуры озаботились сейчас практически все страны, и каждое государство привносит в него свой смысл и свою специфику.

Во-первых, мне не кажется, что можно четко разграничить Критическую инфраструктуру (КИ) и Критическую информационную инфраструктуру (КИИ). Любой компонент инфраструктуры может быть критическим, иногда это затрагивает и цифровые системы, служащие для передачи, обработки или хранения информации. Критичность системы или элемента, в конечном счете, как говорят, "в глазах смотрящего". Все зависит от того, какой экономический ущерб нанесет прерывание обслуживания или сбой, как оно повлияет на безопасность (либо ощущение безопасности). Говоря о КИ, мы часто сразу думаем о катастрофах на макроуровне, таких как крупномасштабные аварии электросети или ИТ-сбои в аэропортах, которые вызывают крупные задержки и отмену вылетов. Но есть и микроуровень. Потеря мобильного соединения с Интернетом на одном-единственном карточном терминале может не восприниматься как КИ-отказ... но если вы владелец маленькой фирмы и терминал ваш, невозможность обработки платежей поставит под угрозу весь бизнес.

Какие информационные услуги и системы, с Вашей точки зрения, относятся к критическим ресурсам глобальной сети Интернет? Национального сегмента Интернета?

В глобальной сети Интернет, на мой взгляд, можно выделить следующие ключевые подсистемы - это физическая инфраструктура (дата-центры, линии связи, каналообразующее, маршрутизирующее, коммутирующее и прочее сетевое оборудование, системы электроснабжения, рабочие станции пользователей и др.) и логическая инфраструктура (системы баз данных, доменных имен DNS, поисковые системы, операционные системы и программное обеспечение пользователей). С точки зрения степени влияния на работу сети Интернет, на мой взгляд, физическая инфраструктура имеет существенно более важное значение. Однако следует отметить, что Интернет развивался не один десяток лет, и за это время появилось множество технических решений, минимизирующих влияние физической инфраструктуры на пользователей путем многократного резервирования и повышения надежности ее отдельных элементов. Конечно, существуют некоторые государства, где по каким-либо причинам (например, политическим) внедрение этих технических решений существенно ограничено, что приводит к повышению критичности инфраструктуры – в качестве примера можно привести выход из строя трансграничных переходов в Сирии в 2012 году. Тем не менее, если рассматривать вопрос на уровне глобальной сети, то сегодняшние реалии таковы, что, например, выход из строя отдельного, даже крупного провайдера или какого-либо дата-центра не оказывает существенного влияния на инфраструктуру в целом. Сюда же можно отнести и точки взаимодействия и обмена трафиком. Большинство операторов Интернета имеют полное резервирование с использованием различных каналов связи, поэтому возможное отключение одной из точек обмена трафиком может лишь привести к перераспределению потоков данных, после чего достаточно быстро сеть примет опять равновесное стабильное состояние.

Я бы отнес к ним несколько основных и вспомогательных систем – конечно, службу доменных имен DNS, маршрутизацию, системы управления и службу сетевого времени (NTP).

Никакие информационные услуги не являются и не могут являться критическими ресурсами глобальной сети Интернет. Наиболее критической является энергосистема, затем - сети электросвязи, и, наконец - системы, поддерживающие технические стандарты, адресацию сети Интернет и маршрутизацию. Что касается «Национального сегмента

Интернет», то для него критичнее всего национальное регулирование. Впрочем, для информационных услуг существует однозначный показатель критичности: в том случае, когда речь идет об оповещении граждан о чрезвычайных происшествиях. Тут необходима простая и безотказно работающая система, на которую должно быть минимизировано даже теоретическое деструктивное воздействие.

Интернет с самого начала проектировался с расчетом на сбои. Вряд ли есть вообще какие-либо системы или компоненты, которые могут считаться критическими на глобальном уровне. Для любой системы, которую можно счесть критической, имеются альтернативные системы, которые могут оказывать эквивалентные услуги в случае ее отказа. Интернет в силу своего децентрализованного устройства (по крайней мере, на техническом уровне) не содержит компонентов, чей отказ приводит к отказу всей системы (так называемых SPOF - single points of failure). С логической или организационной точек зрения, может показаться, что SPOF существуют, но их (временная) недоступность не должна иметь значительного воздействия на потоки данных или услуги, оказываемые по Интернету. Это при условии, что сети спроектированы как положено, с расчетом на возможность отказа или недоступности того или иного элемента или услуги. Это что касается глобального масштаба. На национальном уровне в теории должно быть то же самое. Однако, если рассмотреть вопрос на более детальном уровне, как в примере с владельцем маленькой фирмы, то окажется, что "незначительный локальный сбой", каким он виделся с макроуровня, может оказаться критическим для пользователя, затронутого сбоем. Вообще, чем более децентрализованы система и ее управляющие элементы, тем менее вероятно, что отказ конкретного сервиса приведет к критическому сбою. Дело в том, что в подобных сценариях критические системы, зависящие от этой службы, обычно могут переключиться на резервные системы и альтернативных поставщиков сервисов. Разумеется, есть примеры, когда длительный и масштабный отказ неизбежен и имеет значительные последствия в локальном масштабе, например пожар в центре данных Vodafone в Нидерландах несколько лет назад, когда без связи остались и общественный транспорт, и некоторые госструктуры. Но, опять же, с национальной точки зрения потеря мобильной связи была локализована в небольшом регионе, и удалось относительно быстро и легко справиться с последствиями и восстановить связь.

Это очень интересный вопрос, и подходить к нему можно с разных сторон. Критической обычно принято называть инфраструктуру, от работы которой зависит выполнение какой-то очень важной функции. Однако эта функция может быть очень разной для разных заказчиков. Приведу такой пример – когда-то давно мы работали с крупным банком, строили ему информационную систему. Применяли при этом классический инженерный подход – для повышения надежности дублировали каналы связи, терминалы, обрабатывающее ядро. А потом в разговоре с руководством банка выяснилось, что критичным для бизнеса является работа принтера и наличие в нем бумаги. Просто потому что когда клиент придет, необходимо распечатать договор и подписать его с ним, а занести в общую базу его можно и позже. Соответственно и при обсуждении критичности той или иной инфраструктуры нужно понимать, кому и какую функцию она помогает выполнять. Отсюда следует что для государства это будет один набор технических систем, для пользователей – другой, а для бизнеса – третий, и в общем случае они совсем не обязательно пересекаются.

Есть ли в Интернете «критически важные объекты», влияющие на работоспособность всей глобальной сети?

Безусловно. И помимо всех тех технических систем, которые обычно называют в этой связи (системы DNS корневых и национальных доменов, точки обмена трафиком, сети Tier I операторов, корневые удостоверяющие центры TLS), я бы хотел отметить, что ключевую роль в работе интернета играют отдельные люди и коллективы. Они обладают уникальными знаниями, компетенциями, чрезвычайно важной информацией (пароли, порядок доступа и т.д.). Отсутствие такого человека в доступности может нанести существенный урон работе интернета, сравнимый с отключением любой из технических систем.

Да, в первую очередь маршрутизация, в случае ее масштабного сбоя сеть просто перестанет работать, или информация пойдет в «чужие» руки. Поэтому защита всех узловых элементов сети, например, магистральных маршрутизаторов BGP, серверов маршрутизации (routeservers), там, где они применяются, и прочих, должна быть обеспечена обязательно.

То же самое касается и службы DNS. При ее выходе из строя или манипуляции ею могут возникать и масштабные сбои, а также осуществляться несанкционированный доступ к информации.

Естественно, есть, хотя интернет и является устойчивой и надежной системой – именно так его проектировали в самом начале. Но, тем не менее, отсутствие электричества может оставить без интернета район, город, страну или даже континент. А разрушение магистральной линии связи (например, повреждение подводного кабеля) неоднократно приводило к проблемам с доступом в глобальную сеть в целых регионах (речь идет не только и не столько о России, на памяти относительно недавний случай с Австралией, к примеру). Можно приводить множество примеров того, как можно нарушить связность – но, к счастью, сеть устроена так, что обходные пути находятся достаточно быстро, и работоспособность в той или иной степени восстанавливается.

Пожалуй, единственным критически важным объектом, имеющим косвенное влияние на работоспособность всей глобальной сети, можно назвать систему корневых узлов DNS. И опять-таки, этот объект можно назвать критичным с очень большими оговорками. Известны протоколы связи, которые не используют в своей работе DNS, и их это никак не затрагивает. Следует отметить также, что в виду множественности глобального доменного пространства, используемого во всех странах мира, национальная система DNS (поддерживающая национальные доменные имена), по моему мнению, не является критической и может характеризоваться только как существенная.

Чем нужно руководствоваться при идентификации критической инфраструктуры? Какие факторы определяют критичность инфраструктуры какого-либо объекта?

Тут все и просто, и сложно. Смотрим определение вначале. Видим, что если выполняются описанные там критерии – вот вам и критическая инфраструктура. Пример из московской жизни – перевел МГТС своих абонентов на GPON и запустил телефонию поверх него в режиме IP с сигнализацией SIP, а «старую» телефонию отключил. Вот и стала IP-телефония МГТС-а критической инфраструктурой, потому что может оказаться единственной системой оперативного оповещения граждан. Но вот сам Интернет таким для граждан не является. Они и без него вполне могут прожить. Например, если не работает портал госуслуг, жизнь от этого не остановиться, можно и в МФЦ спокойно сходить. А все меж- и внутриведомственные системы обмена информации по своим каналам связи живут, и серверами внутренними пользуются. Поэтому от Интернета не зависят. Т.е. Интернет еще пока в нашей стране не стал такой критической инфраструктурой. С ним, конечно, гораздо удобнее и продуктивнее, но и без него – ПОКА не катастрофа. Пишу ПОКА, потому что развитие технологий и оптимизация затрат на обмен данными может привести к тому, что Интернет станет просто основной и телекоммуникационной средой для ряда критически важных объектов, и тогда окажется критической инфраструктурой.

Идентификация критической инфраструктуры должна производиться на основе оценки соответствующих экспертных групп. Стартовать можно от уже ранее принятых документов – в качестве примера можно привести упомянутое мною выше постановление правительства РФ.

А что касается факторов, определяющих критичность инфраструктуры, то я отнес бы к ним масштаб негативного воздействия при аварии инфраструктуры, а также роль, которую играет доступ к ней для нормальной жизнедеятельности общества.

Для того чтобы понять, насколько система важна для выполнения какой-то функции (что и определяет принадлежность к критической инфраструктуре), необходимо смоделировать ситуацию, при которой эта система перестает работать и попытаться оценить последствия. И так последовательно «отключая» различные звенья мы выделяем наиболее важные из них, определяем их вес, оцениваем, какой ущерб это может принести смежным системам. И в результате такого ранжирования можно выделить составляющие, которые являются наиболее важными для работы интернета.

В первую очередь - техническими стандартами. Затем - практическим опытом и здравым смыслом. К любому объекту нужен индивидуальный подход, нужно выявить его слабые и сильные стороны в части безопасности и тогда уже говорить о факторах, которые требуют наибольшего внимания. В общем случае я бы отметил три важных фактора: влияние на экономику, влияние на население и влияние на национальную безопасность. Все остальное, по сути, вторично, и если эти три позиции защищены, то можно считать, что критическая инфраструктура имеет высокую защиту.

На этот вопрос нужно отвечать, рассматривая ситуацию снизу вверх. Единственное лицо или организация, которые реально могут определить эффект конкретного сбоя (будь то отказ элемента или системная ошибка) - это тот, кто зависит от соответствующего сервиса. Разумеется, ответы таких лиц необходимо агрегировать и экстраполировать на более высоком уровне, чтобы определить эффект сбоя и вероятность более широкомасштабных отказов. Второй важный шаг - выполнять моделирование и (где возможно) тесты, чтобы обеспечить функционирование отказоустойчивых систем и отсутствие неотслеженных зависимостей или каскадных эффектов, которые могли бы превратить отказ системы или элемента в критический. В рамках этой парадигмы критичность конкретного элемента инфраструктуры определяется критичностью систем и инфраструктуры, зависящих от него, и, что еще более важно, способностью этих систем переключиться на альтернативную.

Кто и как должен быть вовлечен в обеспечение надежности и безопасности критической инфраструктуры? Как должно происходить взаимодействие между сторонами, вовлеченными в процесс обеспечения безопасности?

В этом процессе должны участвовать самые разные стороны, и тут недопустимы перекосы. Опыт многих стран показывает, что операторами критической инфраструктуры очень часто являются коммерческие, негосударственные компании. Конкуренция на свободном рынке позволяет им достигать необходимого качества работы лучше и быстрее любого другого стимулирующего механизма. Безусловно, государство должно принимать участие в этом процессе путем лицензирования, установления стандартов качества, аудита, однако ни в коем случае не должно происходить огосударствления таких операторов. Кроме того желательно избегать образования сверхмассивных структур, отвественных сразу «за все», так как именно они и становятся теми самыми точками максимальной уязвимости.

Это, наверное, самый сложный вопрос. Это и многочисленные учреждения, отвечающие за безопасность страны, например, СовБез, ФСБ, ФСТЭК и т.п., а также организации, отвечающие за функционирование этих инфраструктур. Если посмотреть на историю с МГТС, о которой я говорил чуть раньше, – они тоже должны быть вовлечены в обеспечение надежности. А распределение ролей достаточно стандартно. Агентства по безопасности, в рамках своих полномочий, разрабатывают требования по защите критических инфраструктур, например, ФСТЭК и ФСБ.

Оператор или другая уполномоченная компания, обслуживающая эту инфраструктуру, обеспечивает их выполнение – например, МГТС. А также должен существовать уполномоченный орган, проверяющий выполнение требований – тот же Роскомнадзор.

Это процесс многосторонний, участие всех организаций, структур и физических лиц, имеющих отношение к данной критической инфраструктуре, должно быть четко регламентировано. Соответствующая документальная база должна быть разработана компетентными экспертными группами, с учетом всех технических и юридических аспектов, и с участием государства.

Операторы, управляющие объектами, инженеры, эксперты, системные архитекторы. Формат взаимодействия может быть различным на разных уровнях, главное - не ломать существующие уже способы и модели взаимодействия в области безопасности. Во многом подход к безопасности критической инфраструктуры должен решаться на государственном уровне. В первую очередь нужна полноценная и продуманная нормативная база и координирующий орган, который бы занимался, в том числе, сбором и обменом информацией об угрозах и путях борьбы с ними, следил за актуаль-

ностью нормативных документов и вовремя их пересматривал, внося изменения. Необходимо развивать государственно-частное партнерство и привлекать к решению вопросов безопасности критической инфраструктуры частные компании в области информационной безопасности. Нужно готовить квалифицированные кадры и т.д.

Инженеры, которые проектируют и эксплуатируют инфраструктуру, лучше всего могут оценить надежность и безопасность своих систем и должны иметь достаточное право голоса в процессе. Разумеется, госорганы и академические организации тоже играют роль в поддержке этого процесса, собирая и агрегируя оценки на национальном уровне и обеспечивая просвещение людей о зависимостях между различными сервисами и системами. Что касается взаимозависимости систем, например зависимости центра данных и электросети друг от друга, необходима некая степень (международного) сотрудничества, чтобы гарантировать участие в дискуссии всех заинтересованных сторон и информирование каждой из них о заботах другой и ее возможности урегулирования рисков в своей деятельности.

Какими дополнительными обязанностями и правами должны, с Вашей точки зрения, обладать операторы критической инфраструктуры и услуг, другие вовлеченные стороны?

Наделение какой-то организации статусом оператора критически важной инфраструктуры, безусловно, сильно сказывается на ее работе. Такая компания должна соответствовать большому количеству требований по безопасности, надежности, устойчивости работы, проходить регулярные проверки и аудит. Причем требования эти формируются не только исходя их отраслевых стандартов – в их формировании участвует и «заказчик» - тот, для кого эта инфраструктура особенно важна. Например, в Испании и Португалии расположен ряд узлов связи, которые обеспечивают связность континентальной Европы с Америкой через трансатлантические каналы. Так вот система безопасности ЦОДов, в которых эти узлы связи расположены, должна удовлетворять в том числе и государственным требованиям. В то же время такие организации могут иметь и дополнительные преференции. Прежде всего финансовые о стороны государства – оно платит компаниям за поддержание какой-то крайне важной для всего интернета функции. Также они автоматом получают большие репутационные преимущества: точно так же как раньше только лучшие производители удостаивались звания «Поставщик двора его императорского величества», так и сейчас – это знак высочайшего качества услуг.

Исключительно теми, которые определены консенсусом между всеми заинтересованными сторонами. Операторы сами заинтересованы в том, чтобы вверенные им объекты работали как часы. У каждого есть уже определенные и сформированные временем обязанности, и заниматься каждый должен своим делом.

Жизненно важно, чтобы каждый нес ответственность за свой кусочек этой головоломки, это относится и к конечным пользователям. Конечный пользователь, будь то частное лицо или компания, должен сам выполнять оценку того, насколько критичны для него конкретные сервисы или элементы инфраструктуры, и рассматривать любые альтернативные варианты или резервные системы, которые могли бы предотвратить превращение сбоя в критический.

Мне сложно детально ответить на этот вопрос. Как минимум должна быть обязанность и проработанный порядок оповещения о возникновении сбоев. В зависимости от объекта и уровня инцидента – это может быть и узкий круг лиц, а может быть и население всей страны. Соответственно, операторы такой инфраструктуры должны иметь необходимый доступ к системам оповещения, а также к персональным данным оповещаемых. А также, естественно, иметь утвержденный порядок взаимодействия с силовыми ведомствами.

Права и обязанности операторов и других сторон, участвующих в эксплуатации и поддержке критической инфраструктуры, должны вытекать из документов и регламентов, которые разрабатываются на основе взаимной договоренности и работы экспертных групп. Ключевую роль играет компетентность участников этого процесса, учет международного опыта и разумная регуляция со стороны государства.

За чей счет должно финансироваться обеспечение устойчивости и безопасности таких объектов, если они есть?

Финансирование работы любых технических систем идет за счет того, кому в первую очередь нужно чтобы эти системы работали. Чуть ранее мы говорили о том, что критическая инфраструктура может иметь разный состав в зависимости от того, кому и какую функцию она помогает выполнять. Соответственно будет логичным, если пользователи, государство и бизнес будут оплачивать работу тех систем, которые необходимы для их нормального функционирования, и для выполнения, соответственно, государственных или бизнесовых функций или удовлетворения интересов пользователей.

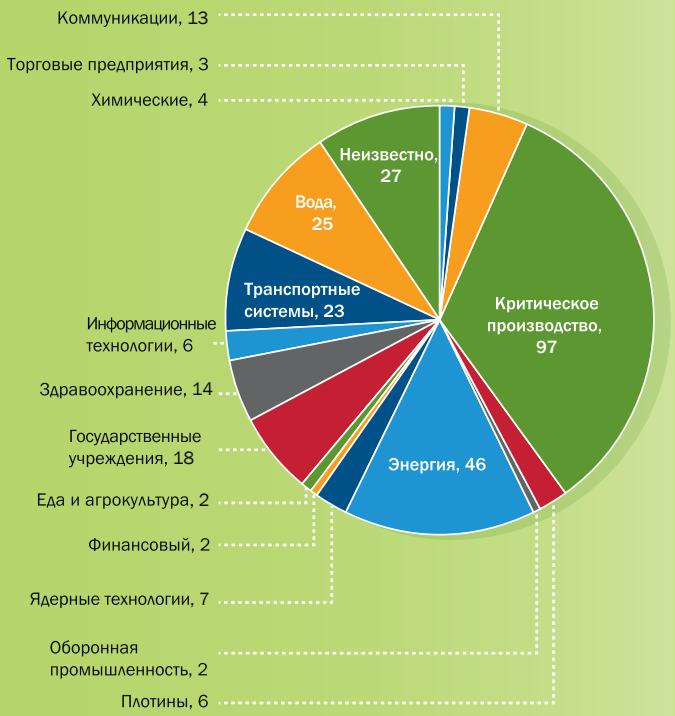
Сеть Интернет успешно развивается на протяжении нескольких десятков лет, и ее относительная устойчивость и безопасность базируется на различных финансовых источниках. Во-первых, это международное сообщество, включая группы (IETF и др.), работающие над стандартами, обеспечивающими стабильность новых решений и платформ – они имеют негосударственное финансирование. Во-вторых, разработанные технологии и сервисы применяются в рамках коммерческих проектов, для которых устойчивость и безопасность являются жизненно необходимыми. Наконец, возможно дополнительное финансирование со стороны государства, в случае возникновения каких-либо требований, диктуемых законодательством или общественными интересами.

За счет их владельцев и заинтересованных сторон. Здесь необходимо применять механизмы партнерства – далеко не всегда у пользователей таких объектов есть выбор, поэтому в устойчивости, безопасности и безотказной работе заинтересованы все, вплоть до государственных органов, если речь идет о функционировании системы, затрагивающей многие сферы деятельности граждан.

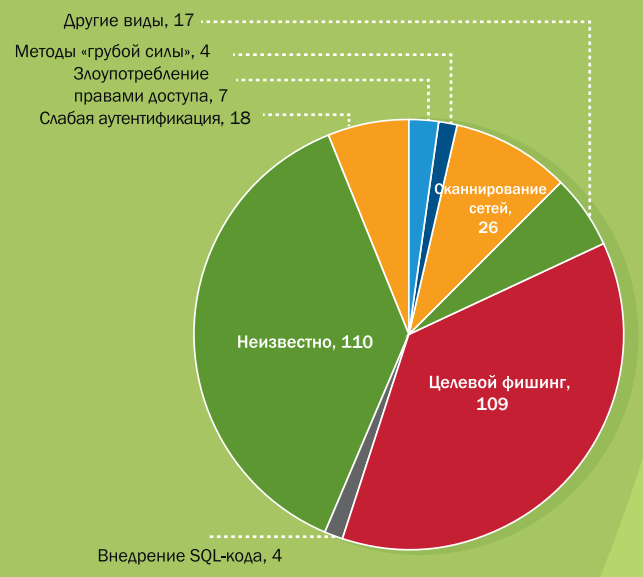
Думаю, что обязательно должно быть государственное финансирование. Так как критические инфраструктуры обеспечивают функционирование критически важных объектов – а это гос и муниципальные учреждения, силовые ведомства и т.п. – т.е в первую очередь бюджетные учреждения, то государство и должно нести затраты на инфраструктуру для их функционирования. Если это «разделяемая» инфраструктура, т.е. используемая и для других, например, коммерческих задач, тогда государство должно обеспечивать только частичное финансирование.

СТАТИСТИКА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗА 2015 ГОД

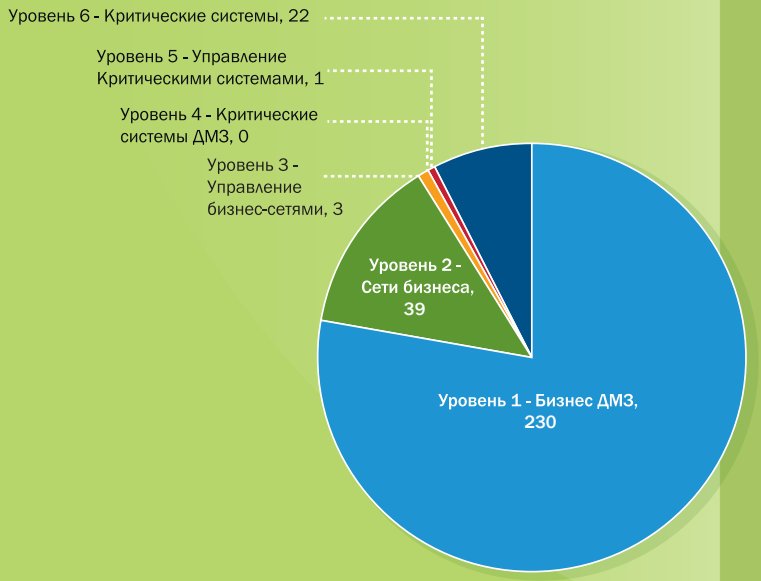
Инциденты по различным областям (295 всего)



Инциденты по источнику заражения (295 всего)



Степень поражения



Источник: NCCIC/ICS-CERT Year in Review (2015), p. 19

Замена в корневой зоне

Джефф Хьюстон (Geoff Huston)

В октябре 2017 года в корневой зоне DNS произойдет важнейшее событие со времени ее подписания в июле 2010 года. Ключ KSK, который служит для удостоверения всех остальных ключей, будет обновлен. Периодическое обновление ключей - нормальная практика, но KSK - ключ особенный и процесс обновления нетривиален. Каков процесс замены ключа, как подготовиться к этому событию и в чем заключаются риски - рассказывает эта статья.

В мире шифрования с открытым ключом часто отмечается, что соответствующий секретный ключ не может навсегда оставаться в секрете. Это не означает, что секретный ключ может держаться в секрете только в течение ограниченного периода времени, а затем лежащая в основе криптография самопроизвольно разрушится и ключ неизбежно раскроет себя! Однако существуют эволюционные факторы, которые стремятся подорвать целостность личного ключа по прошествии длительного времени. Чем больше ключ используется для шифрования продуктов, тем больше информации, указывающей на его секретное значение, становится доступной. Конечно, эти улики являются бесконечно малыми по значению и большинство видов использования секретного ключа, даже сравнительно интенсивного, не дают злоумышленнику преимуществ при его взломе, однако в абсолютном выражении риск остается. В то же самое время, продолжающийся рост вычислительной мощности позволяет легче решать вычислительные проблемы, ранее считавшиеся чрезмерно трудными, поэтому старые ключи, которые несколько лет назад, возможно, соответствовали последнему слову криптографической науки, могут оказаться более уязвимыми для современных компьютерных возможностей. И конечно, всегда существует риск несчастного случая, когда секретный ключ непреднамеренно раскрывается, либо - что до некоторой степени так же плохо, - когда секретный ключ становится недоступным. Последний случай не означает взлом секретного ключа, однако конечный результат аналогичен – ключ становится фактически невозможно использовать.

DNSSEC и заявление о практике администрирования ключами

Таким образом, ни один криптографический секрет не может считаться «абсолютным». Все это является относительным, и применение ключа связано с некоторым риском того, что он не является строгим секретом. Если дело обстоит именно так, и если мы не можем реально понять точные уровни риска, связанные с использованием ключа, то почему мы должны доверять любому виду шифрования с открытым ключом?

Для того, чтобы позволить нам принять более обдуманное решение о степени доверия к открытому ключу, общепринятым выбором для администратора ключей является публикация «Заявления о практике» (Practice Statement), которое подробно описывает процедуры, которые держатель ключа применяет для его обслуживания. Это публичное обязательство администратора ключей в отношении методов, которые используются для поддержания целостности личного ключа.

Обычно в таком документе ожидают увидеть изложение требований, описание оборудования и средств управления, которые применяются в работе с секретными ключами, технических средств контроля, операционных действий и намерений в отношении аудитов соответствия. Таким образом, до тех пор, пока администраторы ключей соблюдают обязательства, изложенные в опубликованном ими заявлении о практике, пользователи, которые полагаются на целостность секретного ключа как на основу их доверия к подписанным объектам в связанной с этим инфраструктуре открытого ключа (PKI, Public Key Infrastructure), имеют в запасе нечто, что может быть более основательным, чем неподтвержденная слепая вера!

Инфраструктура ключа DNSSEC для DNS не использует обычные сертификаты открытого ключа X.509, а задействует иерархическую структуру открытого ключа, в рамках которой цепочки подписания ключа содержатся внутри модели иерархического делегирования структур имен. На вершине структуры имен DNS находится корневая зона, а на вершине соответствующей структуры открытого ключа располагается ключ подписания ключа (KSK, Key Signing Key) корневой зоны.

Если мы хотим доверять целостности KSK в качестве базиса для доверия к DNSSEC, то необходимо взглянуть на заявление о практике оператора KSK корневой зоны. Этот документ был опубликован проектной группой DNSSEC в корневой зоне в октябре 2010 года, его можно найти по ссылке: https://www.iana.org/dnssec/icann-dps.txt. В разделе 6.5 этого документа написано следующее:

Запланировано, что каждый ключ KSK корневой зоны пройдет через церемонию обмена ключами в соответствии с установленными требованиями, либо через пять лет эксплуатации.

При этом некоторую дискуссию вызвало значение фразы «через пять лет эксплуатации»: подразумевала ли эта фраза обязатель-

ство изменить значение KSK на пятую годовщину эксплуатации, либо буквально в любое время после пятой годовщины, что может включать последующий промежуток времени, возможно, длящийся целые десятилетия! Разумная интерпретация этого обязательства представляет собой приблизительную оценку предыдущего, а именно, обязательства, которое включало намерение изменить KSK по истечении пяти лет эксплуатации или через некоторое время после этого срока. Учитывая тот факт, что ключ KSK был введен в действие в июле 2010 года, это означает, что изменение KSK было запланировано примерно на середину 2015 года или около этого срока.

Где мы находимся с этой задачей? Будет ли изменен ключ KSK? Каким образом это будет сделано?

Отчет проектной группы KSK

В марте 2016 года организация ICANN опубликовала отчет проектной группы, которая анализировала эту задачу в течение предыдущих 15 месяцев. Отчет опубликован по адресу: https://www.iana.org/reports/2016/root-ksk-rollover-design-20160307.pdf. Этот отчет последовал за состоявшимся в 2012 году общественным обсуждением, проводившимися в 2013 году технологическими исследованиями и исследованием (также проводившимся в 2013 году) Комитета по стабильности и безопасности при ICANN (https://www.icann.org/en/system/files/files/sac-063-en.pdf). Это означает, что работы по подготовке изменения KSK начались задолго до пятилетней годовщины и продолжаются по сей день.

Первый вопрос заключается в том, почему прилагается столько усилий по изменению ключа KSK корневой зоны? Ключи DNSSEC, как ключи подписания зоны (ZSK, Zone Signing Key), так и ключи KSK, меняются все время, и обычно они не требуют такого же уровня внимания и заботы на протяжении целого ряда лет. Почему этому конкретному ключу KSK уделяется столь особое внимание?

Ключ KSK корневой зоны является «особым», поскольку для него отсутствует вышестоящий ключ, который может «закрепить» изменение ключа. Каждый резолвер, осуществляющий DNSSEC-валидацию, имеет локально кэшированную копию этого значения KSK в качестве доверительного ключа, однако проблема заключается в том, чтобы выполнить набор изменений, которые могут сигнализировать этим резолверам о необходимости загрузки нового ключа в локальный кэш в качестве доверительного, и кроме того, выполнить это безопасным способом. Именно здесь вступают в игру процедуры, описанные в RFC 5011. Поскольку не существует вышестоящего ключа для фиксации изменяющего ключа, RFC 5011 определяет

Почему ключ подписания ключа корневой зоны DNS является особенным? Каким образом этот конкретный ключ отличается от всех остальных ключей в рамках DNSSEC?

Простой ответ заключается в том, что это единственный ключ в рамках всей структуры DNSSEC, для которого не существует «вышестоящего ключа».

В случае ключа ZSK вышестоящим ключом является ключ KSK зоны. Изменение ключа ZSK обычно сопровождается введением нового ключа ZSK при помощи его публикации в наборе DNSKEY зоны (он, как обычно, подписывается ключом KSK). После того, как пройдет определенный период времени, позволяющий распространить старую, кэшированную версию записи DNSKEY по всем авторитетным серверам, плюс значение времени жизни (TTL, Time To Live) для набора ключей, новый ключ ZSK будет готов для использования. К этому моменту все подписи в зоне могут быть «переподписаны» с использованием нового ключа ZSK. Старый ключ ZSK хранится в наборе DNSKEY для того, чтобы обеспечить валидацию ранее кэшированных копий записей подписи (подписанных старым ключом) с помощью старого ключа ZSK. И опять, после распространения и периода TTL может быть выполнен финальный этап, который подразумевает удаление старого ключа ZSK из зоны. До тех пор, пока существует ключ KSK, которым можно подписывать записи, относящиеся к разным ZSK, изменение ключа ZSK является простым и понятным (Рис. 1).

Рис. 1. Изменение ключа ZSK

процесс, в рамках которого старый ключ KSK фактически является точкой привязки изменения ключа, позволяя резолверам доверять входящему ключу KSK на базе их доверия к применявшемуся ранее ключу. Этот процесс влечет за собой подписание уходящим ключом KSK входящего ключа KSK и затем поддержание этого состояния в течение расширенного периода (30-дневный период «добавления удержания»; Add Hold-Down) как средства противодействия определенным видам атак с помощью взломанного набора ключей.

Эти шаги в процессе изменения ключа KSK, предложенные в RFC 5011, показаны на Рис. 3. Изменения в корневой зоне, необходимые для смены KSK, касаются только изменений в наборе записей ресурсов (RRset, Resource Record Set) DNSKEY корневой зоны. Никакая другая часть корневой зоны не меняется из-за этого изменения ключа.

При изучении шагов на Рис. 3, можно заметить, что на начальной стадии RRset DNSKEY содержит действующие ключи KSK и ZSK, а вся запись DNSKEY подписана действующим ключом KSK.

Первый шаг заключается в том, чтобы ввести новый ключ KSK в корневую зону. Это достигается за счет добавления дополнительной записи ресурсов (RR) DNSKEY в корневую зону, что фактически публикует новое значение ключа. Набор RRset DNSKEY по-прежнему подписан действующим ключом KSK. Это состояние сохраняется неизменным в течение не менее 30 дней (период «дополнительного удержания», Hold-Down, определенный в RFC 5011), что помогает смягчить некоторые риски, появившиеся из-за ослабленного ключа. Резолверы, осуществляющие проверки DNSSEC, должны обеспечить валидацию этого набора RRset DNSKEY, а если этот набор является действительным и новый ключ KSK был стабилен в течение периода «дополнительного удержания», то они в состоянии добавить новый ключ KSK в локальный набор достоверных ключей.

Второй шаг заключается в удалении старого ключа KSK из корневой зоны. Это влечет за собой удаление старого ключа из набора RRset DNSKEY и подписание этого набора с помощью нового ключа KSK.

Остается один финальный шаг, и он заключается в выдаче указания резолверам на удаление старого значения ключа из своего локального набора достоверных ключей. Это требует того, чтобы старый ключ KSK был добавлен обратно в набор RRset DNSKEY, но на этот раз с набором битов REVOKE, а также требует подписания набора RRset DNSKEY с использованием старого и нового ключей KSK. После этого старый ключ KSK может быть удален и уничтожен.

Существует целый ряд наблюдений в отношении этого процесса.

Первое наблюдение заключается в том, что второй и третий шаги можно поменять местами. Другими словами, после того, как новый ключ был введен в зону на Шаге 1, старый ключ можно отменить, а

Аналогичным образом, изменение ключа KSK может быть простым и понятным делом. Первый шаг заключается во введении нового ключа KSK в состав набора DNSKEY. На этот момент может быть также добавлена вторая запись RRSIG записи DNSKEY, сгенерированная с использованием нового ключа KSK. В то время, как запись DS родительской зоны ссылается на старый ключ KSK, новая запись RRSIG не будет использоваться для валидации - и поэтому фактически ничего не меняется. После того, как родительская зона «подберет» новую запись DS (соответствующую новому ключу KSK), она может ее немедленно опубликовать. Текущая зона должна продолжать публикацию старого ключа KSK и значения его подписи по крайней мере в течение периода TTL старой записи DS для того, чтобы обеспечить правильное обслуживание валидации для любых кэшированных значений DS. После истечения периода TTL записи DS старый ключ KSK и соответствующая ему запись подписи могут быть удалены из зоны (Рис. 2).

Эти шаги и различные альтернативы подробно рассматриваются в RFC 6781.

Ключ KSK корневой зоны немного отличается, поскольку для него не существует вышестоящего ключа, который можно использовать для «закрепления» меняющегося ключа. Отсутствует ключ для передачи ключа KSK и какой-либо обычный способ, чтобы гарантировать непрерывность цепочки доверия.

Рис. 2. Изменение ключа KSK

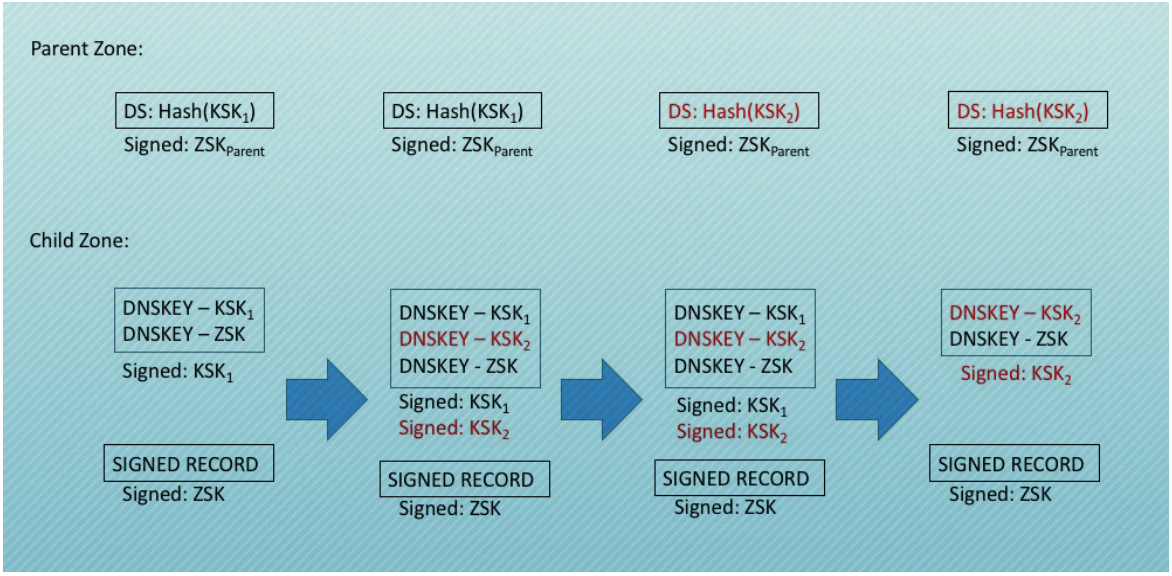
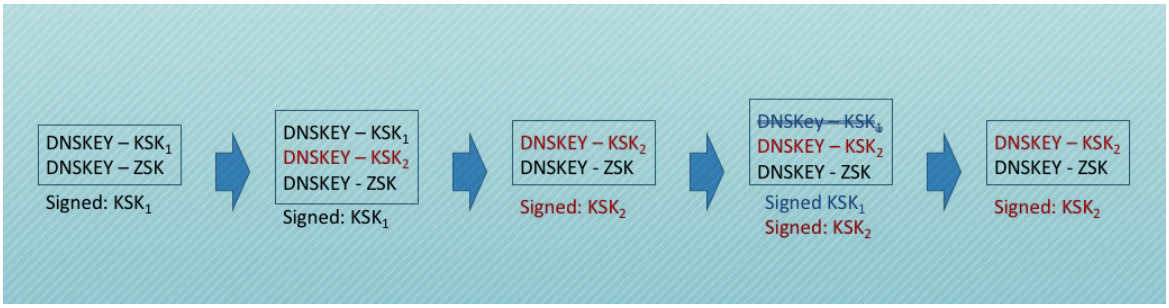


Рис. 3. Изменение ключа KSK корневой зоны – согласно RFC 5011



набор RRset DNSKEY можно подписать как уходящим, так и входящим ключом. После истечения соответствующего периода времени (более длительного, чем время жизни (TTL) для зоны) старый ключ KSK и его подпись могут быть удалены из корневой зоны. Однако, если это сделать, то не будет существовать пути обратно в случае, если процесс сгенерирует неприемлемый уровень ошибок, видимых для пользователя. При помощи разделения операций по изъятию старого ключа и его последующего аннулирования на дискретные события сохраняется возможность восстановления старого (и по-прежнему достоверного) ключа на случай, если введение нового ключа KSK приведет к непредусмотренному уровню отказа DNS.

Второе наблюдение заключается в том, что не существует периода, когда происходит «наложение» старого и нового ключей KSK. Переход между вторым и третьим шагами предусматривает полное удаление старого ключа KSK. На этом этапе не существует наложения, когда оба – старый и новый – ключа KSK одновременно подписывают набор RRset DNSKEY. Причиной этого пропуска является то, что двойное подписание набора RRset DNSKEY не несет никаких выгод в плане помощи при изменении ключа KSK, а, возможно, приводит к незначительному ухудшению положения. В конце Шага 1 все резолверы будут по-прежнему использовать уходящий ключ KSK для валидации подписи DNSKEY. Что касается Шага 2, то те резолверы, которые добавили входящий ключ KSK в свой доверительный набор, будут использовать этот входящий ключ, тогда как другие резолверы окажутся в затруднительном положении без точки доверия. Добавление этапа двойного подписания ничем не отличается от продолжения ситуации Шага 1. Те резолверы, которые не научились доверять новому ключу KSK, и те резолверы, которые подобрали новый ключ KSK как точку доверия, не способны сигнализировать о своем состоянии доверия ни одной третьей стороне, поэтому внешняя среда не становится «мудрее». Недостаток заключается в том, что двойные подписи увеличивают размер ответа на запрос DNSKEY без какой-либо помощи или простого информирования для процесса изменения ключа.

Весь процесс изменения ключа KSK не такой простой, как это описано выше, а кроме того, необходимо учитывать ключ ZSK. Ключ ZSK меняется каждый квартал. В течение 10 дней, предшествующих началу квартала, новый ключ ZSK добавляется в набор RRset DNSKEY вместе с действующим ключом ZSK, фактически передавая резолверам новое значение ключа ZSK. В первый день каждого квартала происходит смена ключа ZSK, при этом корневая зона подписывается новым ключом ZSK. Старый ключ ZSK остается в составе набора RRset DNSKEY в течение последующих 10 дней, что позволяет резолверам с кэшированным материалом, подписанным уходящим ключом ZSK, по-прежнему осуществлять валидацию этой кэшированной информации с помощью набора DNSKEY RRset корневой зоны. После истечения 10 дней старый ключ ZSK удаляется из корневой зоны, и процесс смены ZSK завершается. Если мы будем использовать период перехода к новому ключу ZSK для выполнения шагов по смене ключа KSK, то предполагаемый процесс будет больше походить на то, что изображено на Рис. 4.

Расписание изменения ключа KSK

Еще не утвержденное, предварительное расписание для изменения ключа KSK было предложено в отчете проектной группы (рекомендация 17 отчета проектной группы).

Рекомендованный график имеет следующий вид:

1 апреля 2016 г.

Подготовка нового набора ключей KSK, распространение его на средства хранения вторичных ключей и генерирование материала корневой зоны для использования в будущих шагах по изменению ключа.

11 января 2017 г.

Введение нового значения ключа KSK в корневую зону (Рис. 4, Шаг 1).

1 апреля 2017 г.

Смена ключа KSK и подписание набора RRset DNSKEY корневой зоны с использованием нового значения ключа KSK (Рис. 4, Шаг 3).

11 июля 2017 г.

Повторная публикация старого ключа KSK с набором битов REVOKE и подписание набора RRset DNSKEY с использованием обоих ключей KSK – старого и нового (Рис. 4, Шаг 7).

19 сентября 2017 г.

Завершение: удаление старого ключа KSK из корневой зоны (Рис. 4, Шаг 8).

Примечание редакции:

Окончательный план включает следующие шаги:

- **Октябрь 2016: начало процесса замены KSK: генерация нового ключа KSK.**
- **Июль 2017: публикация нового KSK в DNS.**
- **Октябрь 2017: новый KSK используется для подписания пакета ключей корневой зоны. Это собственно и означает замену ключа.**
- **Январь 2018: отзыв старого KSK.**
- **Март 2018: завершение процесса замены KSK.**

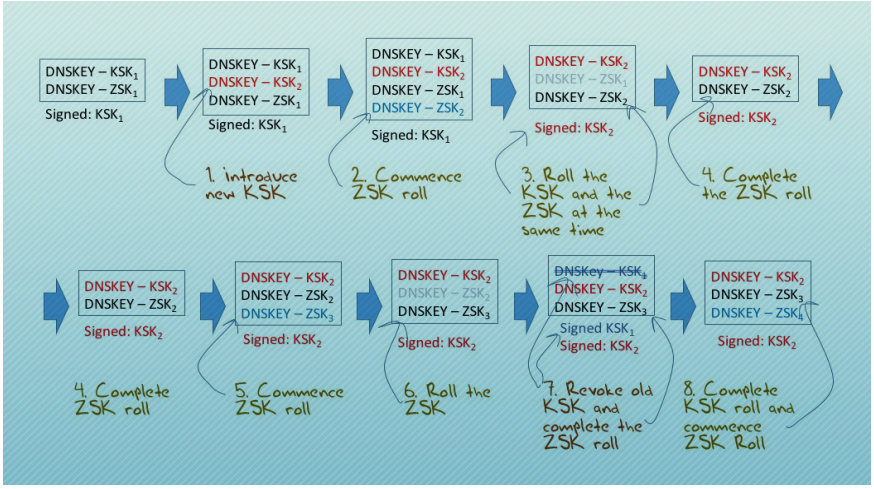
Длительное время ожидания - продолжительностью девять месяцев в 2016 году - отражает периодический график церемоний доступа по ключу. Последующие девять месяцев 2017 года «переплетены» относительно плановых изменений ключа ZSK корневой зоны, при этом изменения ключей KSK планируется вставить между изменениями ключей ZSK (там, где это возможно) для того, чтобы гарантировать, что размеры DNS-ответов не стали чрезмерно большими.

Что меняется, а что нет

Ключ KSK представляет собой асимметричный 2048-битовый RSA-ключ. На данный момент не предлагается менять ни размер ключа, ни криптографический алгоритм, используемый для его генерации.

Целый ряд экспертных организаций считает, что 2048-битовый ключ обеспечивает адекватную стойкость на предстоящие 10-15 лет. Для подтверждения этой точки зрения проектная группа приводит выдержки из отчетов ECRYPT, NIST и ANSSI. Учитывая вышеизложенное, не существует убедительных аргументов, оправдывающих увеличение размера RSA-ключа.

Рис. 4. Изменение ключа ZSK и ключа KSK корневой зоны



Эти отчеты агентств включают:

- http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
- http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
- http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

Альтернативой использованию таких больших RSA-ключей является переход на другой криптоалгоритм. Одна из потенциальных альтернатив RSA – это один из алгоритмов, входящих в набор Алгоритмов цифровых подписей на основе эллиптических кривых (ECDSA, Elliptical Curve Digital Signature Algorithm), которые используют гораздо меньшие по размеру ключи, обеспечивающие аналогичную криптографическую стойкость. Например, ECDSA-ключ, использующий кривую P-256, имеет стойкость, эквивалентную по крайней мере асимметричному 3072-битовому RSA-ключу. Однако, хотя это и может уменьшить размер DNS-ответов при изменении ключа, недостатком такого решения становится то, что поддержка ECDSA в резолверах никоим образом не является всеобщей. Недавно проведенные измерения указывают на то, что один из каждых шести пользователей использует резолвер, обеспечивающий валидацию ответа, подписанного с помощью алгоритма RSA, но не может выполнить проверку ответа, подписанного с помощью ECDSA. Изменение протокола несет риск фактического выключения DNSSEC-валидации для одного из классов резолверов DNS, а также для пользователей, находящихся «позади» этих резолверов DNS.

Вывод из всех этих рассуждений заключается в том, что в данном случае, а именно при первом изменении ключа KSK, изменение, вводимое при смене ключа, намеренно ограничивается значением ключа, при этом не предусматривается изменение протокола или размера ключа. Это отражает консервативный принцип работы: если вы собрались изменить что-то, что никогда не менялось в прошлом, то ограничившись изменением лишь одного атрибута можно ограничить риск отрицательного результата. Это не означает, что задача не сопряжена с риском. Существуют серьезные риски, связанные с этой сменой ключа.

Риски

Имеется целый ряд аспектов риска, связанных с этой сменой ключа.

Перед тем как подробно рассказывать о рисках, необходимо выполнить первый шаг – количественно оценить величину риска.

Сколько пользователей может быть потенциально затронуто сменой ключа KSK? В настоящее время примерно 87% всех уникальных запросов, проходящих через полномочные серверы доменных имен, включают как опцию EDNS0, так и набор битов DNSSEC OK. Другими словами, 9 из 10 пользователей направляют свои запросы резолверам, которые запрашивают цифровую подпись DNSSEC у полномочных серверов доменных имен. Однако запрос данных и их использование, судя по всему, являются двумя разными концепциями. Лишь одна треть из этих запросов сгенерирует последующий набор запросов, необходимых для валидации результата с помощью DNSSEC. Эта цифра, соответствующая 30% от общего количества пользователей, ближе к оценке общего пула риска для смены ключа KSK.

Однако риск сбоя в работе, возможно, не столь велик. Если результат попытки валидации будет неудачным, то половина этого потока запросов переключится на использование резолверов без валидации, тогда как только оставшаяся половина, или 15% всех пользователей, примут ошибку валидации.

Основываясь на этих данных, можно отметить, что изменение материала точки доверия может иметь негативные последствия для примерно 30% пользователей Интернета. Учитывая то, что одна половина этих пользователей в случае отказа переключится на пути без валидации, это подразумевает, что в худшем случае приблизительно 15% от общего числа пользователей может до такой степени почувствовать негативное влияние этой смены ключа, что, если их резолверы потеряют точку доверия KSK, то они не смогут определить все имена DNS, ~~подписанные с помощью DNSSEC~~.

~~Последняя часть этого предложения также важна для оценки риска. Это не значит, что в худшем случае 15% пользователей останутся совершенно без услуг DNS. Это означает, что 15% пользователей не смогут транслировать имена, подписанные DNSSEC. Точные цифры недоступны, но известно, что в то время как значительное число резолверов готово осуществить валидацию ответов, гораздо меньшее число DNS-имен подписаны. Таким образом, теоретический максимум 15% пользователей ослабляется наблюдением, что только незначительная часть всех имен подписана.~~

Я оставлю здесь оригинальный текст, перечеркнув его, в качестве иллюстрации того, что в тех случаях, когда дело касается DNS, сле-

дует всегда проявлять чрезвычайную осторожность в наших предположениях. Мое предположение о том, что это затронет только определение имен, подписанных с использованием DNSSEC, фактически не является правильным. Поскольку корневая зона подписана, валидирующий резолвер попытается удостовериться в том, что предположительно неподписанный ответ DNS действительно не подписан, и что это не является результатом попытки некоей третьей стороны подменить ответ. Поэтому резолвер попытается найти точку в пути преобразования имени, в которой состояние подписания DNSSEC переключается с подписанного на неподписанное, и удостоверить это состояние, тем самым убеждая себя, что ответ действительно не подписан. Это означает, что любой из этих валидирующих резолверов не сможет предоставить никакого ответа, поскольку его состояние точки доверия не соответствует корневому. Если клиент выключит все проверки DNSSEC (задаст бит Checking Disabled (проверка деактивирована) в EDNS0), то резолвер ответит на все запросы, однако во всех других случаях – как для подписанных, так и для неподписанных имен – он возвратит ответ SERVFAIL. Это значительно повышает риск сбоя.

Что может пойти не так?

Главный риск – это невозможность загрузить новый ключ KSK как доверительный ключ из-за неспособности выполнить процедуру согласно RFC 5011. Один класс уязвимых резолверов DNS имеет активированную валидацию DNSSEC, но не поддержку RFC 5011. Это может быть относительно редкой комбинацией, однако Интернет поддерживает самое разнообразное программное обеспечение, и было бы опрометчиво утверждать, что такая комбинация просто не существует. Вероятно, она все-таки существует, однако очень трудно оценить, какое количество резолверов относится к этой категории. Возможно, более частым случаем являются те резолверы DNS, локальная конфигурация которых выключает «автоуправляемые» доверительные ключи. Такая настройка фактически не дает резолверу загрузить новое значение ключа KSK при его публикации в корневой зоне. И опять, изначально просто невозможно определить, сколько резолверов работают с вручную сконфигурированными ключами, и сколько пользователей находятся «позади» таких резолверов, а также окажутся ли готовыми системные администраторы к ручной загрузке новых ключей KSK при их объявлении в корневой зоне. Существуют резолверы, которые используют текущий достоверный ключ KSK через локальный конфигурационный файл, но которые активируются в закрывающемся 30-дневном окне перед сменой ключа KSK. Эти резолверы не увидят новый ключ KSK в течение периода «дополнительного удержания», продолжающегося полные 30 дней, но, тем не менее, ожидается, что они будут следовать процедуре смены ключа KSK. И наконец, существуют резолверы, использующие устаревшую среду конфигурирования, которые активируются после смены ключа KSK. Эти резолверы будут отброшены в сторону и не смогут действовать как валидирующие резолверы DNSSEC до тех пор, пока новое значение ключа KSK не будет загружено в их локальную конфигурацию.

Вторым основным риском является неспособность загрузить новый ключ KSK из-за проблем, связанных с большими по размеру DNS-ответами. Размер подписанного ответа на запрос о получении набора RRset DNSKEY корневой зоны обычно колеблется между 736 и 883 октетами (байтами). Этот размер увеличивается в ходе смены ключа ZSK, когда в набор RRset DNSKEY загружены два значения ключа ZSK. Ожидается, что могут возникнуть проблемы с протоколом UDP, если размер ответа начнет приближаться к лимиту полезной нагрузки в 1.232 октета для нефрагментированного протокола пакета UDP в IPv6. Кроме того, существует общий лимит в 1.500 октетов для максимального размера IP-пакетов в большей части Интернета, который (лимит) соответствует полезной нагрузке UDP в IPv6, равной 1.452 октета, и полезной нагрузке UDP в IPv4, равной 1.472 октета. При введении нового ключа KSK в набор RRset DNSKEY размер подписанного ответа будет равен 1.011 октетам, а в последние 10 дней непосредственно перед сменой ключа KSK будут существовать два значения ключа KSK и два значения ключа ZSK, что в сумме составляет 1.158 октетов полезной нагрузки DNS. Аннулирование старого ключа KSK предусматривает добавление значения старого ключа KSK в набор RRset DNSKEY и подписание с использованием обоих ключей KSK – старого и прибывающего. Это сгенерирует самый большой размер ответа, равный 1.297 октетам.

Конечно, это предполагает, что ключ ZSK корневой зоны представляет собой постоянное 1024-битовое значение. Если ключ ZSK увеличится в размере, то соответствующий размер пакета также должен вырасти. Хотя в настоящее время 2048-битовый ключ KSK, по-видимому, не представляет собой проблему, то же самое нельзя сказать о 1024-битовом ключе ZSK. Несмотря на то, что никто не утверждает, что выполнил факторизацию ключа такого размера в течение любого полезного промежутка времени прямо сейчас, многие государственные агентства больше не считают 1024-битовые ключи достаточно стойкими. Переход на 2048-битовый ключ RSA для ZSK добавит еще 128 октетов к размеру этих ответов.

Например, см. публикацию NIST 800-57, Часть 1, версия 4, в которой отмечается, что «комбинации размера ключа/алгоритма, которые имеют оценочную стойкость защиты менее 112 битов [2014-битовые ключи RSA обладают этой стойкостью защиты], больше не утверждаются для обеспечения криптографической защиты Информации федерального правительства [США]».

Возможно, существуют сетевые тракты, которые не обеспечивают передачу пакетов UDP с полезной нагрузкой размером 1.297 октетов. Безусловно, существует вероятность, что имеются сетевые тракты, создающие проблемы для пакетов UDP с полезной нагрузкой размером 1.158 октетов. В этом случае резолвер может попытаться уменьшить размер буфера EDNS0, намекая полномочному серверу доменных имен на уменьшение количества данных, загруженных в дополнительный раздел, и стараясь уменьшить размер ответа. Если на данном этапе сервер не способен выполнить такое уменьшение, то он отправит обратно усеченный ответ UDP и тем самым просигнализирует резолверу о том, что тот должен повторить попытку отправить запрос с использованием транспорта TCP. В этом случае мы можем опять ожидать появления некоторых проблем. DNS через TCP поддерживается не повсюду, и поэтому может также закончиться неудачей.

План Б

Таким образом, мы можем с уверенностью ожидать некоторого «урона» при этой смене ключа KSK. Какой уровень урона будет чрезмерно большим и что можно сделать для смягчения последствий?

Мы ожидаем, что некоторые резолверы не смогут странсировать имена DNS при переключении ключа KSK (Шаг 3 на Рис. 4). В этом случае урон будет нанесен практически немедленно, и некоторое подмножество резолверов DNS, обеспечивающих валидацию DNSSEC, не сможет определять имена, подписанные с помощью модулей DNSSEC. Вероятно, что многие из этих затронутых резолверов могут быть очень быстро исправлены при помощи ручной загрузки

нового ключа KSK в качестве доверительного либо посредством их переконфигурирования с полным запретом на выполнение валидации DNSSEC.

Однако существует второй период уязвимости, в течение которого мы ожидаем, что некоторые резолверы DNS не смогут определять имена после аннулирования старого ключа KSK (Шаг 7 на Рис. 4). Причиной станет то, что в течение этого периода размер ответа DNSKEY вырастет до 1.297 октетов, и это вызовет проблемы у части резолверов, особенно в случае использования UDP через IPv6, поскольку размер такого ответа превысит гарантированный размер нефрагментированного пакета IPv6, равный 1.280 октетам, после того, как заголовки UDP и IPv6 (48 октетов) будут добавлены к полезной нагрузке DNS. Экспериментальные исследования (см. раздел 6.1.2 отчета проектной группы) показывают, что «этот 1% резолверов, которые стабильно сталкиваются с отказами два или большее число раз, используются менее чем тремя тысячами оконечных систем или 0,04% оконечных систем в рамках выборки».

Как часть потенциального «Плана Б», который может быть задействован при смене ключа KSK, отчет проектной группы содержит следующие рекомендации:

Рекомендация 14: Для того, чтобы обеспечить поддержку ряда потенциальных вариантов операционной обстановки, которые могут потребовать отката изменений, внесенных в корневую зону в ходе каждого этапа смены ключа KSK, необходимо генерировать Подписанные запросы на получение ключа [SKR, Signed Key Request] с использованием применявшегося ранее ключа KSK, запросы SKR с использованием как применявшегося ранее, так и поступившего ключей KSK и запросы SKR с использованием поступившего ключа KSK. Кроме того, проектная группа рекомендует двойное подписание в качестве предпочтительного механизма для ответа на требование по выполнению отката в Квартале 2 процедуры смены ключа.

[Эта рекомендация заключается в том, чтобы заранее подготовить набор ключей, чтобы, если возникнет необходимость в откате смены KSK ключа, то этот набор был бы уже доступен администраторам корневой зоны.]

Рекомендация 15: Партнеры по управлению корневой зоной должны выполнить или поручить выполнение программы измерений, которая способна определить влияние изменений на поведение валидирующих резолверов DNSSEC, а также способна оценить группу оконечных узлов, на которые негативно повлияли изменения в поведении валидирующих резолверов.

[Эта рекомендация заключается в том, что менеджеры корневой зоны должны организовать непрерывное измерение в рамках всего процесса смены ключа KSK.]

Рекомендация 16: Откат шага в рамках процесса смены ключа необходимо инициировать в том случае, если программа измерений показала, что как минимум 0,5% оценочного количества конечных пользователей Интернета было негативно затронуто изменением через 72 часа после того, как каждое изменение было развернуто в корневой зоне. [Эта финальная рекомендация заключается в определении «порогового» ущерба в данном контексте.]

Почему 0,5%? Методы измерения носят относительно грубый характер, и поэтому только проведение измерений в течение расширенного периода времени позволяет их уточнить до возрастающих уровней детализации. Если требуется измерить показатели валидации DNSSEC на уровне дней, то экспериментальная погрешность составляет +/-0,1%, поэтому пороговое значение 0,4% или более низкое не поддается измерению с разумным уровнем достоверности (доверительной вероятности). В связи с этим 0,5% предложено как значение, немного превышающее минимальный измеримый порог при использовании каждодневного метода измерения.

Почему 72 часа? Мы ожидаем, что в первый день или два те операторы резолверов DNS, которые были негативно затронуты, самостоятельно примут меры по исправлению ситуации и восстановят обслуживание своих пользователей. Любой долговременный ущерб, который не был исправлен локальными действиями, будет, по всей вероятности, очевиден через 72 часа.

Следующие шаги

Однако это никоим образом не означает конец истории. Еще предстоит выполнить много работы.

Нам, по всей видимости, нужно подумать о проблеме резолверов и точек доверия. Здесь частью фактора неизвестности является неспособность резолверов сообщить о своих точках доверия. Если бы резолверы были способны сообщать о своих точках доверия, предположительно через опцию EDNS0, встроенную в запросы к корневым серверам, то стало бы возможным отследить, в каком масштабе публикация нового ключа KSK была «подхвачена» резолверами в качестве нового доверительного ключа. Конечно, это не приведет к отмене допущений, на которых основана оценка риска, поскольку мы перейдем от двухвидовой классификации резолверов (те, которые выбрали новый ключ KSK в качестве доверительного ключа, против тех, которые это не сделали) к четырехвидовой классификации (добавляем к предыдущей классификации резолверы, которые способны сообщать о своих доверительных ключах, против тех, которые не способны это сделать).

Мы не можем продолжать увеличивать размер ключа RSA, учитывая ограничения, налагаемые размером пакета UDP, и превратности фрагментации пакетов UDP. Возможно, следующий ключ KSK должен быть заменен на ключ с использованием алгоритма ECDSA, и, возможно, мы должны подумать об одновременном переходе от ZSK к ECDSA.

Кроме того, в текущей среде не существует никаких условий по любому виду чрезвычайной смены ключа KSK. Если используемый ключ KSK больше не доступен, либо если он был раскрыт, то модель транзитивности доверия, в рамках которой старый ключ подписывает новый, больше нельзя использовать для распространения нового ключа KSK. Возможно, настало время подумать о предварительной подготовке ключей KSK и о поддержании некоего набора ключей KSK, объявленных для периода «дополнительного удержания». В результате, если текущий ключ KSK больше не будет доступен, либо если он будет раскрыт иным образом, появится возможность в очень короткие сроки перейти к предварительно подготовленному ключу KSK.

Источник: Rolling the Root, http://www.potaroo.net/ispcol/2016-03/rolling.html

Введение в Simple Cloud Identity Management

Крис Филипс (Chris Phillips)

С ростом числа и популярности различных облачных услуг все острее встает задача надежного удостоверения идентичности пользователя и защиты этой информации. Без широкого применения стандартного способа для создания учетных записей пользователей компании вынуждены создавать собственные системы. Это, в свою очередь, ведет к удорожанию таких систем, недостаточной защищенности и создает серьезные трудности при переходе пользователя между провайдерами. Протокол SCIM предлагает прагматичное решение этой проблемы.

Работа над простым управлением идентичностью в облаках (Simple Cloud Identity Management или SCIM) перешла в фазу разработки стандарта в марте 2012 года во время IETF 83, завершив за собой «полный сбор» на BoF-сессии. Чартер рабочей группы SCIM был представлен директорам областей месяцем позже и обсуждался в многочисленных сообществах по управлению идентичностью и доступом, таких, как Internet Identity Workshop (IIW), рабочие группы Internet2 и TERENA, в рамках Kantara Initiative и в нескольких информационно-разъяснительных кампаниях участников SCIM.

Что такое SCIM?

Протокол SCIM использует прагматичный подход к проблеме удостоверения идентичности пользователя среди многочисленных провайдеров облачных услуг. Слово Simple (простое) в названии протокола появилось отнюдь не случайно; это принцип, который использовали участники для эволюционного развития концепции и который, как они надеются, будет по-прежнему применяться при ее прохождении через IETF на пути к превращению в формальный стандарт. На веб-сайте SCIM размещена фраза, которая кратко резюмирует этот подход: «По сути, сделать это быстро, дешево и просто, обеспечив перемещение пользователей в облако, из облака и по облаку».

Почему именно теперь?

Без широкого применения стандартного способа для создания учетных записей пользователей, сервисы вынуждены создавать собственные системы. В свою очередь, любой компании, ведущей бизнес с таким сервисом, приходится нести затраты на использование специализированного интерфейса конфигурирования для каждого сервиса и специализированной схемы, которая практически не подлежит повторному использованию. Конфигурирование внутри самих организаций испытывает такие же проблемы.

Хотя в этой области и существуют стандарты, их принятие и распространение остается на низком уровне. Перед нами встает неожиданная проблема масштабирования - вместо того, чтобы беспокоиться об общей масштабируемости, основной вопрос касается возможности масштабирования до требуемого размера. Организации может требоваться только незначительная часть функциональности, предлагаемой этими протоколами, для возможности работы с соответствующей долей ресурсов и инфраструктуры.

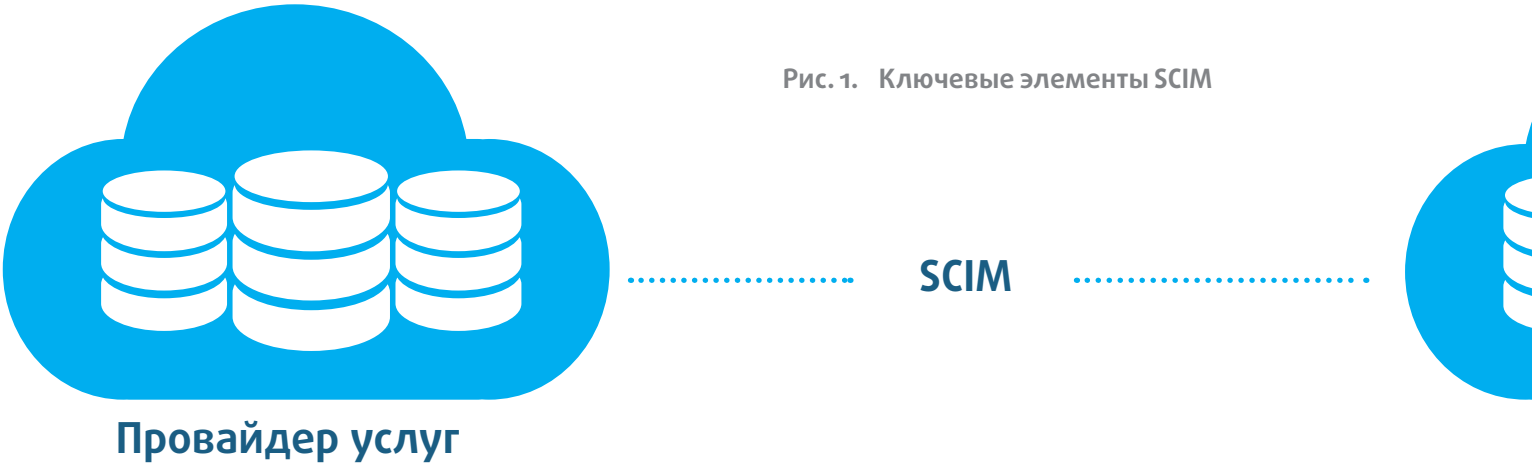


Рис. 1. Ключевые элементы SCIM

Прагматичный подход SCIM привлекателен тем, что он задуман быть «проворным» и менее обременительным для внедрения по сравнению с существующими протоколами, а кроме того, его применение более эффективно и экономично, чем построение и обеспечение работы специально созданной среды конфигурирования.

Протокол

Протокол SCIM предоставляет общую пользовательскую схему и модель расширения, выраженные в формате JavaScript Object Notation (JSON)1 или формате XML через HTTP с помощью программного интерфейса Representational State Transfer (RESTful (https://ru.wikipedia.org/wiki/REST)). На рис. 1 показаны следующие ключевые элементы SCIM:

• провайдер услуг, который хранит обрабатываемую информацию об идентичности;

• потребитель, который представляет собой веб-сайт или приложение, использующее протокол SCIM для управления данными идентичности, которые поддерживаются провайдером услуг;

• ресурсы, которые представляют собой управляемые провайдером услуг артефакты, содержащие один или несколько атрибутов.

Запросы SCIM составляются с помощью операций HTTP, а ответы возвращаются внутри тела HTTP-отклика, отформатированные как JSON или XML, в зависимости от запроса; при этом статус запроса указывается как в коде состояния HTTP, так и в теле запроса.

Операции и ожидаемые действия для HTTP

Действие операции **HTTP**

GET – извлекает ресурс полностью или частично.

POST – создает новый ресурс или массово модифицирует ресурсы.

PUT – модифицирует ресурс с использованием полного, указанного потребителем ресурса (замена).

PATCH – модифицирует ресурс с использованием набора указанных потребителем изменений (частичное обновление).

DELETE – удаляет ресурс.

Полную подробную информацию об откликах протокола можно найти в спецификации протокола SCIM (https://datatracker.ietf.org/doc/rfc7644).

Схема

Схема SCIM была создана под влиянием подхода, использованного в Portable Contacts (http://www.portablecontacts.net/draft-schema.html), вместе с некоторыми дополнительными элементами, взятыми у исходных участников. По сравнению с другими форматами модель Portable Contacts обеспечивает дополнительную гибкость отображения сложности данных, что позволяет отражать сложные отношения данных на уровне пользователя. Сохраняя приверженность простоте, основная схема SCIM нацелена на охват 80% базовых атрибутов пользователя, позволяя внедрить ее максимально быстро и просто. Если отображения между используемым набором идентичности и SCIM не существуют, то доступны расширения для адаптации схемы. Конечные точки SCIM можно опросить подобно серверам LDAP, что позволяет определить индивидуальные настройки схемы.

Ресурсы с соответствующими конечными точками

Ресурс	Конечная точка	Операции	Описание
User	/Users	GET, POST, PUT, PATCH, DELETE	Извлечение/добавление/изменение пользователей
Group	/Groups	GET,POST, PUT,PATCH, DELETE	Извлечение/добавление/ изменение групп
Service Provider Configuration	/ServiceProviderConfigs	GET	Извлечение информации о конфигурации провайдера услуг
Schema	/Schemas	GET	Извлечение схемы ресурса
Bulk	/Bulk	POST	Массовая модификация ресурсов

Побочным эффектом такого подхода является то, что протокол SCIM способен инкапсулировать больше данных об идентичности, чем используемый в LDAP профиль inetOrgPerson или SAML (Security Assertion Markup Language). Подход к решению этой проблемы заключается в создании рекомендаций для отображений LDAP и SAML, которые будет управлять преобразованием высокоточной схемы SCIM в формат с низкой точностью. Целевой результат таких отображений – облегчить работу специалистов по внедрению и обеспечить непротиворечивость для тех, кому требуются отображения. Могут быть опубликованы и другие отображения, в зависимости от наличия спроса на них.

SCIM, схема и область действия

Схема была одной из наиболее часто обсуждаемых тем в SCIM и IETF, при этом ставились следующие вопросы:

• следует ли ограничивать значения атрибутов на базе значений

других атрибутов?

- следует ли сделать ожидаемым или обязательным применение определенных методов управления доступом с использованием определенных атрибутов?

- чего ожидать от SCIM в области управления уникальными идентификаторами?

Каждый вопрос был интересен сам по себе в качестве темы управления идентичностью. И все-таки, простота как основополагающий принцип SCIM предполагает, что эти требования должны быть наложены/спрофилированы в самой верхней части спецификации с тем, чтобы обеспечить удовлетворение потребностей каждого уникального варианта использования. Ограничение протокола SCIM минимальной стандартной схемой, имеющей гибкую модель информации и объединенной со структурированным транспортом данных, обеспечивает повышение полезности и поощряет внедрение. В то же самое время, существует возможность использовать SCIM в качестве низкоуровневого строительного блока для более продвинутых прикладных областей, сконцентрироваться на применении политики и делегировать транспортировку данных протоколу SCIM.

Исполняемый код

Там, где это возможно, проводились сеансы совместимости спецификаций для отладки программного обеспечения и получения опыта их применения на практике. Еще до начала работы по стандартизации в IETF были проведены три таких сеанса, при этом второй состоялся в Париже накануне IETF 83, всего в нем было задействовано девять участников. Очные сеансы оказали неоценимую помощь при идентификации пробелов и неоднозначностей, которые подлежат прояснению.

Дальнейшие перспективы

Протокол SCIM находится в состоянии версии 1.0 с декабря 2011 года благодаря активному участию сообщества. Производители используют исполняемый код в течение месяцев - и целый ряд из них включили SCIM в состав ключевых возможностей своих продуктов7, собирая благодаря этому ценный опыт в условиях реальной обстановки, принимая как должное эту технологию и проходя через жизненный цикл своих продуктов. Другие производители остались в стороне либо для того, чтобы посмотреть, наберет ли протокол популярность, либо по причине того, что они испытывают неудобства в связи с неопределенностью, окружающей новый протокол, и ждут, что в дальнейшем произойдет с SCIM и IETF.

Были предложены этапы реализации проекта концепции с целью принятия основной схемы SCIM, определения интерфейса RESTful и вариантов использования в качестве действующего документа к концу лета 2012 года, и формализации привязок SAML и отображений LDAP к лету 2013 года. Это позволит заполнить некоторые пробелы для тех производителей, которые ждут развития событий, и создаст определенность в других областях протокола.

Протокол SCIM находится в состоянии версии 1.0 с декабря 2011 года благодаря активному участию сообщества. Производители используют исполняемый код в течение месяцев - и целый ряд из них включили SCIM в состав ключевых возможностей своих продуктов, собирая благодаря этому ценный опыт в условиях реальной обстановки, принимая как должное эту технологию и проходя через жизненный цикл своих продуктов.

Рабочая группа SCIM WG имеет в своей повестке дня целый ряд претендующих на внимание тем, которые мы здесь представим в качестве беглого наброска будущих дискуссий.

Определение и рекомендации для возможных топологий

Описание возможных топологий развертывания поможет идентифицировать, где и каким образом можно применить SCIM в качестве способа для поощрения внедрения. Слово «cloud» (облачное), входящее в состав наименования протокола SCIM, немного искажает смысл, его наличие не должно препятствовать развертыванию SCIM внутри организации. Внутреннее развертывание может быть более привлекательным, чем соединение с производителем продукта SAAS (Software as a Service). При внутреннем развертывании появляются дополнительные возможности для кастомизации, а также более полно реализуются владение и контроль над процессами конфигурирования, поэтому развертывание SCIM обеспечивает равную, если не большую полезность, упрощая внутреннюю среду подготовки и консолидируя компоненты в рамках общей модели с SCIM в качестве одного из основных элементов.

Детализация подходов к обеспечению безопасности конечных точек

Проблема заключается в том, что один размер не подходит для всех ситуаций, и не все узлы равно оснащены для выполнения одной модели вместо другой. Протокол SCIM требует использования TLS 1.2 и рекомендует применять OAuth Bearer Token в качестве метода для стимулирования взаимодействия между конечными точками SCIM, однако остается достаточно гибким, разрешая использование других протоколов.

Одной из привязок, которая изучается вместе с протоколом SCIM, является язык SAML и то, каким образом он может и должен взаимодействовать с SCIM. С точки зрения безопасности, SAML предоставляет SCIM модель доверия через федерации SAML (частные или общедоступные) и поднимает другие интересные вопросы в области безопасности. Необходимо ли в равной степени доверять всем конечным точкам внутри одного доверительного набора? И это лишь один из многих вопросов в этой сфере. Вероятно, что среды SAML получат выгоду от возможности расширить свой опыт с помощью формализации вокруг подготовки конечных точек SAML.

Схема

Существует целый ряд пунктов для обсуждения, которые могут касаться схемы. Некоторые из них уже упоминались, за исключением более тонкого и скользкого - «еще одной функциональной возможности» подхода к дополнениям схемы. Это проявляется в возникновении все большего числа атрибутов, находящихся вне основной схемы, до тех пор, пока в расширении становится больше атрибутов, чем в ядре. Протокол SCIM является достаточно гибким для того, чтобы это было возможно, но следует ли это поведение поощрять, препятствовать ему или это не должно нас заботить? Является ли

это антишаблоном для укрепления базовой модели атрибутов? Возможно, это приемлемый способ использования SCIM, если он упрощает инфраструктуру в целом, либо это метод для обеспечения неувядаемой популярности схемы и достижения максимальной гибкости с течением лет. Эту тему будет интересно обсудить.

Настоящий краткий экскурс в темы подготовки и конфигурирования высветил некоторые подлежащие дальнейшему исследованию области. По мере того, как протокол SCIM переходит к следующему раунду улучшений, поддержание баланса между простотой, практичностью и гибкостью – даже в том случае, если они противоречат друг другу – позволит повысить долговечность SCIM в качестве инструмента, входящего в состав комплекта промежуточного ПО.

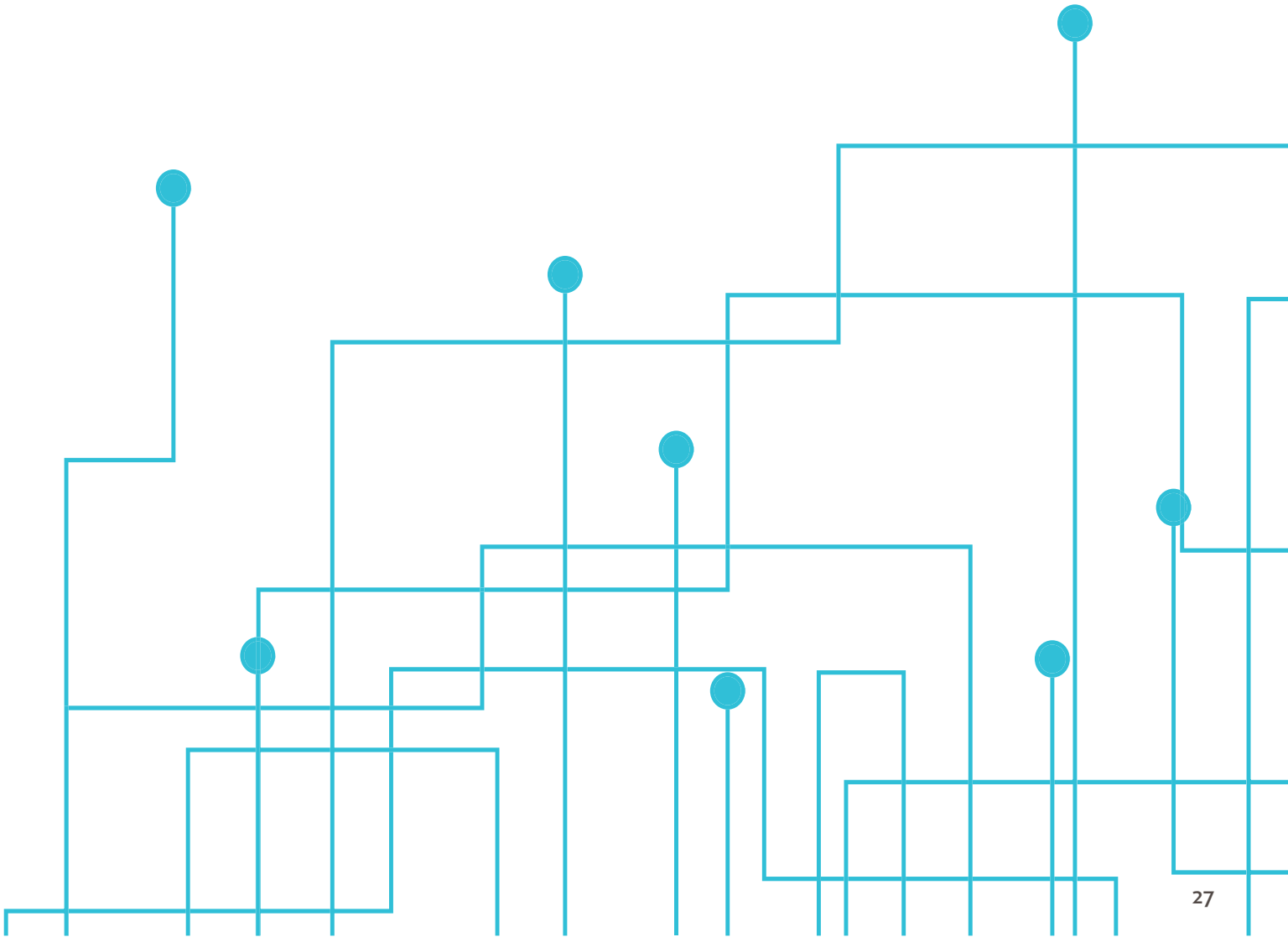
Примечание редактора

Рабочая группа System for Cross-domain Identity Management (SCIM) была учреждена группой IESG 21 июня 2012 года в Прикладной области IETF и закончила свою работу в 2014, полностью выполнив стандартизацию протоколов и схемы SCIM. Хотя основные концепции SCIM не изменились, любознательный читатель может сам увидеть, как дискуссионные вопросы, обсуждаемые в этой статье, нашли свое отражение в окончательные спецификациях. Основные спецификации SCIM на настоящее время:

RFC7643 System for Cross-domain Identity Management: Core Schema (https://datatracker.ietf.org/doc/rfc7643/) – определяет основную схему SCIM

RFC7644 System for Cross-domain Identity Management: Protocol (https://datatracker.ietf.org/doc/rfc7644/) – определяет протокол SCIM

Источник: Rough Guide, http://www.ietfjournal.org/an-introduction-to-simple-cloud-identity-management/



Согласованная Директива ЕС по кибербезопасности

Агентство Allen & Overy

18 декабря 2015 г. был опубликован согласованный текст Директивы по сетевой и информационной безопасности (NIS Directive). В связи с тем, что кибербезопасность явно становится одним из ключевых бизнес-рисков, введение в рамках Европейского Союза специальных законов, регулирующих эту область, представляется очень важным. Данная статья содержит обзор нового законодательства и оценивает последствия Директивы NIS.

Основные сведения. Директива NIS стала кульминацией процесса, который начался в 2013 году, когда Европейская Комиссия одобрила стратегию ЕС в области кибербезопасности и предложила проект новой Директивы. Директива NIS является одним из важнейших компонентов общей стратегии, направленной на предотвращение кибератак и нарушений в работе сетевых систем, а также предлагающей реакцию на эти угрозы. Европейская Комиссия признала, что инциденты в области кибербезопасности становятся все более частыми и масштабными, характеризуются увеличивающейся сложностью и имеют трансграничную природу. Поскольку такие инциденты могут привести к крупному ущербу для безопасности и экономики, Европейская Комиссия согласилась с тем, что действия по предотвращению угроз и развитию сотрудничества должны быть улучшены, а уровень прозрачности для инцидентов кибербезопасности необходимо повысить.

Поэтому целью Директивы NIS является гарантирование высокого общего уровня безопасности сетевых и информационных систем в рамках ЕС. Для того чтобы этого добиться, было решено обязать государства-участники повысить свою готовность и улучшить сотрудничество друг с другом, а также обязать операторов, которые предоставляют критически важные услуги, связанные с определенными объектами инфраструктуры, и провайдеров отдельных цифровых услуг принять соответствующие меры по управлению рисками безопасности и сообщать о серьезных инцидентах компетентным национальным органам. Все это, по мнению Европейской Комиссии, является жизненно важным для обеспечения безопасной и вызывающей доверие цифровой среды в рамках всего ЕС.

То, что начиналось как предложенная Европейской Комиссией инициатива по коренной реформе, было до некоторой степени размыто Европейским Парламентом и Советом. Это привело к длительному обсуждению с участием этих трех институтов. Произошла задержка при согласовании Директивы NIS, но в конечном счете был достигнут компромисс.

Существовали серьезные разногласия, касающиеся включения Европейской Комиссией в сферу действия Директивы NIS «посредников Интернета» или «платформ цифровых услуг» в рамках первоначального предложения. Это включение было отклонено Европейским Парламентом, а также значительным числом государств-участников. Поэтому итоговое включение в сферу действия Директивы таких объектов, как облачные платформы, интернет-магазины и биржи, а также механизмы онлайнового поиска является важным достижением.

Хотя национальные особенности существуют при реализации любых Директив, Директива NIS особенно сопряжена с противоречиями при ее применении, поскольку большая ее часть определяет действия, которые необходимо выполнить государствам-участникам, оставляя детали на усмотрение таких стран. В особенности, пока еще не совсем ясно, каким образом государства-участники будут реализовывать требования по организации сотрудничества с целью обеспечения скоординированного ответа на инциденты, поскольку в настоящее время их подходы отличаются.

В этой статье мы опишем некоторые ключевые особенности Директивы NIS и то, как они могут повлиять на ведение бизнеса.

Требования к государствам-участникам

Создание национальных систем

Согласно Директиве NIS, государства-участники должны гарантировать, что у них имеется минимальный уровень национальных возможностей и средств, путем создания или определения, а также наделения адекватными ресурсами:

- стратегии в области сетевой и информационной безопасности, определяющей стратегические цели, а также соответствующую политику и регулятивные меры, направленные на достижение и поддержание высокого уровня безопасности сетей и информационных систем;
- одного или нескольких национальных уполномоченных органов для отслеживания реализации NIS на своей территории и для оказания помощи по ее последовательной реализации в рамках ЕС – государства-участники могут поручить эту роль существующему агентству или агентствам;
- единой национальной точки контакта (канал контакта) по вопросу безопасности сетей и информационных систем для установления и поддержания связи между государствами-участниками, группой

взаимодействия и сетью групп реагирования на инциденты, связанные с компьютерной безопасностью (CSIRT, Computer Security Incident Response Team) – государства-участники могут поручить эту роль существующему агентству или агентствам;

- одной или нескольких групп CSIRT, отвечающих за управление рисками и инцидентами.

Взаимодействие между государствами-участниками и их группами CSIRT

Директива NIS также требует организовать расширенное взаимодействие между государствами-участниками, создав:

- группу взаимодействия, составленную из представителей государств-участников, Комиссии и Европейского агентства по сетевой и национальной безопасности (ENISA, Commission and the European Network and Information Security Agency) – чьи функции заключаются в рассылке данных и обмене информацией между ее участниками, а также во взаимодействии при борьбе с угрозами и инцидентами в области кибербезопасности;

- сеть национальных групп CSIRT, составленную из представителей групп CSIRT государств-участников и CERT-EU (Группа реагирования на компьютерные происшествия для институтов, организаций и агентств ЕС) с привлечением Европейской Комиссии в качестве наблюдателя, целью которой является организация быстрого и эффективного операционного взаимодействия при помощи, помимо прочего, обмена информацией и поддержки государств-участников при разрешении трансграничных инцидентов на добровольной основе.

Требования к операторам жизненно важных услуг (Essential Services)

Кто является «оператором жизненно важных услуг»?

Директива NIS налагает обязательства как на государственных, так и на частных «операторов жизненно важных услуг». Эти услуги относятся к типам, перечисленным в Приложении II (см. ниже), и включают энергетику, транспорт, банковское обслуживание, инфраструктуру финансовых рынков, здравоохранение, подачу и распределение питьевой воды, цифровую инфраструктуру. Такие организации должны соответствовать всем нижеследующим критериям:

- организация предоставляет услугу, которая имеет жизненно важное значение для поддержания критической социальной и/или экономической деятельности;

- предоставление этой услуги зависит от сетевых и информационных систем;

- инцидент, негативно влияющий на сетевые и информационные системы такой услуги, будет иметь значительные разрушительные последствия для ее предоставления.

Каждое государство-участник идентифицирует организации, которые соответствуют определению «оператора жизненно важных услуг» согласно вышеперечисленным критериям, учрежденные на своей территории, что означает эффективную и реальную деятельность в рамках стабильной структуры (филиалы и дочерние предприятия включаются в это определение). Этого можно добиться за счет принятия списка, перечисляющего всех операторов жизненно важных услуг, или при помощи принятия объективных, количественно измеряемых критериев (например, объем произведенной продукции оператора жизненно важных услуг или количество пользователей), которые позволяют определить те организации, к которым будет применяться Директива NIS, и те, к которым она не будет применяться. При определении значимости потенциального разрушительного действия государства-участники будут учитывать отраслевые факторы и как минимум следующие межотраслевые факторы:

- количество пользователей, полагающихся на услугу, предоставляемую организацией (т.е. объем ее деятельности на территории государства);

- •зависимость других секторов, перечисленных в Приложении II, от услуги, которая предоставляется организацией;

- влияние, которое инциденты смогут оказать (по показателю степени и продолжительности) на экономическую и социальную деятельность либо на общественную безопасность;

- доля организации на рынке;

- географический охват в отношении области, которая может быть затронута инцидентом;

- важность организации для поддержания достаточного уровня услуги, принимая во внимание доступность альтернатив для предоставления такой услуги.

Типы организаций, которые могут являться «операторами жизненно важных услуг»

В Приложении II к Директиве NIS перечислены или даны перекрестные ссылки на типы государственных и частных организаций, которые могут являться «операторами жизненно важных услуг». Сюда относятся следующие секторы:

- цифровая инфраструктура – точки обмена интернет-трафиком, реестры доменных имен высшего уровня и поставщики услуг системы доменных имен;

- энергетика – поставщики электроэнергии/газа, операторы распределительных систем, операторы передающих систем, операторы систем хранения, операторы СПГ (сжиженного природного газа) и операторы, управляющие средствами производства нефти и газа, нефтеперерабатывающими и очистными установками и заводами;

- транспорт – воздушные и морские перевозчики, операторы управления трафиком и перевозками, аэропорты, железные дороги, операторы управления дорожным движением и операторы интеллектуальных транспортных систем;

- банковское обслуживание – кредитные организации в соответствии с Нормами требований к капиталу (Capital Requirements Regulation) (575/2013);

- инфраструктура финансовых рынков – фондовые биржи и центральные контрагенты;

- здравоохранение – поставщики услуг здравоохранения (включая больницы и частные клиники);

- питьевая вода – организации, занимающиеся поставкой и распределением питьевой воды.

Безопасность и отчетность об инцидентах

Если оператор жизненно важных услуг подпадает под действие Директивы NIS и размещается в государстве-участнике, то он должен:

- принять адекватные и пропорциональные технические и организационные

меры по управлению рисками, включая меры по предотвращению и минимизации влияния инцидентов, которые могут негативно затрагивать сети и информационные системы, используемые в целях обеспечения непрерывности таких услуг;

- выполнять требования схем отчетности, которые будут установлены государством-участником, и согласно которым организация должна «без излишнего промедления» уведомлять уполномоченный орган или группу CSIRT «об инцидентах, которые оказывают значительное влияние на непрерывность предоставляемых ими жизненно важных услуг».

«Инциденты» - это те события, которые оказывают реальное негативное влияние на безопасность сетевых и информационных систем. Директива NIS устанавливает параметры, которые необходимо учитывать при оценке «значимости» влияния любого инцидента:

- количество пользователей, затронутых прекращением оказания жизненно важных услуг;
- продолжительность инцидента;
- территориальное распределение с учетом области, затронутой инцидентом.

Необходимо отметить, что модель, на которой основана Директива NIS, представляет собой существующую Рамочную директиву ЕС для электронных коммуникаций (2002/21/ЕС), которая в настоящее время требует от телекоммуникационных компаний принятия мер по управлению рисками и уведомления регуляторов о серьезных нарушениях сетевой безопасности. Поэтому телекоммуникационные компании исключены из-под действия Директивы NIS.

В тех случаях, когда оператор жизненно важных услуг полагается на стороннего поставщика цифровых услуг (см. ниже) для предоставления своих услуг, обязательство по уведомлению об инцидентах, оказывающих значительное влияние на непрерывность предоставления жизненно важных услуг, должно быть возложено на оператора, а не на провайдера цифровых услуг.

Правоприменение и санкции

Уполномоченные органы могут потребовать от операторов жизненно важных услуг:

- предоставить информацию, необходимую для оценки безопасности их сетей и информационных систем, включая задокументированные политики безопасности;
- предоставить доказательства эффективной реализации политик безопасности, например, результаты аудита безопасности, проведенного уполномоченным органом или правомочным аудитором, в последнем случае предоставить эти результаты, включая базовые свидетельства, в распоряжение уполномоченного органа.

По результатам оценки либо информации, предоставленной оператором жизненно важных услуг, либо материалов аудита безопасности, уполномоченный орган может выдать оператору жизненно важных услуг обязывающие инструкции по исправлению практик своей операционной деятельности.

Требования к провайдерам цифровых услуг

Что такое «цифровая услуга»?

Директива NIS налагает обязательства на провайдеров «цифровых услуг». К ним относятся услуги Информационного общества (согласно определению, данному в Статье 1(b) Директивы 2015/1535) описанных ниже типов.

В Приложении III к Директиве NIS (вместе с соответствующей декларативной частью) перечисляются типы цифровых услуг, на которые распространяется действие Директивы. Эти типы услуг включают:

- интернет-магазины и биржи – Директива охватывает услуги, позволяющие онлайновым покупателям и/или трейдерам осуществлять онлайновые продажи и заключать сервисные контракты. Онлайновые услуги, которые позволяют сравнивать цену конкретных продуктов или услуг, предлагаемых разными трейдерами, и затем перенаправляют пользователя на сайт предпочитаемого трейдера для покупки продукта, не включены в сферу действия настоящей Директивы;
- интернет-поисковики – услуги, которые позволяют пользователю осуществлять поиск, теоретически, по всем веб-сайтам или по всем веб-сайтам на конкретном языке с помощью запросов, входят в сферу действия настоящей Директивы. Директива не распространяется на предоставление функций поиска, которые ограничиваются контентом конкретного веб-сайта;
- сервисы облачных вычислений – существует целый ряд разных моделей предоставления услуг облачных вычислений. Директива распространяется на услуги, которые обеспечивают доступ к масштабируемому и гибкому пулу разделяемых компьютерных ресурсов. Это означает, что сюда относятся сервисы облачных вычислений, которые способны реагировать на увеличение или уменьшение спроса на ресурсы или вычислительные мощности со стороны многочисленных пользователей, получающих доступ к сервису в разных географических районах, однако при этом обработка выполняется отдельно для каждого пользователя, хотя сервис и предоставляется на том же электронном оборудовании.

Территориальная сфера действия и нормативно-правовая ответственность

Любое юридическое лицо, предоставляющее «цифровую услугу» указанного выше типа – «провайдер цифровых услуг» – должно выполнять соответствующие обязательства согласно Директиве NIS, если это лицо предлагает услуги на территории любого государства-участника.

Подобно Общему регламенту о защите персональных данных и его концепции «единого окна», считается, что провайдер цифровых услуг подпадает под юрисдикцию того государства-участника, на территории которого находится его основной орган управления (т.е. страна-участник его головного офиса в ЕС). Если провайдер цифровых услуг ведет деятельность за пределами ЕС, но предлагает свои услуги в государстве-участнике, то он должен назначить «представителя», находящегося в этом государстве-участнике, и будет подпадать под юрисдикцию того государства-участника, в котором располагается этот представитель. Существует форма механизма взаимодействия, которая требует оказания помощи от других заинтересованных государств-участников (например, стран, где размещаются сети и информационные системы).

Будет очень интересно понаблюдать, будет ли зависеть выбор организаций от подхода, применяемого разными государствами-участниками, или они поместят свои «главные органы управления» в разных государствах-участниках из-за отличающихся регуляторных обязательств.

Безопасность и отчетность об инцидентах

Если провайдер цифровых услуг подпадает

под действие Директивы NIS, то он должен:

- принять адекватные и пропорциональные технические и организационные меры по управлению рисками. Эти меры должны обеспечивать адекватный уровень безопасности с учетом:

  безопасности систем и средств производства;

  управления инцидентами;

  управления непрерывностью бизнеса;

  мониторинга, аудита и тестирования;

  соблюдения международных стандартов.

- принять меры в целях обеспечения непрерывности предоставления услуг при помощи предотвращения и минимизации влияния инцидентов, которые негативно затрагивают безопасность используемых сетей и информационных систем;

- выполнять требования схем отчетности, которые будут установлены государством-участником, и согласно которым организация должна «без излишнего промедления» уведомлять уполномоченный орган или группу CSIRT о любом «инциденте», который оказывает «значительное влияние» на предоставление цифровой услуги.

Директива NIS устанавливает параметры, которые необходимо учитывать при оценке влияния любого инцидента:

- количество пользователей, затронутых инцидентом, в особенности, пользователей, которые полагаются на эту услугу при предоставлении своих собственных услуг;

- продолжительность инцидента;

- территориальное распределение с учетом области, затронутой инцидентом;

- степень нарушения функционирования услуги;

- степень влияния на экономическую и социальную деятельность.

Правоприменение и санкции

Уполномоченный орган может потребовать от провайдера цифровых услуг:

- предоставить информацию, необходимую для оценки безопасности его сетей и информационных систем, включая документально оформленные политики безопасности;

- исправить любую ситуацию, связанную с неспособностью выполнить релевантные требования, установленные в Директиве.

Провайдеры цифровых услуг должны подвергаться исключительно ретроспективному (по факту) надзорному контролю со стороны уполномоченных органов, которые должны принимать меры только в случае получения доказательств того, что провайдер цифровых услуг не выполняет требования Директивы. Такие свидетельства могут быть предоставлены самим провайдером цифровых услуг, уполномоченным органом, включая уполномоченный орган другого государства-участника, или пользователем услуги. Провайдер цифровых услуг, в отличие от оператора жизненно важных услуг, не обязан предоставлять соответствующему уполномоченному органу свидетельства того, что он соблюдает требования Директивы. Необходимо отметить, что Европейская Комиссия не имеет намерений, чтобы Директива создавала общее обязательство для уполномоченного органа по надзору за провайдерами цифровых услуг.

В преамбуле Комиссия предполагает, что требования по обеспечению безопасности для провайдеров цифровых услуг должны быть менее строгими, чем аналогичные требования, предъявляемые к операторам жизненно важных услуг, поскольку степень риска для безопасности предоставляемой услуги будет более высокой для организаций, относящихся к последнему классу. Обязательства провайдеров цифровых услуг согласно Директиве NIS не будут применяться к микропредприятиям и малым компаниям, которые признаются таковыми в соответствии с Рекомендациями Комиссии 2003/361/ЕС.

Общие требования

Трансграничное совместное использование информации

Любое уведомление об инциденте, отправленное оператором жизненно важных услуг/провайдером цифровых услуг, должно также включать информацию, позволяющую уполномоченному органу (или группе CSIRT) определить любое трансграничное воздействие инцидента. Базируясь на этой информации, уполномоченный орган (или группа CSIRT) должен проинформировать другие затронутые государства-участники в том случае, если инцидент оказывает значительное воздействие. При любом подобном раскрытии информации будут соблюдаться коммерческие интересы и интересы безопасности уведомляющей стороны, а также будет обеспечиваться конфиденциальность любой информации.

Раскрытие для неограниченного круга лиц

После консультации с затронутым оператором жизненно важных услуг/провайдером цифровых услуг уведомленный уполномоченный орган или группа CSIRT может сделать общедоступной информацию об отдельных инцидентах, если информированность общественности необходима либо для предотвращения подобного инцидента, либо для устранения последствий продолжающегося инцидента. Что касается уведомлений, отправленных исключительно поставщиками цифровых услуг, уведомленный уполномоченный орган или группа CSIRT на свое усмотрение, после консультации с уведомляющей стороной, информируют общественность в тех случаях, когда такое раскрытие информации находится в общественных интересах.

Стандартизация

Для того чтобы содействовать сближающейся реализации, Директива NIS требует от государств-участников поощрять использование европейских или международно признанных стандартов и/или спецификаций, относящихся к безопасности сетей и информационных систем. Эти стандарты и/или спецификации подробно не описываются в Директиве NIS. Однако Директива предусматривает, что ENISA может сотрудничать с государствами-участниками с целью выработки рекомендаций и инструкций в отношении технических аспектов, которые необходимо учитывать, а также использования уже существующих стандартов, включая национальные стандарты государств-участников. Преамбула предполагает, что может возникнуть необходимость в разработке гармонизированных стандартов, гарантирующих высокий уровень безопасности на уровне ЕС.

Правоприменение и санкции

Государства-участники обязаны вводить в действие «эффективные, пропорциональные и сдерживающие» санкции в случае неспособности оператора жизненно важных услуг/провайдера цифровых услуг выполнить положения Директивы NIS, касающиеся требований безопасности и уведомления об инцидентах. Обязательства в области обеспечения безопасности и уведомления будут применяться к операторам жизненно важных услуг/провайдерам цифровых услуг независи-

мо от того, осуществляют ли они техническое обслуживание своих сетей и информационных систем самостоятельно или передали его на аутсорсинг.

Пока еще не совсем ясно, какой санкционный режим разработают государства-участники в соответствии с требованиями Директивы NIS.

Что Директива NIS означает для бизнеса?

Учитывать возможность быть пойманным

Операторы, работающие в определенных сферах деятельности, чьи услуги являются «жизненно важными», или провайдеры определенных «цифровых услуг» должны знать об обязательствах по соблюдению требований, наложенных на них Директивой NIS, и оценить риски, с которыми они сталкиваются, а также принять адекватные и пропорциональные меры кибербезопасности для защиты своих сетей и информационных систем от несанкционированного доступа. Такие меры могут потребоваться для соблюдения европейских или международно признанных стандартов, установленных государствами-участниками, которые еще должны быть определены.

Важно понять, что в рамках существующих обязанностей необходимо соблюдать осторожность, и согласно корпоративной ответственности либо (в случае компаний, котирующихся на бирже) правилам фондовой биржи, от компаний уже могут фактически потребовать провести оценку таких рисков и принять адекватные меры вне зависимости от Директивы NIS. В любом случае, компаниям рекомендуется реализовать или обновить политики, процедуры и контрольные списки кибербезопасности, возможно, после проведения консультаций с уполномоченным органом или группой CSIRT. Этого могут также потребовать страховщики компании, если осуществляется страхование киберрисков, хотя мы обычно рекомендуем не приобретать страховые полисы, согласно которым страховая защита исключается в случае несоблюдения внутренней политики или процедуры.

Уведомление об инцидентах безопасности

Операторы жизненно важных услуг/провайдеры цифровых услуг должны ввести в действие процедуры для оценки значимости любого инцидента, связанного с безопасностью сети и информации, в соответствии с критериями, установленными в Директиве NIS, для того, чтобы определить необходимость уведомления уполномоченного органа или группы CSIRT и выполнить такое уведомление.

В рамках режима уведомления оператор жизненно важных услуг/провайдер цифровых услуг не обязан информировать любые другие стороны (например, заказчиков, сотрудников или правоохранительные органы). Однако национальный уполномоченный орган или группа CSIRT могут проинформировать общественность в тех случаях, когда информированность общественности необходима либо для предотвращения подобного инцидента, либо для разрешения продолжающегося инцидента, или когда это будет в общественных интересах по иным причинам. Перед тем, как сделать информацию общедоступной, будут проведены консультации с уведомляющей стороной, а ее коммерческие интересы и конфиденциальность информации будут в общем и целом соблюдаться. Уведомление не повлечет за собой повышение ответственности уведомляющей стороны.

Добровольная отчетность

Организации, не подпадающие под действие Директивы NIS, могут – в тех случаях, когда они сталкиваются с инцидентами, оказывающими значительное воздействие на предоставляемые ими услуги – добровольно уведомить соответствующие органы государства-участника, в котором они располагаются. Это может привести к расширению сферы действия требований к отчетности «по обычаю», или в соответствии с инструкциями регулирующего или отраслевого органа.

Потенциал для введения нескольких обязательств об отчетности

Операторы жизненно важных услуг/провайдеры цифровых услуг должны быть осведомлены о том, что от них могут потребовать предоставить несколько отчетов об инциденте. Например, согласно новому Общему регламенту о защите персональных данных, об инцидентах безопасности, которые могут быть связаны с нарушением конфиденциальности персональных данных, необходимо сообщить органу, отвечающему за защиту данных, а также национальному уполномоченному органу или группе CSIRT, согласно Директиве NIS. Аналогичным образом, принятые во многих странах положения о регулировании финансовых услуг уже требуют отчитываться об инцидентах, связанных с нарушением целостности данных о клиентах, или влияющих на непрерывность оказания услуг. Это создает целый ряд потенциальных проблем, включая управление разными триггерами отправки отчетов о нарушениях с разными ожидаемыми сроками.

Преамбула признает эту потенциальную возможность для повышения административной нагрузки, когда инцидент безопасности также связан с нарушением конфиденциальности персональных данных, и предлагает, чтобы агентство ENISA организовало взаимодействие с органами по защите персональных данных и помогло в создании правил, облегчающих отчетность об инцидентах, связанных с нарушением конфиденциальности персональных данных.

Дополнительные национальные требования

Поскольку эта директива носит минимальный гармонизирующий характер, отдельные государства-участники не могут уменьшать уровень требований, установленных в Директиве NIS. Однако по отношению исключительно к операторам жизненно важных услуг государства-участники могут выходить за пределы Директивы NIS и устанавливать в рамках национального законодательства более высокие стандарты для сетевой и информационной безопасности. Это может привести к различиям в реализации Директивы NIS среди государств-участников.

Сроки

Государства-участники имеют в своем распоряжении до 21 месяца, начиная с даты публикации Директивы NIS (ожидается весной), для опубликования национальных законов, реализующих Директиву NIS, и для ввода их в силу.

Передовая практика в сфере отчетности об инцидентах

Как становится ясно по таким инициативам, как Директива NIS, от компаний все больше ожидают, что они будут сообщать об инцидентах безопасности либо отраслевым регулирующим органам, заказчикам и другим затронутым контрагентам, либо широкой общественности. Хорошее «ведение хозяйства» для готовности к уведомлению о нарушениях включает:

- реализацию в рамках всей компании политики NIS, обеспечивающей непрерывную безопасность IT-систем и информации;
- предупредительную идентификацию уязвимых областей в IT-сетях/системах;
- подготовку плана реагирования на ин-

циденты NIS, включая координацию, коммуникацию, криминалистическую экспертизу/расследование, отчетность и – последнее, но не менее важное – планы восстановления;

- создание независимой команды реагирования (идентификация участников и запасных участников, разъяснение их соответствующих ролей, ответственности и определение органов, принимающих решения);

- обеспечение того, чтобы поставщики (и их субподрядчики) реализовали меры безопасности и регулярно предоставляли свидетельства адекватности и эффективности этих мер, а также их соответствия уровню технологического развития;

- реализацию программ обучения и повышения осведомленности для того, чтобы обеспечить осведомленность релевантных сотрудников и поставщиков о плане реагирования NIS и чтобы снабдить их необходимыми ресурсами для его выполнения.

ОГОВОРКА ОБ ОГРАНИЧЕНИИ ОТВЕТСТВЕННОСТИ: Принимая во внимание универсальный характер этой статьи, предоставленная здесь информация может оказаться неприменимой во всех ситуациях, при выполнении действий на основе этой информации необходимо заручиться специальными юридическими рекомендациями, учитывающими конкретную ситуацию.

Примечание редакции: В статье обсуждается проект Директивы ЕС NIS. После опубликования статьи Директива была принята Европейским парламентом 6 июля 2016 года. Хотя небольшие редакционные изменения были внесены в окончательный вариант, они не меняют содержания Директивы и, таким образом, анализ, представленный в статье, остается в силе. Директива вступила в силу в августе 2016 года. Начиная с этого момента государства-члены должны в течение 21 месяца перенести директиву в свои национальные законы и затем в течение шести месяцев определить операторов жизненно важных услуг.

Источник: EU Directive On Cybersecurity Agreed, http://www.jdsupra.com/legalnews/eu-directive-on-cybersecurity-agreed-74898/

Контакт: Игорь Горчаков, партнер, +7 985 991 4913

Обзор, анализ и рекомендации по защите Критической информационной инфраструктуры (Critical Information Infrastructure, CII). Модели управления CII

Настоящая глава описывает три модели управления защитой CII (Critical Information Infrastructure Protection, CIIP), которые используются шестнадцатью исследованными странами-членами ЕС. Управление CIIP относится ко всем структурам и процессам, которые связаны с руководством в области CIIP, осуществляемым государственными (например, государственная администрация или правоохранительные органы) или частными (например, ассоциации, операторы CII, отраслевые группы CSIRT) субъектами (деятельности). Оно может относиться к процессам принятия решений, а также к операционным мероприятиям по защите CII.

Настоящая глава описывает три модели управления защитой CII (Critical Information Infrastructure Protection, CIIP), которые используются шестнадцатью исследованными странами-членами ЕС. Управление CIIP относится ко всем структурам и процессам, которые связаны с руководством в области CIIP, осуществляемым государственными (например, государственная администрация или правоохранительные органы) или частными (например, ассоциации, операторы CII, отраслевые группы CSIRT) субъектами (деятельности). Оно может относиться к процессам принятия решений, а также к операционным мероприятиям по защите CII.

Разные модели иллюстрируют специфические формы управления CIIP, которые определяются их общими характеристиками. Модели не исключают друг друга, а скорее являются точками спектра. Например, централизм управления CIIP в рамках одной страны может меняться, и хотя некоторые страны можно отнести либо к централизованным, либо к децентрализованным, другие страны находятся между этими двумя точками. То же самое справедливо и для степени вовлечения частного сектора. В нижеследующем разделе представлены примеры государств-участников, которые соответствуют определенной модели или её определяющим характеристикам.

Эти модели помогают понять, каким образом организована защита CIIP в отдельных странах-участниках и какие меры и действия в сфере CIIP могут передаваться от одного государства-участника другому. Некоторые меры, предпринятые странами-участниками с централизованным подходом к CIIP, могут не работать в странах, которые придерживаются децентрализованного подхода (и наоборот), из-за отличающихся сфер ответственности, процессов и отношений между соответствующими заинтересованными сторонами. Аналогичным образом меры, предпринятые государством-участником с высоким уровнем участия частного сектора, могут не поддаваться переносу в страны, в которых управление CIIP в основном осуществляется правоохранительными органами или агентствами по чрезвычайным ситуациям (и наоборот). Однако страны-участники с похожими характеристиками в сфере управления CIIP могут лучше подходить для обмена передовым опытом и эффективными мерами CIIP.

Управление CIIP является ключевой особенностью для понимания того, каким образом организована защита CIIP в разных государствах-участниках и до какой степени меры в этой области могут переноситься из одной страны в другую.

Модель 1: Децентрализованный подход

Децентрализованный подход характеризуется следующими особенностями:

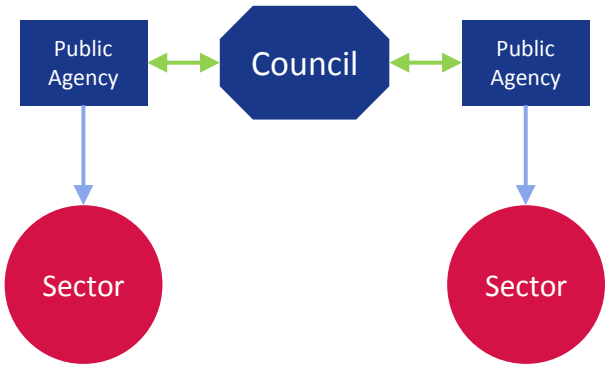
- принцип субсидиарности (разрешение проблем на возможно более низком уровне);
- тесное сотрудничество между государственными агентствами;
- отраслевое законодательство.

Секторная ответственность

Вместо того, чтобы создавать сильное CIIP-агентство со сферой ответственности, включающей все или несколько критически важных секторов, децентрализованный подход использует принцип субсидиарности. Это означает, что ответственность за CIIP возложена либо на отраслевой орган, либо на сами компании и на самих операторов CII.

Поэтому у многих государств-участников, которые укладываются в эту модель, отсутствует централизованное агентство, отвечающее за CIIP, при этом они возложили ответственность за CIIP на отраслевые государственные органы.

Рис. 1. Децентрализованный подход



Тесное сотрудничество между государственными агентствами

Из-за наличия широкого спектра государственных агентств, вовлеченных в CIIP, многие государства-участники разработали схемы сотрудничества в целях координации работы и усилий различных заинтересованных сторон. Эти схемы сотрудничества могут принимать вид неформальных сетей либо официально оформленных форумов или советов. Однако эти схемы сотрудничества служат исключительно целям информационного обмена и координации между различными государственными агентствами, но не имеют полномочий по управлению ими.

Отраслевое законодательство

Страны, которые используют децентрализованный подход, часто воздерживаются от разработки законодательства, регулирующего CIIP сразу для всех критически важных секторов. Вместо этого принимаемые законы и нормативные акты носят отраслевой характер и поэтому могут сильно меняться от сектора к сектору.

Примеры децентрализованного подхода

Швеция является хорошим примером страны, которая следует децентрализованному подходу к CIIP. Страна использует «системную перспективу», и это означает, что главные задачи CIIP, такие как идентификация важнейших сервисов и ключевых инфраструктур, координация и поддержка операторов, задача законодательного регулирования, а также мероприятия по обеспечению готовности к чрезвычайным ситуациям, попадают в сферу ответственности различных агентств и муниципальных образований. Среди этих организаций можно выделить Шведское агентство по нештатным гражданским ситуациям (MSB, Swedish Civil Contingencies Agency), Шведское почтовое и телекоммуникационное агентство (PTS, Swedish Post and Telecom Agency) и несколько агентств, относящихся к сфере обороны и правоохранительной деятельности.

Для того, чтобы обеспечить координацию действий между разными агентствами и государственными организациями, правительство Швеции разработало коллективную сеть, состоящую из государственных организаций, на которые возложена «специальная ответственность за безопасность общественной информации». Эта Группа сотрудничества в области информационной безопасности (SAMFI, Cooperation Group for Information Security) включает представителей различных государственных органов, она собирается несколько раз в год для обсуждения вопросов, связанных с национальной информационной безопасностью. Предметные области SAMFI, в основном, относятся к политико-стратегической повестке дня и охватывают такие темы, как технические проблемы и стандартизация, национальные и международные разработки в области информационной безопасности, управление и предотвращение IT-инцидентов (Swedish Civil Contingencies Agency, MSB).

Швеция не опубликовала централизованного закона в отношении CIIP, который бы действовал для операторов CII из всех секторов и отраслей. Вместо этого принятие законодательства, содержащего обязательства для компаний внутри конкретных секторов, отнесено к сфере ответственности соответствующих государственных органов. Например, MSB имеет право на выпуск нормативных актов для государственных органов в области информационной безопасности, тогда как PTS может обязать операторов реализовать определенные технические или организационные меры защиты на основе подзаконных актов.

Еще одним примером страны, которая проявляет характеристики, присущие этой модели, является Ирландия. Ирландия следует «доктрине субсидиарности», в рамках которой каждое министерство отвечает за идентификацию CII и оценку риска внутри своего собственного сектора (отрасли). Более того, на национальном уровне не было введено в действие никаких специальных нормативных требований для CIIP. Законодательство остается отраслевым и существует, в основном, для энергетического и телекоммуникационного секторов (2015). В качестве других примеров можно привести Австрию, Финляндию, Кипр и Швейцарию.

Модель 2: Централизованный подход

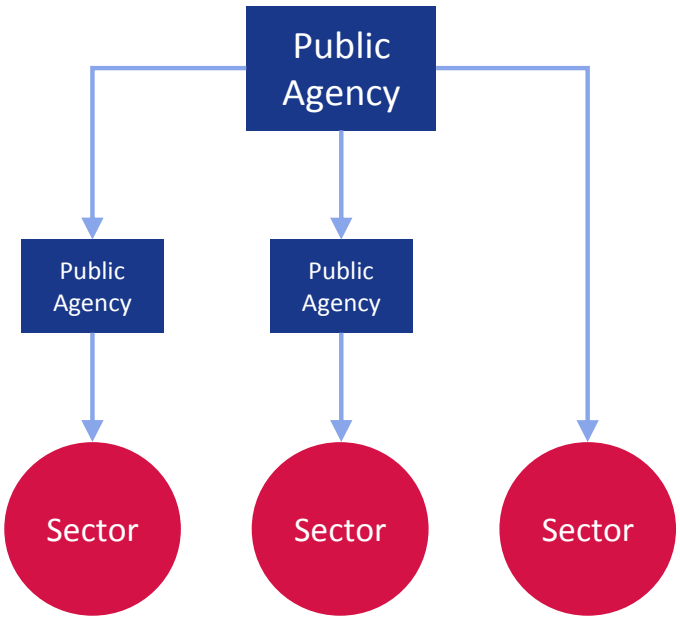
Централизованный подход характеризуется следующими особенностями:

- центральный орган для всех секторов;
- всеобъемлющее законодательство.

Центральный орган для всех секторов

Страны-участники, которые используют централизованный подход, создали государственные органы, обладающие сферами ответственности и широкими компетенциями для нескольких или сразу для всех критических секторов, либо расширили полномочия существующих государственных органов.

Рис. 2. Централизованный поход



Эти главные государственные органы в области CIIP объединили решение таких задач, как планирование на случай чрезвычайных обстоятельств, управление в чрезвычайных ситуациях, задача законодательного регулирования и поддержка частных операторов. Во многих случаях национальные или правительственные группы CSIRT являются

частью государственного органа по защите CIIP.

Всеобъемлющее законодательство

Всеобъемлющее законодательство формирует обязательства и требования для всех операторов CII во всех секторах и отраслях. Этого можно добиться за счет принятия новых всеобъемлющих законов или при помощи дополнения существующих отраслевых нормативных актов.

Примеры централизованного подхода

Франция является хорошим примером государства-члена ЕС с централизованным подходом. В 2011 году французское агентство ANSSI было объявлено главным национальным ведомством в сфере защиты информационных систем. ANSSI осуществляет тщательный надзор за «критически важными операторами» (OIV, operator of vital importance): агентство может приказать операторам OIV соблюдать меры безопасности, оно имеет полномочия на проведение аудитов безопасности для операторов. Более того, оно является Единой точкой контакта для OIV, которые обязаны докладывать агентству об инцидентах информационной безопасности. В случае инцидентов безопасности ANSSI действует как агентство по чрезвычайным ситуациям в сфере CIIP и определяет меры, которые операторы должны предпринять в ответ на кризис. Действия правительства координируются в рамках центра управления ANSSI. Обнаружение угроз и реагирование на инциденты на операционном уровне осуществляются организацией CERT-FR, которая входит в состав ANSSI.

Франция создала всеобъемлющую нормативно-правовую базу в сфере CIIP. В 2006 году премьер-министр приказал составить список секторов критически важной инфраструктуры. Базируясь на этом списке, который идентифицировал 12 ключевых секторов, правительство определило примерно 250 операторов OIV. В 2013 году был опубликован Закон военного планирования (LPM, Military Programming Law), который устанавливает различные обязательства для OIV, например, отчетность об инцидентах и реализацию мер безопасности. Эти требования являются обязательными для всех операторов OIV во всех секторах.

Среди проанализированных государств-членов ЕС централизованный подход является исключением. Большинство стран используют коллективный, децентрализованный подход. Однако Франция – это не единственная страна, которая проявляет характеристики централизованного подхода. В качестве примеров других стран с характеристиками централизованного подхода можно привести Чешскую Республику (центральный государственный орган) и Германию (всеобъемлющее законодательство).

Модель 3: Совместное регулирование с частным сектором

Подход по совместному регулированию с частным сектором характеризуется следующими особенностями:

- юридически оформленное сотрудничество с частным сектором;
- горизонтальные отношения между государственными и частными сторонами.

Юридически оформленное сотрудничество с частным сектором

Типовой формой юридически оформленного сотрудничества между государственным и частным сектором являются государственно-частные партнерства (Public-Private Partnerships, PPP), которые обычно основываются на соглашении между сторонами. Государственные и частные действующие лица могут предоставить партнерству разные ресурсы; например, правительство может предложить политическую легитимность и денежные фонды, тогда как частные действующие лица могут добавить специальный опыт и знания, а также эффективность. Благодаря PPP правительства способны осуществлять регулирование в тех областях, для которых у них отсутствуют знания и опыт.

Горизонтальные отношения между государственными и частными сторонами

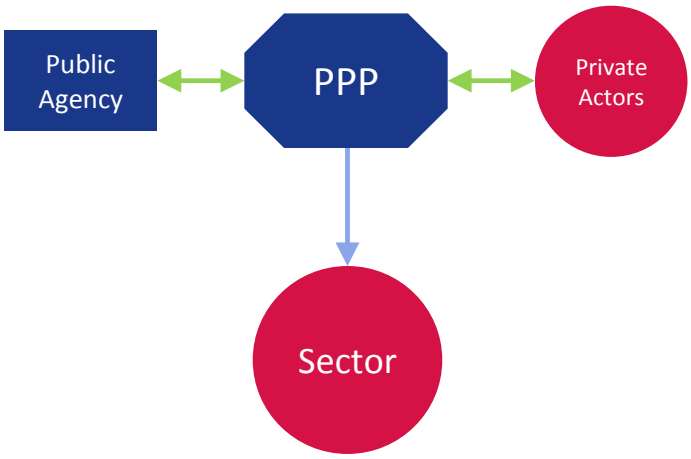
Хотя и не исключительно, PPP часто характеризуются горизонтальными отношениями между государственными и частными участниками, а это означает, что стороны находятся в равных условиях и принимают совместные решения. Процесс принятия решений основан на переговорах, а не на иерархических командных структурах [17]. В некоторых случаях такой вид отношений также отражается в процедуре соблюдения формальных требований, которая не основывается на сильной нормативно-правовой базе и механизмах принуждения, а базируется на добровольных действиях и доверии.

[17] Хорошее практическое руководство по коллективным моделям для эффективных PPP можно найти по адресу: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps

Примеры совместного регулирования с частным сектором

Пример совместного регулирования в сфере CIIP можно найти в Нидерландах. Главным агентством по CIP является Национальный центр по кибербезопасности (NCSC, National Cyber Security Centre). Он основан как центральный информационный хаб и центр экспертизы в сфере кибербезопасности в рамках Национального координатора безопасности и борьбы с терроризмом (NCTV, National Coordinator for Security and Counterterrorism). NCSC включает несколько партнерств между государственными и частными участниками, такими как различные центры анализа и обмена информацией (ISAC, Information Sharing and Analysis Centre) и советы реагирования ICT, которые анализируют ситуацию в ходе крупномасштабного IT-кризиса или угрозы. NCSC подчеркивает, что сотрудничество с частными заинтересованными сторонами основано на равенстве и доверии.

Рис. 3. Совместное регулирование



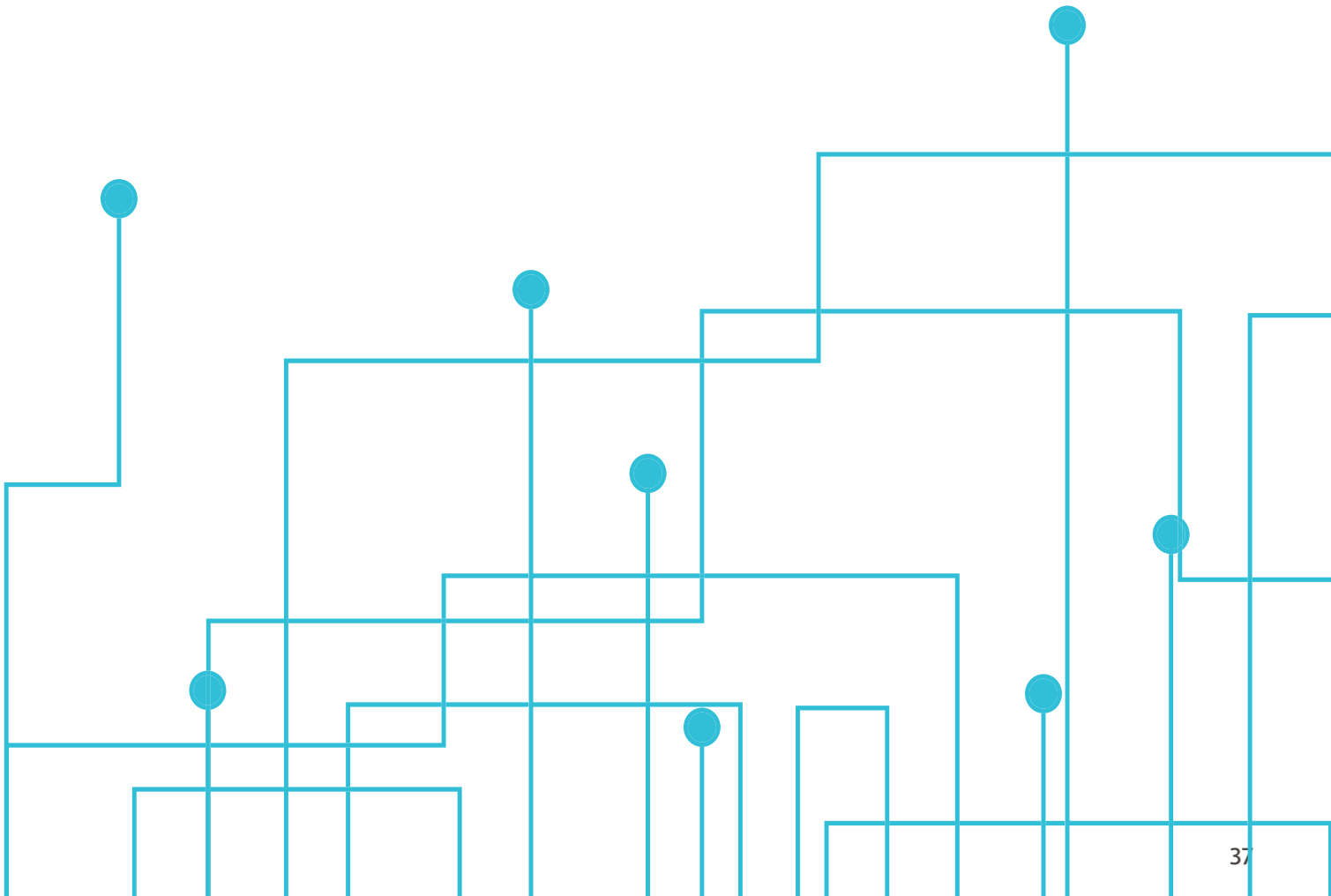
Кроме того, Голландский совет по кибербезопасности предлагает рекомендации на стратегическом и политическом уровнях. Совет включает представителей разных мини-

стерств, академии и частного сектора и имеет государственно-частный характер.

Участие в различных центрах анализа и обмена информацией базируется на конфиденциальности, это означает, что участников не принуждают и не обязывают обмениваться информацией с другими сторонами, они делают это на добровольной основе. Ожидается, что все представители будут уважать взаимные договоренности и обращаться с информацией об угрозах, рисках и других деликатных темах как с конфиденциальными данными.

Как правило, юридические обязательства и требования, установленные в Нидерландах, имеют более строгий характер в отношении сектора телекоммуникаций и ядерной отрасли. Однако голландские компании не обязаны отчитываться об инцидентах информационной безопасности, и значительная часть уведомлений делается на добровольной основе.

Источник: Глава 2.3 отчета ENISA "Stocktaking, Analysis and Recommendations on the Protection of CIIs», январь 2016, https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis



Обзор, анализ и рекомендации по защите Критической информационной инфраструктуры (Critical Information Infrastructure, CII). Основные выводы

Сарри Анна, Мулинос Константинос

Мы публикуем выборочные материалы отчета ENISA "Stocktaking, Analysis and Recommendations on the Protection of CIIs" (https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis). В данной главе представлены основные результаты, полученные на основе многочисленных интервью и онлайн-опросов.

На основе собранной информации (интервью и онлайновые опросы) были идентифицированы некоторые основные результаты. Ключевые выводы представлены вместе с разными категориями аналитической основы. Общее число проанализированных стран для каждой категории может меняться в диапазоне от 12 до 18, в зависимости от полученной в ходе интервью и онлайновых опросов обратной связи.

Некоторые ключевые результаты относятся к критически важным отраслям (секторам). Не все страны идентифицируют одни и те же отрасли (сектора) как критически важные. В приведенной ниже таблице дан обзор отображения критически важных отраслей, идентифицированных каждой страной. Эта таблица основана на материалах из исследования ENISA «Методологии идентификации активов и услуг, относящихся к критически важной информационной инфраструктуре» (Methodologies for the Identification of Critical Information Infrastructure Assets and Services), опубликованного в декабре 2014 года (ENISA 2014). Обратите внимание на то, что в таблице представлена только часть стран, которые изучались в ходе настоящего исследования.

Типы государственных ведомств

Для того, чтобы справиться с проблемой CIIP, страны ЕС либо создали новые ведомства, либо расширили сферу ответственности и полномочия существующих агентств. Национальные агентства делятся на следующие категории:

- EMR: агентство по чрезвычайным ситуациям или CIP
- INT: спецслужба
- ISA: агентство по информационной безопасности
- ISF: форум информационной безопасности
- NRA: национальный регулятор или агентство
- MIN: министерство

Большинство из этих категорий не требует пояснений, однако необходимо отметить некоторые различия между ISA и ISF. Агентства по информационной безопасности представляют собой государственные агентства, которые уделяют основное внимание безопасности информационной и телекоммуникационной инфраструктуры. Во многих случаях они руководят национальной или правительственной группой CSIRT. Обычно это либо независимые агентства, либо подразделения министерств с высокой степенью автономии. В отличие от ISA, форумы информационной безопасности формируются как организации, в рамках которых различные агентства тесно сотрудничают друг с другом. Благодаря такой модели сферы ответственности и компетенции каждого существующего агентства, в основном, остаются неизменными. Сам по себе форум ISF обычно не имеет полномочий на выдачу обязывающих инструкций операторам CII. Форумы ISF часто организуются в странах, которые следуют принципу субсидиарности (решения проблем на местном уровне) и децентрализации.

Необходимо отметить, что не все страны создали главный или ведущий государственный орган по проблеме CIIP. Некоторые страны-участники, особенно те из них, которые придерживаются принципа субсидиарности, возложили ответственность на отдельные министерства и операторов CII. В этих случаях мы идентифицировали агентство с наибольшей сферой ответственности или с наибольшим вовлечением в вопросы CIIP. В некоторых странах-участниках ответ-

Таблица 1 Критически важные отрасли для каждой страны. Основано на материалах: ENISA, Methodologies for the Identification of Critical Information Infrastructure Assets and Services 2014, стр. 5-6.

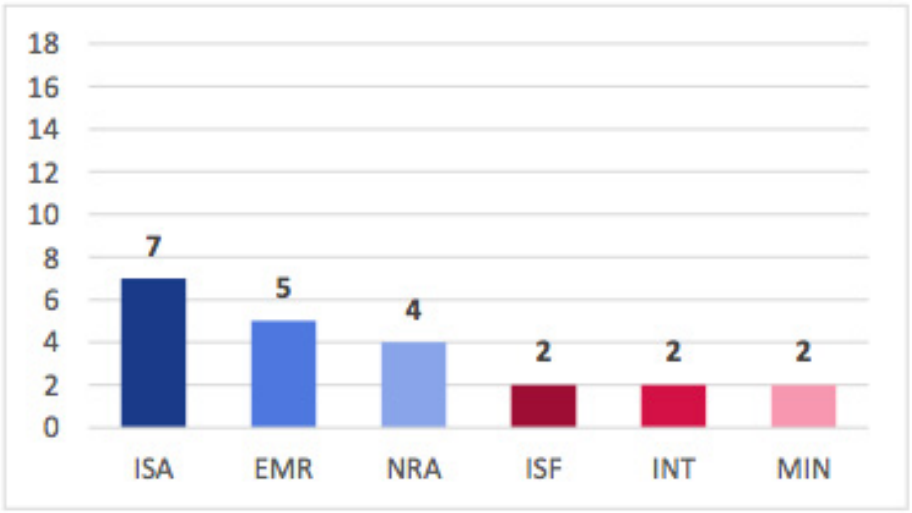
Сектор	Энергетический	ICT	Водоснабжение	Пищевая промышленность	Здравоохранение	Финансы	Правопорядок	Гражданская администрация	Транспорт	Химическая и ядерная промышленность	Космические и научные исследования
AU	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
CZ	✓	✓	✓	✓		✓		✓	✓		
DK	✓	✓		✓	✓				✓		
EE	✓	✓	✓	✓	✓	✓	✓	✓	✓		
FI	✓	✓	✓	✓	✓	✓	✓		✓		
FR	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
DE	✓	✓	✓	✓	✓	✓	✓		✓		
HU	✓	✓	✓	✓	✓	✓	✓		✓		
IT	✓								✓		
NL	✓	✓	✓	✓		✓	✓	✓	✓	✓	
PL	✓	✓	✓	✓	✓	✓		✓	✓	✓	
ES	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
CH	✓	✓	✓	✓	✓	✓		✓	✓		

ственность за CIIP разделена между двумя агентствами. В таких случаях оба агентства рассматривались по отдельности.

На приведенном ниже рисунке – количество разных типов государственных агентств по CIIP в 17 странах-членах ЕС и в одной стране EACT (Европейская ассоциация свободной торговли).

Изученные страны назначили ответственными за CIIP различные национальные агентства. Однако рисунок показывает, что большинство стран имеют склонность поручать CIIP своим агентствам по информационной безопасности. По-видимому, это показывает, что CIIP рассматривается как проблема, наиболее тесно связанная с информационной безопасностью. Кроме того, CIIP является подклассом CIP, и это могло стать причиной того, что пять стран решили возложить ответственность за нее на национальное агентство EMR. CIIP также требует наличия обширных знаний в области IT и «ландшафта частных операторов». Обычно NRA объединяет эти две сферы, и возможно, по этой причине четыре страны передали им ответственность CIIP. Лишь небольшое число стран назначили INT ответственными за CIIP. В двух случаях министерства выполняют задачи, дополняющие работу другого национального агентства.

Рис. 1. Национальные агентства



Сферы ответственности национальных агентств

Мы изучили сферы ответственности и задачи, присвоенные национальным агентствам в области CIIP, для 12 стран (11 стран-членов ЕС и одна страна, входящая в EACT):

Рисунок показывает, что большинство задач выполняется на операционном уровне (темно-синий цвет). Только семь-восемь стран имеют дополнительные сферы ответственности на стратегическом или политическом уровнях, например, разработка стратегий, предложения по принятию нового законодательства или надзор за деятельностью национальной группы CSIRT (светло-синий). Только треть изученных стран поручали таким агентствам надзор за другими организациями (помимо CSIRT) (красный). Сюда относились, в основном, задачи законодательного регулирования.

Формы сотрудничества между государственными и частными заинтересованными сторонами

Исследованные государства-участники разработали разные формы сотрудничества с частным сектором с использованием разных степеней институционализации. Государственно-частное партнерство является юридически оформленной формой сотрудничества между государственными и частными действующими лицами. Обычно эти партнерства определяются через долгосрочные обязательства разных заинтересованных сторон, договора или совместные заявления, которые устанавливают цели и сферы ответственности партнерства, а также совместную ответственность за результат. Рабочие группы и форумы представляют собой менее

Рис. 2. Сферы ответственности национальных агентств

четко оформленную (в юридическом смысле) форму сотрудничества, часто они носят временный характер, требуют меньшего количества ресурсов и обязательств со стороны различных заинтересованных сторон.

Представленный ниже рисунок показывает, сколько стран развили различные формы сотрудничества с частными заинтересованными сторонами. Всего было исследовано 18 стран (17 стран-членов ЕС и одна страна, входящая в EACT):

Десять из 18 изученных стран создали формальные государственно-частные партнерства (Public-Private Partnerships, PPP) для решения задач CIIP. Шесть стран полагаются на менее формализованные формы сотрудничества, такие как рабочие группы или сети. Некоторые из этих стран в настоящее время находятся в процессе создания PPP в соответствии со своими стратегиями в области кибербезопасности. Две страны осуществляют неформальную коммуникацию с частными заинтересованными сторонами.

Юридически оформленные формы сотрудничества между государственными агентствами

Помимо обычных каналов коммуникации, все 17 исследованных стран создали некоторую форму юридически оформленного сотрудничества между государственными агентствами для решения задач CIP. Эти структуры могут принимать самый разный вид: консультативные советы, координационные группы, форумы, кибер-центры или группы для совещания экспертов. Однако их целью всегда является обмен информацией и координация действий различных агентств. Большинство стран разработали новые виды механизма сотрудничества для конкретных целей CIP. Некоторые страны вместо этого расширили сферу действия существующих организаций, которые отвечают за управление в чрезвычайных ситуациях или за безопасность поставок инфраструктуры и услуг.

Рис. 3. Формы сотрудничества между государственными и частными заинтересованными сторонами

Оценка риска

Оценка риска включает идентификацию угроз, потенциальных последствий (воздействия) этих угроз и их вероятности. В некоторых странах национальная оценка риска проводится национальным агентством для всех релевантных отраслей. Другие страны, особенно те из них, которые используют более децентрализованный подход к CIIP, оставляют оценку риска отраслевым ведомствам или операторам CI. Приведенный ниже рисунок показывает, сколько стран проводят оценку риска и какого рода, а также, сколько стран оставляют оценку риска индивидуальным операторам.

Большинство из изученных стран (15 стран-членов ЕС и одна страна, входящая в EACT) проводили оценки риска на национальном уровне либо планируют это сделать в будущем. В четырех странах оценка риска проводится отраслевыми агентствами или министерствами. В пяти странах не выполняется ни национальной, ни секторальной оценки риска. Вместо этого считается, что оценка риска входит в сферу ответственности частных операторов. Однако это не обязательно означает, что правительство заставляет операторов проводить оценки риска. Это можно рассматривать как индикатор того, на каком уровне, по мнению правительства, лучше всего решать эту проблему:

Рис. 4. Оценка риска

на национальном уровне, на секторальном (отраслевом) или на уровне оператора.

Учения по кибербезопасности

Все исследованные страны проводят регулярные учения (тренировки) по CIIP. Существуют три разных типа учений, связанных с CIIP:

- внутриотраслевые тренировки;
- межотраслевые тренировки;
- международные тренировки.

Большинство внутриотраслевых и межотраслевых учений проводятся в финансовой, энергетической и телекоммуникационной отраслях. Другими важными секторами являются государственная администрация, транспорт и логистика, здравоохранение.

Наиболее посещаемыми международными учениями стали проводящиеся под эгидой НАТО Locked Shields и Cyber Coalition, а также тренировки по программе ENISA Cyber Europe. Другими важными международными учениями были Cyberstorm IV (International Watch and Warning Network, IWWN), командно-штабные учения ENISA Cyber Atlantic, учения НАТО Crisis Management Exercise CMX и Nordic Cyber Security Exercise.

Национальная группа реагирования на инциденты, связанные с компьютерной безопасностью (CSIRT)

Группы CSIRT могут различаться по своей клиентуре. Государственные группы CSIRT обычно предлагают услуги органам государственной администрации и агентствам. Национальные группы CSIRT имеют более широкую область действия, поскольку их клиентура включает операторов критически важной инфраструктуры и иногда отдельных граждан. Однако в некоторых случаях могут существовать распределения обязанностей между обоими типами CSIRT.

Рис. 5. Национальная группа реагирования на инциденты, связанные с компьютерной безопасностью

Четырнадцать из исследованных стран сформировали национальные группы CSIRT. В двух случаях национальная группа CSIRT также служит в качестве правительственной CSIRT. Четыре страны не создали специализированных национальных групп CSIRT, однако в них либо запущен процесс создания национальной CSIRT, либо совместная ответственность возложена на сообщество частных и внутриотраслевых групп CSIRT (например, в случае Германии).

Отчетность об инцидентах информационной безопасности

Большинство изученных стран реализовали обязательную отчетность об инцидентах в телекоммуникационном секторе [15], однако только меньшинство реализовало такую отчетность для всех секторов. При этом охват схем отчетности сильно различается. Некоторые страны обязывают операторов CII отчитываться об инцидентах информационной безопасности вне зависимости от сектора (отрасли), если эти инциденты оценивались как критические. Другие страны реализовали обязательную отчетность только для конкретных секторов.

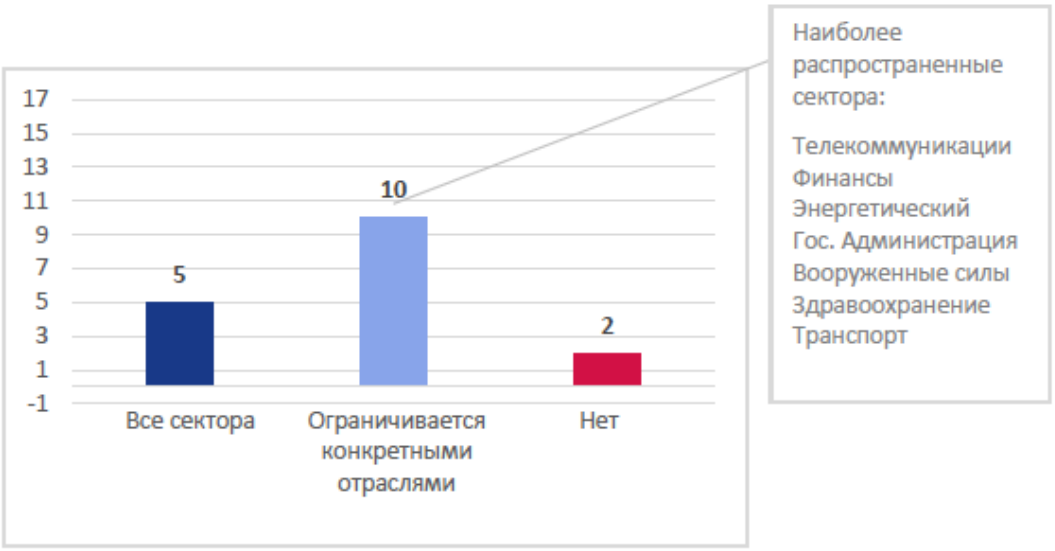
Приведенный ниже рисунок показывает охват обязательной отчетности об инцидентах информационной безопасности для исследованных стран (16 стран-членов ЕС и одна страна, входящая в EACT):

[15] Все государства-участники реализовали обязательную отчетность об инцидентах в секторе телекоммуникаций в соответствии со статьей 13a требований (Нормативно-правовой базы электронных коммуникаций ЕС - прим. редактора). Более того, Швеция намеревается ввести обязательную отчетность об инцидентах для государственных организаций.

Пять стран ввели обязательную отчетность об инцидентах информационной безопасности для всех секторов (отраслей), послед-

ней из них стала Германия. Большинство стран-членов ЕС разработали обязательную отчетность об инцидентах только для некоторых секторов. Все страны, входящие в число десяти, которые ограничили отчетность об инцидентах конкретными секторами, установили такие обязательства для сектора телекоммуникаций. Другими важными секторами являются финансы, государственное управление и энергетическая отрасль. Только две страны не установили обязательную отчетность в каком-либо секторе. В Нидерландах в настоящее время разрабатывается новый закон, который будет включать обязательную отчетность об инцидентах. Детали этого законопроекта (например, установка правоприменительных механизмов) зависят от содержания окончательной директивы NIS (Network and Information Security Directive).

Рис. 6. Отчетность об инцидентах информационной безопасности



Меры безопасности

Аналогичную картину можно наблюдать для обязательных мер безопасности [16]. Те же самые пять стран-участников, которые реализовали обязательную отчетность об инцидентах для всех секторов (отраслей), также реализовали и обязательные меры безопасности для всех секторов.

[16] Статья 13a также подразумевает обязательные меры безопасности для сектора телекоммуникаций.

До того, как CIIP стала важной частью политической повестки дня, большинство стран уже установили обязательные меры безопасности для некоторых секторов. Конкретные секторы, которые уже во многом полагаются на IT или предоставляют критически важные услуги населению (например, телекоммуникационный, финансовый

Рис. 7. Меры безопасности

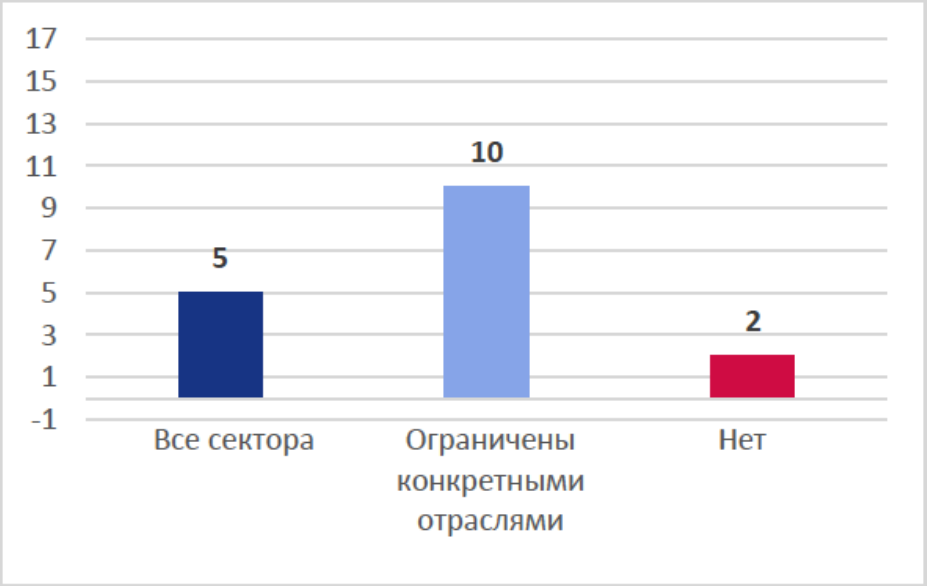
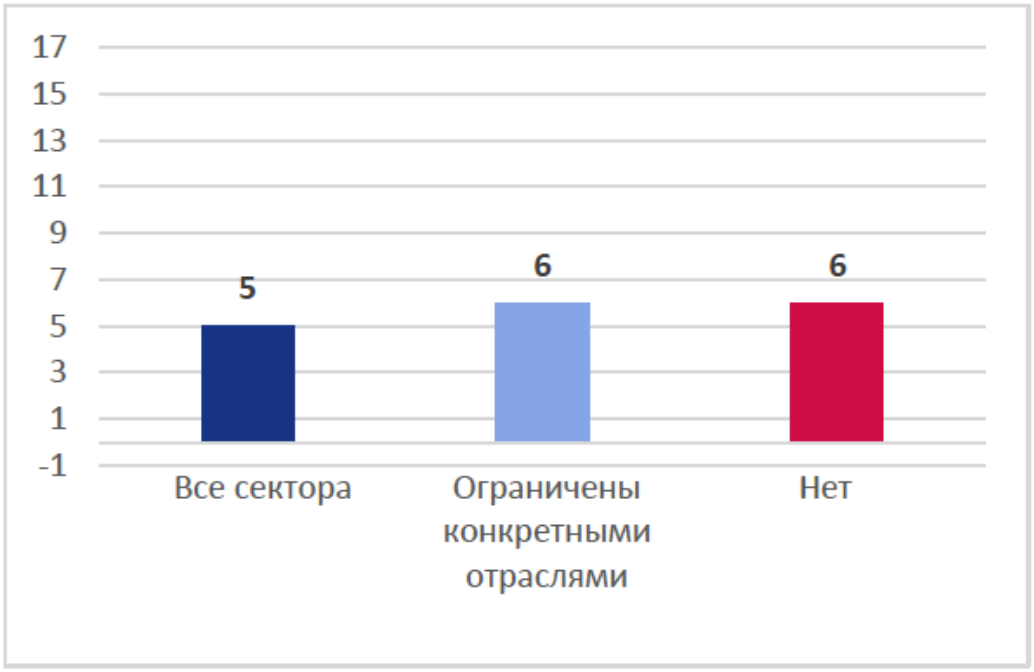


Рис. 8. Аудиты безопасности



и энергетический сектора). Это объясняет, почему большинство стран реализовали обязательные меры безопасности только в конкретных отраслях. Страны без обязательных мер безопасности обычно считают, что информационная безопасность входит в сферу ответственности частных компаний. Однако, по-видимому, существует небольшая тенденция, в рамках которой страны вводят более полное законодательство в области CIIP, которое охватывает все критически важные сектора.

Аудиты безопасности

По-видимому, аудиты безопасности либо имеют наименьший приоритет, либо их труднее всего реализовать для стран ЕС: шесть стран не реализовали обязательные аудиты безопасности и только пять стран обязывают операторов всех секторов проводить аудиты.

Те же самые пять стран, которые реализовали обязательные меры безопасности, также реализовали и обязательные аудиты безопасности. Анализ показывает, что аудиты безопасности либо имеют меньший приоритет, либо их труднее реализовать для правительств стран-участников.

Стимулы к инвестированию

Теоретически страны могут дать импульс операторам CII по инвестированию в безопасность при помощи таких стимулов, как субсидии или налоговые льготы. В таких областях, как защита окружающей среды и экология, налоговые льготы доказали, что они могут успешно применяться для стимулирования компаний в целях реализации экологических стандартов. Однако почти ни одна из исследованных стран-участников не предлагает такие стимулы в сфере CIIP-безопасности. Некоторые страны считают, что в долгосрочной перспективе давление рынка в достаточной степени простимулирует операторов CII на инвестирование в дополнительные меры безопасности. Исключением из этого ряда является Финляндия, в которой компании, инвестирующие в операционные меры безопасности, получают право на налоговые послабления при соблюдении определенных условий.

Источник: Глава 2.2 отчета ENISA "Stocktaking, Analysis and Recommendations on the Protection of CIIs», январь 2016, https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

Уроки мультистейк-холдеризма

Леонид Тодоров

О том, как мы урок мультистейкхолдеризма получали

Доводилось ли тебе, любезный читатель, служить в рядах победо- и орденоносных Вооруженных Сил СССР? Даже если и нет, то вряд ли нужно объяснять тебе значение не утерявшего своей актуальности девиза «Подальше от начальства, поближе к кухне», что впитал ты с молоком матери. Другое дело, что родившемуся в лихие 90-е, тебе вряд ли удастся применить его на практике так, как это делали мы с А. К., одним из отцов российского Интернета, в суровые годы солдатчины, возведя этот навык в разряд высокохудожественного акта. Помню, однажды... Прошу прощения, отвлекся.

Даже внешне герр профессор Вольфганг К. - истинное воплощение мультистейкхолдера: невысокий, коренастый, в бороде и очках, он катается среди банкетирующего сообщества, как красный шарик в снукере, приходя в контакт с каждым и всеми одновременно. Его энергия и готовность к диалогу поистине поразительны: кажется, разбуди его ночью, и он с места в карьер прочтет тебе лекцию «О генезисе и ключевых трендах развития мультистейкхолдерной модели». Он даже школу создал, летнюю, по управлению Интернетом. В общем, как я про себя давно решил:

Быстрый шаг и взор горящий,
Борода, почет и честь,
Он стейкхолдер настоящий,
У него и школа есть!

Отличала герра профессора и потрясающая способность первым оказываться у станции с едой, что порождало у нас с А. К. немалую ревность, - поди ж ты, вроде лицо сугубо гражданское, в СА никогда не служившее, а туда же, с нами, матерыми волчарами, которые как-то изъяли у духов (молодых солдат)... Простите, опять отвлекся.

И решили мы поднять, так сказать, перчатку, тем более что перед всемирным форумом по управлению Интернетом в Кении (помнится, я уже писал о своем дебюте на нем в качестве новой звезды российской школы танца) фортунанам благоволила: что-то у герра профессора приключилось с ногой - и прыть его поубавилась.

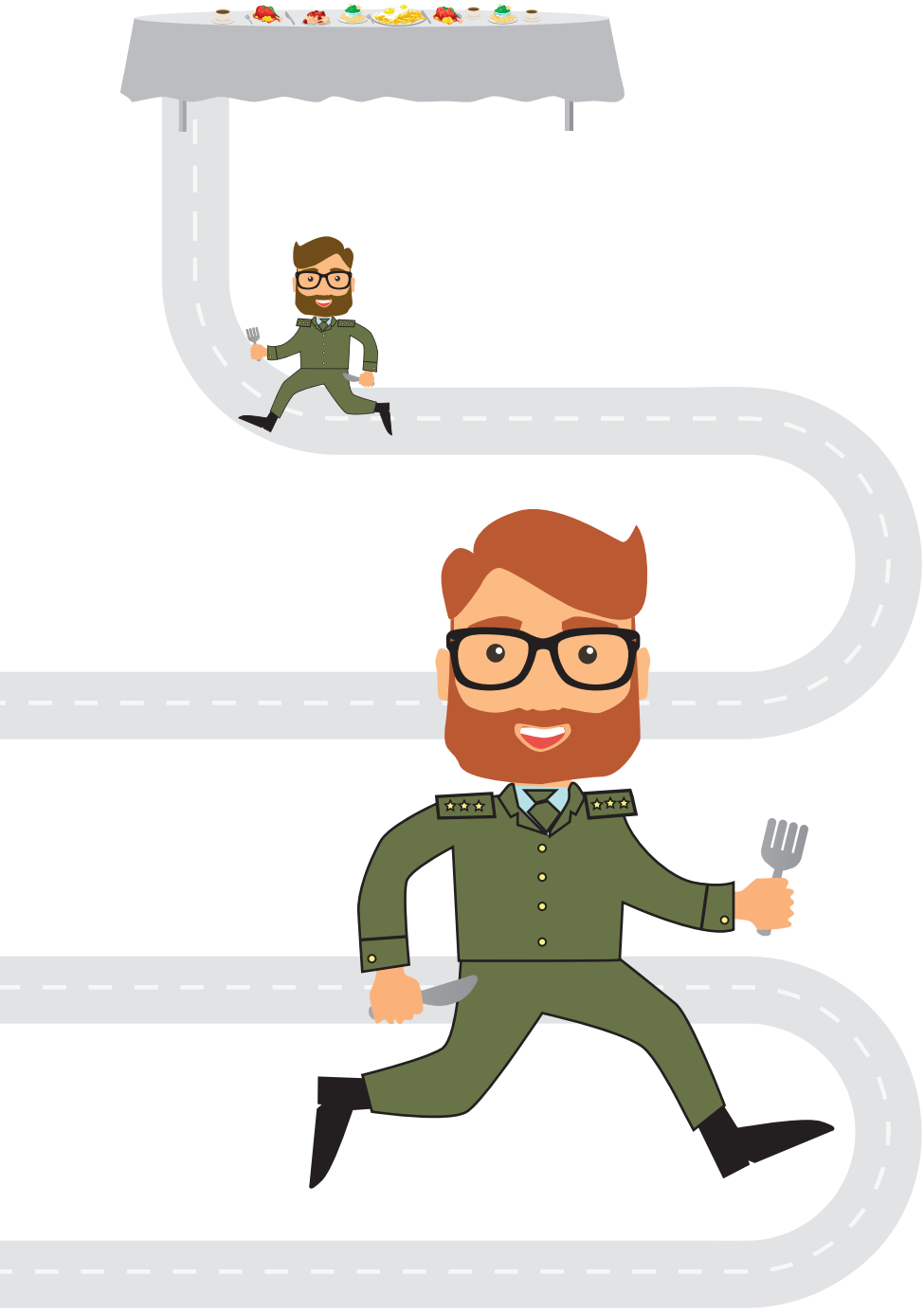
На огромном футбольном поле были рядами накрыты столы для сотен гостей. На некотором расстоянии от них расположились станции с рядами сверкающих, надраенных крышек, надежно прикрывающих эвересты продуктов местной кулинарии – всего того, чем богата кенийская нива. Перемигиваясь, мы с А. К. оказались в полупозишн в непосредственной близости от такой станции. Что до герра профессора, то, приволакивая ножку, он отловил какого-то гигантского роста местного стейкхолдера и что-то с жаром ему втолковывал, тыча пальцем в третью сверху пуговицу пиджака собеседника, приходившуюся ему аккурат на уровне бороды.

Разметив дистанцию и определив угол атаки, мы застыли в ожидании вступительной речи кенийского министра. Министр, как водится у настоящих шоуменов, мастерски держал паузу: жал руки отцам Интернета, смачно, по-брежневски, лобызал руководство ICANN, радушно приветствовал выстроившихся шпалерами многочисленных зарубежных замминистров, - ну, в общем, кто видел по

ТВ рабочие поездки руководства РФ по регионам, волен нарисовать для себя эту картину.

Но вот он и на трибуне, раскрыл папочку и начал исполнять партию Великого Мганги ((с) Жюль Верн). Здесь самое главное - не пропустить финала, так что мы слегка расслабились, тем более что местная обслуга уже приступила к рóзливу.

Вот и крещендо: пошли обещания углублять, расширять, продвигать, укреплять... Мы привстали в ожидании бурных аплодисментов за ВИП-столами, напряжение росло, и да! Как выстрел из стартового пистолета прозвучало завершающее «Thank You!» Мы с Андреем К., пригнув головы и набирая скорость, как пара квортербеков, синхронно рванули к станции. Но что это? Вихрем пронеслись мимо нас очки, борода и огненный взор, и вот уже герр профессор у станции и наваливает, наваливает в тарелку, мчась этаким маленьким, упитанным паровозиком вдоль прямоугольников из металла и пряных запахов. Где больная нога, равные возможности для всех ключевых заинтересованных сторон где, о читатель? Широкой бороздой в эверестах еды отозвался этот слаломный проход, и понуро бредя вслед, стряхивала с гигантских ложек себе в тарелки винегрет из кенийских деликатесов пара возомнивших о себе невесть что ветеранов в/ч 74326, которые, бывало... Э, да что там...



...Мы пережили, конечно, это фиаско, кожа у нас толстая. И нет худа без добра: с тех пор завелась у нас привычка перед каждым нашим представительским мероприятием предложить близким друзьям и коллегам: «А не покормить ли нам герра профессора на предмет мультстейкхолдеризма?» Хороший был пароль - сторонний стейкхолдер не поймет, а значит, не «упадет на хвоста», как говаривали в стародавние времена в славных рядах Вооруженных Сил СССР.

Но тягаться с Вольфгангом К. мы зареклись – лишнее подтверждение великого тезиса о том, что мультистейкхолдеризм – это о сотрудничестве и координации, а не о попытках установить гегемонию и нарушить баланс интересов всех ключевых заинтересованных сторон.

Обзор, анализ и рекомендации по защите Критической информационной инфраструктуры (Critical Information Infrastructure, CII). Передовой опыт

Настоящая глава идентифицирует образцовый передовой опыт защиты CII (Critical Information Infrastructure Protection, CIIP) среди государств-членов ЕС в области схем обмена информацией между государственными и общественными организациями и частными лицами, подготовки CII к чрезвычайным ситуациям, обязательств и требований к операторам CII. Будут предоставлены примеры государств-участников, которые разработали рекомендуемые нормы в определенной области. Список примеров не является исчерпывающим и служит исключительно в качестве стимула для других государств-членов ЕС.

Настоящая глава идентифицирует образцовый передовой опыт защиты CII (Critical Information Infrastructure Protection, CIIP) среди государств-членов ЕС в области схем обмена информацией между государственными и общественными организациями и частными лицами, подготовки CII к чрезвычайным ситуациям, обязательств и требований к операторам CII.

Будут предоставлены примеры государств-участников, которые разработали рекомендуемые нормы в определенной области. Список примеров не является исчерпывающим и служит исключительно в качестве стимула для других государств-членов ЕС.

Партнерство с частными заинтересованными сторонами

Структурами ICT в различных отраслях бизнеса в основном владеют частные компании, а это означает, что сотрудничество государственных организаций с операторами CII имеет критически важное значение для того, чтобы гарантировать, что знания о текущих угрозах являются актуальными, и чтобы обеспечить, при необходимости, быстрое получение поддержки в ответ на инциденты.

Нидерланды являются хорошим примером надежного партнерства с частным сектором. Национальный центр кибербезопасности (NCSC, National Cyber Security Centre) служит в качестве центральной точки для целого ряда государственно-частных партнерств. В рамках NCSC было основано несколько партнерств, основной целью которых стало обнаружение, отклик и анализ. Кроме того, Совет по кибербезопасности (Cyber Security Council), состоящий из представителей государственных организаций и частных компаний, служит в качестве консультативного органа. Благодаря этому центр NSCS обеспечивает тесное партнерство с частными заинтересованными сторонами на стратегическом и операционном уровнях.

Еще одним примером тесного сотрудничества с частным сектором стала Австрия. Эта страна учредила Платформу кибербезопасности (Cyber Security Platform), в состав которой входят представители частных и государственных операторов CII, а также соответствующих государственных агентств. Целью этой платформы является облегчение коммуникации между своими участниками. На операционном уровне была создана группа GovCERT в качестве главной государственной CSIRT (группы реагирования на инциденты, связанные с компьютерной безопасностью). Ею руководит Ведомство федерального канцлера в сотрудничестве с CERT (частная инициатива).

Схемы обмена информацией

Многие государства-члены ЕС разработали схемы обмена информацией для того, чтобы распределять важную информацию между соответствующими государственными агентствами и частными операторами. Однако формы сотрудничества могут отличаться для разных стран. Схемы обмена информацией гарантируют, что все релевантные заинтересованные стороны будут проинформированы о текущих угрозах и рисках и смогут принять соответствующие

меры. Кроме того, они позволяют укрепить сотрудничество и координацию действий и таким образом способствуют эффективному использованию ресурсов.

Германия создала целый ряд широкомасштабных схем обмена информацией с участием государственных и частных агентств. Обмен информацией между правоохранительными органами и спецслужбами реализован через Национальный центр кибербезопасности (National Cyber Response Centre)[1], в рамках которого участники информируют друг друга в ходе ежедневных совещаний и семинаров. Обмену информацией с частным сектором способствуют UP KRITIS и Alliance for Cyber Security: UP KRITIS[2]– это государственно-частное партнерство, его главной задачей является формирование коммуникаций и сотрудничества в области CIIP между частными и государственными заинтересованными сторонами на стратегическом и операционном уровнях. В то время как UP KRITIS концентрирует свое внимание на сотрудничестве с компаниями критически важных секторов, Alliance for Cyber Security (Альянс за кибербезопасность) имеет более широкую повестку дня, в него входят все релевантные организации в области компьютерной безопасности. Для того, чтобы укрепить безопасность всех заинтересованных сторон, альянс предлагает общий «пул информации», регулярные отчеты об угрозах и обмен знаниями между своими участниками (Federal Office for Information Security 2013, 2015).

Шведская Группа сотрудничества в области информационной безопасности (SAMFI, Cooperation Group for Information Security)[3] – это еще один пример передового опыта в сфере обмена информацией. В отличие от Германии, основное внимание уделяется не правоохранительным органам и спецслужбам, а властям, отвечающим за безопасность социальной и общественной информации. В рамках SAMFI разные органы власти не только обмениваются информацией о недавних угрозах, но и обсуждают стратегические вопросы, а также национальные и международные тенденции развития. Представители разных органов власти встречаются несколько раз в год и коллективно работают в составе рабочих групп над решением текущих проблем. (Swedish Civil Contingencies Agency, MSB).

Развитие сообщества CSIRT

В большинстве стран существуют самые разнообразные группы CSIRT с разными компетенциями. Образование и развитие крепкого сообщества с участием разных национальных групп CSIRT, включая разделение ответственности и обмен информацией, поможет получить взаимные преимущества, например, повышение уровня знаний и более эффективное использование ресурсов.

Хороший пример крепкого сообщества с участием групп CSIRT существует в Польше. В Польше ни одна из групп CSIRT не получила статус национальной CSIRT. Вместо этого сообщество разных групп CSIRT совместно отвечает за безопасность. CERT.gov.PL представляет собой главную группу CSIRT для государственных учреждений, но она также предлагает свои услуги операторам CI на основе формальных соглашений. CERT Polska стала первой группой CSIRT в Польше, она входит в состав Исследовательской и академической компьютерной сети (NASK, Research and Academic Computer Network). Эта группа обладает специальными знаниями и опытом в области анализа и исследования инцидентов информационной безопасности, а также предоставляет информацию об угрозах и инцидентах. Эта информация доступна в базе данных, которую могут использовать частные и государственные организации. CERT.gov.PL и CERT Polska работают в тесном контакте, например, управляя базой данных, посвященной сетям honeypot (незащищённая сеть для изучения приёмов хакеров). Более того, они сотрудничают с целым рядом секторальных групп CSIRT, таких как MilCERT и CERT Orange (телекоммуникационный сектор).

Другими примерами применения передовых наработок при развитии CSIRT-сообществ являются Нидерланды или Германия. В Германии был создан CERT-Verbund – альянс различных немецких государственных групп CSIRT (CERT-Bund, военная группа CERTBw и несколько групп CERT федеральных земель), частных CSIRT крупнейших компаний и групп CSIRT частных поставщиков продуктов и услуг в области информационной безопасности (в числе прочих участников). Каждая группа CSIRT по-прежнему отвечает за собственную аудиторию, однако участники альянса обмениваются информацией и поддерживают друг друга при разрешении инцидентов. CERT-Verbund – это институциональный фундамент для такого сотрудничества. Организация открыта для приема всех типов групп CSIRT из Германии. Участники определили стандартизованные технические и организационные интерфейсы для обмена информацией. При этом важнейшей частью становится статистическая оценка совместно используемых данных и предоставление информации стратегического анализа.

Оценка риска

Оценка риска включает идентификацию потенциальных угроз, последствия этих угроз (воздействие) и их вероятность.[4] Анализ рисков является необходимым шагом подготовки и управления кризисом и инцидентами. В некоторых странах национальная оценка риска проводится национальным органом власти для всех релевантных секторов. Другие страны, особенно те из них, которые используют более децентрализованный подход к CIIP, оставляют оценку риска внутриотраслевым ведомствам или операторам CI.

В качестве примера централизованной оценки риска на национальном уровне можно привести Швецию. Шведский комитет MSB был уполномочен на продолжение работ по оценке риска на национальном уровне, начавшихся в 2011 году. Он разработал методологию оценки риска, идентифицировал 27 конкретных серьезных (национальных) событий и разработал 11 сценариев на основе набора этих событий.

Дания не придерживается национального плана оценки риска, поскольку управление отраслевыми рисками рассматривается как более успешный способ смягчения рисков. При этом было образовано Подразделение по оценке киберугроз (Cyber Threat Assessment Unit), в состав которого входят специалисты из разных отраслевых органов государственной власти. Целью этого подразделения является проведение оценок риска для разных отраслей.

В качестве примера децентрализованного подхода можно привести Швейцарию. Швейцария использует подход, который уделяет большое внимание индивидуальной ответственности. Критически важные подотрасли руководят идентификацией рисков информационной безопасности для своих процессов и систем. Полагают, что подотрасли лучше всего знают свои собственные процессы и системы. Государство поддерживает этот процесс при получении соответствующего запроса.

Управление кризисами информационной безопасности

Хорошее управление кризисами информационной безопасности включает определение ролей и сфер ответственности при чрезвычайных ситуациях в области информационной безопасности, а также координацию и процедуры принятия решений с участием соответствующих заинтересованных сторон, обладающих необходимыми компетенциями и опытом. Более того, управление кризисами информационной безопасности должно быть согласовано с другими существующими национальными системами антикризисного и аварийного управления.

Хорошим примером передового опыта в этой области является структура управления кризисами информационной безопасности в Нидерландах. При принятии решений применяется Национальная инструкция по принятию решений в кризисных ситуациях (National Manual on Decision-making in Crisis Situation) (National Coordinator for Security and Counterterrorism 2013). В случае возникновения аварийной ситуации, связанной с ICT, национальная антикризисная организация управляется директором по кибербезопасности Национального координатора по безопасности и антитеррористической деятельности (входит в состав министерства безопасности и правосудия). Меры по оперативному взаимодействию и антикризисные меры предлагаются Национальным центром кибербезопасности.

Управление кризисами информационной безопасности осуществляется в тесном сотрудничестве с частным сектором. В случае возникновения кризиса, связанного с информационной безопасностью, начинает активную работу Бюро оперативного реагирования ICT. Это Бюро сформировано как государственно-частное партнерство, в его состав входят эксперты по ICT из затронутых отраслей. Оно предлагает советы и рекомендации. Кроме того, центр NCSC договорился с государственными и частными заинтересованными сторонами о методах антикризисного управления.

Исчерпывающая правовая основа

Некоторые страны сформулировали проекты новых законов и нормативных актов для того, чтобы решить проблему растущих угроз CII. Эта законодательная основа часто подгоняется под потребности операторов CI всех релевантных отраслей, а не ограничивается лишь некоторыми из них. Эта законодательная основа часто включает обязательную реализацию технических и организационных мер безопасности в соответствии с национальными и международными стандартами. Прочие требования могут включать обязательное уведомление об инцидентах и регулярные внешние аудиты систем безопасности. Эти законы гарантируют единообразный уровень безопасности для всех отраслей и, в случаях обязательной отчетности о состоянии безопасности, позволяют государству анализировать входящие отчеты об инцидентах, отслеживать уровни угроз, выдавать предупреждения подвергшимся угрозе операторам CI и, при необходимости, предлагать поддержку.

В качестве примера передового опыта в этой области можно привести Францию. Закон о военном планировании (LPM13, Military Programming Law) обязывает «операторов особой важности» (OIV, operator of vital importance) сообщать об инцидентах кибербезопасности агентству Agence nationale de la sécurité des systèmes d'information (ANSSI), а также реализовывать технические и организационные меры в области информационной безопасности. Кроме того, OIV обязаны проводить аудиты кибербезопасности, которые должны выполняться либо агентством ANSSI, либо провайдером услуг, аттестованным ANSSI (French Senate 2013). Аналогичные обязательства были приняты в Германии, в которой недавно вступил в силу Закон об IT-безопасности (IT Security Act)14. Недавно принятый закон обязывает операторов реализовывать адекватные организационные и технические меры в области информационной безопасности в той степени, в которой это необходимо для обеспечения доступности их критически важных услуг. Более того, организации должны проводить аудиты безопасности, создавать контактные точки внутри своей структуры и сообщать о существенных инцидентах в области IT-безопасности, если имелась вероятность, что они могли затронуть доступность критически важных услуг.

Источник: ENISA: Stocktaking, Analysis and Recommendations on the protection of CIIs(2.1 Best practices)

Примечания:

1. http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html

2. http://www.kritis.bund.de/SubSites/Kritis/EN/Home/home_node.html

3. http://rib.msb.se/Filer/pdf/26177.pdf

4. Для анализа подходов оценки риска на национальном уровне см.: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report

IT-конференции

Ольга Александрова-Мясина

Начну этот выпуск с того, что в моей жизни стало много нетворкинга с коллегами. А всё потому, что мы переехали в новый офис на улицу 8 Марта, и я вынужденно пересела с машины на метро. Теперь мы ходим вместе из офиса, а иногда и в офис, если случайно встречаемся по пути. Установили программу измерения шагов и соревнуемся, и пишем забавные комментарии друг другу, и стараемся как-то разнообразить наши будни. Самое жизнерадостное в этом переезде - это соседство с областной психиатрической больницей.

Так как некоторые пациенты лечатся амбулаторно, то иногда его величество случай подкидывает нам забавные моменты. Например, недавно я встретила в парке у метро эксгибициониста. Так как никогда со мной такого раньше не случалась, даже в школьные годы, я, конечно, страшно оживилась, чем и напугала его. Персонаж сбежал от меня, сверкая пятками, и было принято волевое решение за ним не гнаться...

Но это все лирика, перейдем к мероприятиям первого полугодия. А их выдалось так много, что, боюсь, не хватит даже места обо всех рассказать подробно.

С нами остались наши ежегодные конференции + мы стали принимать активное участие в мероприятиях дружественных организаций. Подробно писать про RIGF в этот раз не буду, так как формат мы сохранили прошлогодний и даже место проведения не стали менять, и про этот форум я уже писала в предыдущих выпусках. Но на форуме 2016 года произошло событие, о котором я не могу не рассказать – речь идет о меморандуме «О развитии Рунета», который подписали регистратуры российских доменов.

В этом сакральном действии участвовали: Координационный центр национального домена сети Интернет (домены .ru и .рф), Фонд содействия развитию технологий и инфраструктуры Интернет (домены .москва и .moscow), Координационный центр Регионального домена Республики Татарстан (домен .tatar), Фонд поддержки сетевых инициатив «Разумный Интернет» (домен .дети), «Фонд Развития Интернет» (домен .su) и компания «Русские имена» (домен .рус).

От регистратуры доменов .ru и .рф меморандум подписал директор Координационного центра национального домена сети Интернет Андрей Воробьев. «Наш меморандум направлен на повышение качества использования российского доменного пространства и построение партнерских отношений между всеми российскими регистратурами. Мы объединим наши усилия для решения множества масштабных задач, которые стоят перед регистратурами», - сказал Андрей Воробьев.

Дмитрий Бурков (регистратура доменов .москва и .moscow) также положительно отозвался о меморандуме: «Меморандум – это координация наших действий, это четкое понимание того, что регистратуры могут сделать вместе, это совместные действия по продвижению определенной культуры».

Владимир Мамонтов (регистратура домена .дети) отметил, что Интернет сегодня играет важнейшую роль в жизни общества: «Интернет способствовал уменьшению лицемерия в мире, благодаря появлению Интернета стал выше уровень образованности людей и шире их кругозор. И мы будем стремиться и дальше развивать сеть в этих направлениях, усиливая все положительные стороны Интернета».

Дмитрий Елизаров (.tatar) рассказал о том, что подписание меморандума для национального культурного домена .tatar означает возможность учиться и перенимать опыт у коллег.

Галина Солдатова, представляющая старейший российский домен .su, напомнила, что домен .su является точкой отсчета для всего российского доменного пространства, и регистратура .su готова поделиться своим опытом и знаниями с другими российскими регистратурами.

«Российским регистратурам нужно объединяться и работать вместе», – заключил Алексей Созонов, представлявший регистратуру домена .рус.

Сегодня в России зарегистрировано 10 доменов верхнего уровня – как национальных, так и появившихся в ходе программы new gTLD. Большинство этих доменов открыты для всех, они формируют российский доменный ландшафт и обеспечивают пользователям возможность участвовать в развитии российского Интернета. Четыре кириллических домена - .рф, .дети, .москва и .рус – делают Интернет еще более доступным для тех, кто не владеет или еще плохо владеет английским языком. И все актуальнее становится задача плотного взаимодействия регистратур, формирования единого подхода к повышению интернет-грамотности населения России, повышения безопасности Рунета, совместной просветительской деятельности. Эти задачи и будет решать меморандум регистратур российских доменов о развитии адресного пространства Рунета, который дает старт новому типу взаимодействия между российскими регистратурами – взаимодействию, в основе которого лежит сотрудничество и общее стремление к развитию российского Интернета.

Потом пришел май вместе со школьными экзаменами и запахом сирени. Для многих россиян май ассоциируется с длинными выходными и с возможностью устроить дополнительный отпуск, для меня же – со школьными экзаменами. Я остро помню свои собственные экзамены и всегда переживаю из-за дочкиных. Но когда надо собирать дорожную сумку в Питер, не до сантиментов, потому что там ждал меня IPv6 Day and More – конференция MSK-IX. Поехала во вторую

столицу на один день – рано утром выехала, поздно вечером вернулась. Последнее время всегда стараюсь так сделать, если появляется возможность: командировок очень много, и как бы я ни любила поездки, новые впечатления, встречи с разными людьми, моя любимая кровать и домашние тапки с заячьими ушами всегда выигрывают у отельных белых халатов и пушистых одноразовых шлёпок. Кстати, недавно заметила, что и ночные посиделки с друзьями для меня тоже стали проигрывать домашнему уюту. И если приглашают в гости к 10 вечера, всегда найду причину не пойти, даже если приходится честно сказать, исчерпав все разумные аргументы: «Вы извините, но я как карета из сказки «Золушка»: ровно в полночь превращаюсь в тыкву». Так и говорю, а дальше как пойдет. Обычно прокатывает.

Мы с коллегами ехали на «Сапсане», и для меня это счастливая возможность послушать аудиокнигу. Должна вам признаться, что книги из телефона - это реально крутое достижение человечества! За один только месяц в машине, в метро и на беговой дорожке удалось проглотить три исторических книги, две профессиональных и одну на иностранном языке. Нехорошо хвастаться, но это мой личный и персональный рекорд, такого количества книг я никогда бы не осилила, если бы читала их глазами. Просто потому, что нет столько времени. А чем заканчивается «почитать перед сном», многим, наверное, знакомо.

Время пролетело быстро, в Питере я сразу побежала в музей связи, где проходила конференция. Коллеги уже были на площадке и размечали диспозицию.

Участники дня IPv6 с удовольствием осматривали уникальную коллекцию музея, посвященную истории развития средств связи. Здесь представлены экспонаты, рассказывающие об истории почтовой, телеграфной и телефонной связи, радиосвязи и радиовещания, телевидения, мобильной, космической и спутниковой связи. Вообще это самый лучший музей связи в России – такой большой и разнообразной коллекции больше нет ни у одного российского связного музея.

Открыл конференцию технический директор MSK-IX Александр Ильин. Он предложил участникам конференции не только слушать доклады и выступления, но и самим участвовать в обсуждении актуальных тем. Тут же была предложена первая тема для обсуждения – доклад менеджера по региональному развитию MSK-IX Константина Степанова, в котором он рассказал о том, как MSK-IX работает в Санкт-Петербурге, и что компания планирует делать в этом регионе в ближайшее время.

«Мы постоянно создаем новые сервисы и новые услуги для того, чтобы привлекать новых участников обмена трафиком и наращивать наше присутствие во всех регионах. Сегодня MSK-IX – это ведущая платформа для обмена трафиком между сетями, мы поддерживаем распределенную сеть точек обмена трафика. В России точки обмена трафиком компании расположены в девяти городах. Так что сотрудничество и партнерство с MSK-IX – это быстрый старт новых площадок и возможность подключения новых точек не только в Москве и Санкт-Петербурге, но и в других городах России», – рассказал Константин Степанов.

И это подтверждается статистикой. Более 600 организаций используют сервисы MSK-IX для развития сетевого присутствия в ключевых телекоммуникационных центрах России. К MSK-IX подключены операторы связи, социальные сети, поисковые системы, видеопорталы, провайдеры облачных сервисов, корпоративные и научно-образовательные сети. MSK-IX имеет свою уникальную аудиторию, которая больше, чем у любого другого европейского IX. Кроме того, 55% участников MSK-IX используют в своей работе протокол IPv6.

Директор по внешним связям RIPE NCC в Восточной Европе и Средней Азии Максим Буртиков подробно остановился на том, как развивается протокол IPv6 в России. «Сегодня в России работает 51 «пятизвездочный» LIR, при этом имеется огромный потенциал для роста. Так, 27 из этих LIR предоставляют контент по IPv6, остальные дают интернет-доступ по IPv6 для своих клиентов. Кроме того, более 50% всех автономных систем в России анонсируют IPv6». Максим Буртиков обратил внимание на то, что на внедрение IPv6 влияют как региональные, так и внешние факторы (например, развитие Интернета вещей). Кроме того, на повестке дня все чаще оказывается информационная безопасность, и протокол IPv6 оказывается крайне полезным для обеспечения кибербезопасности.

Российский день IPv6 продолжился круглым столом «Развитие бизнеса в современных условиях. Телеком, дата центры и OTT», участники которого обсудили вопросы качества услуг и ценообразования, роста трафика индустрии OTT, движения в сторону потребителя как одного из основных трендов сегодняшнего дня. Коммерческий директор MSK-IX Евгений Морозов отметил различия в подходах к работе с клиентами в сферах B2B и B2C в разных странах мира:

«Мы ведем работу с профессиональными участниками российского телеком-рынка и стремимся поддерживать прямой контакт с нашими клиентами. Бизнес в России делают люди, а не тарифы».

Вел круглый стол руководитель проектов развития MSK-IX Сергей Киселев, в дискуссии приняли участие Дмитрий Петров ("Комфортел"), Владимир Кузнецов ("Телеум"), Вячеслав Волков ("Миран"), Евгений Малиновский (SDN), Николай Красько (SPB

TV) и Павел Поздняков ("Иновентика").

Завершился Российский день IPv6 докладами Василия Томилина (Cisco) «IPv6 в локальных сетях - возможные атаки и защита от них» и Михаила Родионова (Fortinet) «Защищенные операторские сети».

Так как в этот раз мероприятие объединили с питерским Beering'ом (от слова beer - типа все пиво пьют), то по завершению многие отправились на кораблик, где и происходил Beering. Собственно, наши участники в большинстве своем решили подтвердить, что «в Питере пить» (с), но меня снова ждал вокзал. Вернее, ждать он меня не хотел, поэтому мы с коллегами чуть не опоздали на поезд. Пришлось бежать по Невскому проспекту, расталкивая прохожих локтями – хорошо, что аудиокниги я слушаю не только в поезде, но и на беговой дорожке. В вагон мы забежали за 3 минуты до отправления. Мне казалось, что язык к горлу прилип, так мне было плохо после этой пробежки с утяжелением. Но всё закончилось хорошо, и вечером того же дня я опять была в Москве!

Потом как-то очень быстро пришло время форума «ИТ+Суверенитет». Форум совпал с дочкиным экзаменом по математике, мне было сложно сфокусироваться на деловой программе, но всё получилось.

Форум «ИТ+Суверенитет» стал вторым в серии из восьми форумов «И+», проводимых в 2016 году. Организован он был Институтом Развития Интернета при поддержке Координационного центра национального домена сети Интернет.

Форум открыл советник президента РФ, председатель совета ИРИ Герман Клименко, который пригласил участников форума обсудить конкретные шаги по развитию российской индустрии программного обеспечения и информационных технологий, вопросы импортозамещения, роль информационной безопасности в развитии киберсуверенитета страны.

Председатель комитета Госдумы по информационной политике, информационным технологиям и связи Леонид Левин отметил, что ключевой задачей в области импортозамещения является поиск путей для ускорения развития отечественной IT-индустрии. Он пообещал участникам форума, что законодатели будут предпринимать все меры для защиты российского IT-бизнеса. Также Леонид Левин обратил внимание на ту роль, которую в области обеспечения IT-суверенитета страны играет Координационный центр национального домена сети Интернет: «Координационный центр активно участвует в работе международных организаций в направлении развития диалога всех заинтересованных сторон в области управления Интернетом».

О том, как к курсу на импортозамещение относятся признанные эксперты отрасли, рассказал директор РАЭК, член совета ИРИ Сергей Плуготаренко. «С уверенностью можем сказать, что на данный момент имеется значительная экспертная и отраслевая поддержка курса на импортозамещение в области программного обеспечения. Однако часть экспертов ИРИ скептически относятся к установленным срокам реализации,

объемам и результативности курса на импортозамещение. В связи с этим необходимо проделать дополнительную экспертную, законотворческую и отраслевую работу по этому вопросу. Также требуется поддержка на всех уровнях и дополнительное стимулирование российских разработчиков», - резюмировал Сергей Плуготаренко.

Круглый стол «Роль информационной безопасности в обеспечении суверенитета» собрал экспертов, представляющих крупнейших игроков российского рынка информационной безопасности, инфраструктурные компании, общественные и международные организации, государственные органы. Заместитель министра связи и массовых коммуникаций РФ Алексей Соколов подчеркнул, что Интернет сегодня является одной из основных движущих сил экономического роста, и безопасность инфраструктуры отечественного сегмента Интернета является одной из первоочередных задач государства.

Генеральный директор MSK-IX Елена Воронина отметила важность обеспечения надежной и стабильной работы инфраструктуры Интернета. Она сказала, что в России функционирует большое количество автономных сетей, которые не имеют единой системы административного управления, но в своей работе руководствуются едиными организационными принципами. «Инфраструктура – это основа всей системы Интернета, и к ней нужно относиться с уважением и бережно, иначе можно ее сломать. Необходимо создать рабочую площадку, где все участники могли бы внести свой вклад в формирование документов отрасли. Надо разрабатывать документы, которые касаются инфраструктуры, и после этого необходимо проводить техническую экспертизу. Специалистов, которые могли бы помогать в этом направлении, немного, и их нужно привлекать к работе и учитывать их мнение» - сказала Елена Воронина.

Участники круглого стола высказали общее мнение о том, что совместная работа всех заинтересованных сторон в области обеспечения кибербезопасности Интернета является ключевым фактором для стабильной работы российского Интернета.

После форума я не продолжила networking, а поспешила домой к дочери, чтобы успеть до темноты отпраздновать с ней удачно сданный экзамен.

Через несколько дней мне опять надо было ехать в Питер на конференцию «ХостОбзор». На Московском вокзале я встретила коллег, и мы все отправились в «Райволу», где традиционно уже много лет проходит конференция "ХостОбзор". В этот раз конференция открыла Неделю российского Интернета в Санкт-Петербурге.

В этом году форум впервые проходил под новым названием «Всероссийский форум хостинг-провайдеров и регистраторов доменов» и включал большой блок вопросов по работе системы регистрации. Изменение формата форума было отмечено официальным представителем ICANN по региону Восточная Европа и Средняя Азия, который также посетил мероприятие.

Начальник отдела работы с регистраторами Координационного центра национального домена сети Интернет Георгий Георгиевский рассказал об основных тенденциях развития системы регистрации, перечислил типичные ошибки, которые совершают регистраторы, и поделился планами развития. По его словам, количество регистраторов, аккредитованных в зонах .ru и .рф, растет хорошими темпами, и в ближайшее время стоит ожидать аккредитации новых регистраторов. И забегая вперед, отмечу – Георгий не ошибся. За неполных девять месяцев 2016 года в доменных зонах .ru и .рф было аккредитовано 9 новых регистраторов, что является рекордом для российских национальных доменов.

Представитель Технического центра Интернет Дмитрий Белявский рассказал об инструментах, которые помогают компаниям начать регистраторский бизнес, сохраняя все существующие партнерские отношения. «Аккредитация в качестве регистратора доменов .ru/.рф дает бизнесу много преимуществ. Так, регистратор может напрямую работать со своими клиентами и лучше контролировать свои бизнес-процессы. Продукт Технического центра Интернет «Виртуальный регистратор» дает возможность полнофункциональной работы с реестрами и управления всеми своими аккаунтами из единого интерфейса», - рассказал эксперт.

Также на форуме прошла специальная сессия с участием представителей Роскомнадзора, во время которой обсуждались вопросы лицензирования хостинг-провайдеров, взаимоотношения с правообладателями и проект изменений в правила регистрации доменных имен в доменах .ru и .рф.

Вопросы лицензирования хостинг-провайдеров впервые обсуждались на площадке "ХостОбзора" в прошлом году с участием представителей Министерства связи и массовых коммуникаций РФ. Результатом работы стало официальное письмо министерства о том, что услуги хостинга не подлежат лицензированию. В ходе сегодняшней конференции представитель Роскомнадзора подтвердил эту позицию, и по итогам секции было принято решение выпустить официальные разъяснения, на которые хостинг-провайдеры могли бы ссылаться.

Наибольший интерес участников вызвал вопрос взаимоотношения хостинг-провайдеров и регистраторов доменных имен с правообладателями. По словам Сергея Копылова, заместителя директора Координационного центра национального домена сети Интернет по правовым вопросам, сформировать корректную судебную практику по вопросам ответственности за правонарушения в области интеллектуальной собственности можно, только проводя планомерную разъяснительную работу среди судей, которые выносят решения по такого рода делам.

Также в присутствии регистраторского сообщества обсудили проект изменений в правила регистрации доменных имен в доменах .ru и .рф, которые будут рассмотрены на ближайшем собрании Совета Координационного центра национального домена сети Интернет. Так, предлагается дополнить правила в части, касающейся внесения в стоплист доменов пожизненно заблокированных ресурсов. Эта мера поможет избежать ситуаций, при которых домен заблокированного ресурса освобождается и попадает в третьи руки, а новый администратор может пострадать от того, что его ресурс автоматически попадает под блокировку.

Темы все были актуальные и наболевшие, потому бурные дискуссии продолжались даже после официальной части. Справедливости ради надо сказать, что такой формат характерен для этого мероприятия и, как говорил мой старинный приятель, «за это мы его и любим». Но на ужине участники все же решили немного отвлечься от работы и перешли к обсуждению птички в клетке. Стали спорить – живая она или нет. Мнения разделились, и кто-то из участников спора

сказал: «Да живая она, живая! Терпеливая просто...» Так мы теперь и называем эту искусственную тушку в главном ресторане «Райволы»: «Терпеливая птичка».

Уезжать обратно из Санкт-Петербурга мне пришлось накануне свадьбы моей школьной подруги. Представляете, она исполнила свою мечту детства и вышла замуж на Английской набережной. Но мне не удалось увидеть это событие своими глазами: надо было срочно возвращаться в Москву для оформления важных документов. «Сапсан», где были жених и невеста, промчался мимо моего поезда, и мы даже не успели помахать друг другу рукой – так это было стремительно. Мне было грустно, и я мысленно просила у подруги прощения за казус, который мне подстроила жизнь.

Потом я поехала на конференцию ICANN, второй раз в жизни. Было это в Хельсинки, столице Финляндии. Жили мы в недостроен-

ной гостинице на берегу залива и наслаждались местной едой и... медлительностью. За завтраком нас обслуживала эстонка, которой нравилось говорить с нами по-русски, а нам нравилось с ней иногда болтать. Так вот даже она – уроженка Эстонии – жаловалась на местный колорит: «Здесь никто не спешит вообще. Потому что зачем спешить?» На такой аргумент как-то даже не знаешь, что и ответить. А действительно, зачем? Таким образом, чашку кофе мы ожидали в среднем 15-20 минут, про еду, конечно, отдельный разговор. Еда в Хельсинки для нас привычная и удивительно вкусная. Это был невероятный гастрономический разврат; оленина, солонина, мясо медведя, косули и других диких животных. А также клюква, морошка и другие северные ягоды + мороженое из селедки – потрясающе вкусное.

Теперь переходим к официальной части! Пятьдесят шестая встреча корпорации ICANN была названа исторической, поскольку следующая встреча ICANN пройдет в ноябре, а в конце сентября истекает срок контракта между ICANN и Министерством торговли США. И если предложения по передаче функций контроля над доменной системой интернет-сообществу будут приняты, нынешняя встреча станет, по сути, последней для текущей модели управления Интернетом.

Встречу открыл старший вице-президент ICANN Дэвид Олив. Затем к собравшимся обратился с приветствием новый президент ICANN Йоран Марби, для которого встреча в Хельсинки стала первой в этой должности. В ходе церемонии открытия состоялось вручение наград Multistakeholder Ethos Award. На сей раз их были удостоены Кейт Дэвидсон (Общество Интернета) и Чак Гомес (Verisign).

В программе встречи в Хельсинки было обсуждение ключевых вопросов развития доменной системы и управления Интернетом. В частности, прошло несколько заседаний и рабочих встреч правительственного консультативного комитета ICANN и организации поддержки национальных доменов ccNSO. На этих встречах подробно обсуждались дальнейшие шаги ICANN в свете скорой передачи функций IANA мультистейкхолдерному сообществу.

После плодотворной работы на конференции мы отбыли в Москву, усталые, но, как принято говорить, довольные.

Потом пришло время нашей традиционной конференции TLDCON, которая проходила уже в девятый раз; а лично для меня она была седьмой. И каждый из этих семи раз был как первый – в первую очередь из-за смены страны проведения. С самого начала было решено, что TLDCON будет проводиться в разных странах для того, чтобы ближе познакомиться с интернетчиками из разных стран. Но везде свои особенности и свой колорит, что приходилось учитывать. Хорошо помню свою первую конференцию в пансионате «Волжский утес» под Сызранью (это недалеко от Самары).

Именно там мы погрузили наших иностранных спикеров в атмосферу настоящей России, а где-то даже и СССР - с «карточками пациентов» и едой из советского прошлого. Мы приходили утром на завтрак, а на столах стоял кефир, который нужно было выпить с вечера и кто не выпил – сам дурак. За обедом мы спорили о том, из чего сделано блюдо – из рыбы, мяса или курицы. И помню, как один из иностранных спикеров решил немного самостоятельно попутешествовать, не зная русского языка, и поехал

куда-то, не дожидаясь трансфера. Никогда не забуду, как стояла на крыльце, махала ему рукой и думала, что больше никогда не увижу... Но как-то он выкрутился и даже добрался потом до дома, о чем мне сообщили социальные сети.

В этом году конференция началась для меня с невероятного стресса. Мы вылетали большой компанией в воскресенье рано утром из Шереметьево. Ранние подъемы для меня не проблема, поэтому я выставила на телефоне будильник, вызвала на нужное время такси и легла спать. Проснулась я сама по себе, за окном уже светало, схватила телефон, чтобы проверить время, и... о, ужас! Телефон «умер», он ни на что не реагировал, нажатие разнообразных кнопок и втыкание в него зарядки не принесло результатов. Между тем, времени было уже 6 утра – и я уже должна была стоять в аэропорту и встречаться с коллегами. Узнать, ждет ли меня водитель после часа опоздания, и сообщить коллегам о неприятности я тоже, соответственно, не могла.

Но чудеса иногда случаются, и это был именно такой день. Разбудив в доме всех просьбой вызвать такси и надев то, что было под рукой, я выбежала из дома. Такси через онлайн-сервис примчалось невероятно быстро (хотя потом я узнала, что и вызванный с вечера водитель мирно спал в машине). Быстро прыгнув на заднее сидение, я сказала:

- Надо доехать до аэропорта за 20 минут.

Водитель невозмутимо кивнул, включил опцию «полет» и далее со мной не разговаривал. В дороге мне как-то удалось реанимировать телефон, и коллегам было сообщено о том, что я опаздываю. Ровно в 6:30 я стояла в зоне таможенного досмотра в терминале. Руки тряслись, прическа напоминала воронье гнездо, хотелось пить, а также сделать всё остальное, к чему привыкли люди по утрам. Вдалеке заметила коллег, они приветливо замахали мне рукой, но улыбаться в ответ я совсем не могла. Потом еще долго приходила в себя, так как в таком

режиме ехала на самолет в первый раз в жизни (очень надеюсь, что и в последний).

Тбилиси встретил солнцем и теплом. Отель, где проходила конференция, стоял на окраине города. Не потому, что мы садисты, а потому, что на обозначенный период ни одного свободного зала в центре города не было. И если бы мы немного помедлили с

бронированием – например, решили бы в марте, когда ездили в Тбилиси для выбора отеля и формирования культурно-развлекательной программы, поискать еще варианты – то и этого отеля нам бы не досталось: все места на сентябрь там были разобраны. Наладила Грузия бизнес и туристический поток, причем как-то неожиданно и стремительно.

Обычно на конференции самый сложный – это первый день, и его нужно просто пережить, потом всё идет как-то легче. Накануне вечером я сказала коллегам:

- Хочу, чтобы уже был вечер первого дня! Сделайте мне монтаж.

Но в этот раз чуда не произошло, и надо было проживать первый день минуту за минутой, от начала и до конца.

Первое заседание TLDCON было посвящено самой главной теме конференции 2016 года – IDN-доменам. На секции выступили представители регистратур доменов верхнего уровня, использующих национальные алфавиты – кириллических .укр, .дети, .срб, .бел, .сайт, .онлайн и грузинского IDN-домена. Каждый из выступавших рассказал о том, как развивается его домен, с какими сложностями пришлось столкнуться, какие интересные решения удалось найти. Как выяснилось, одна из основных проблем IDN-доменов – это сложности с поддержкой IDN, которые до сих пор наблюдаются со стороны почтовых систем и социальных сетей. Поэтому регистратуры решили обратиться к ним с просьбой продолжать работу над поддержкой IDN. К петиции могут присоединиться регистратуры всех доменов верхнего уровня на национальных языках – эта проблема касается не только кириллических доменов, но и всех остальных IDN.

«На сегодняшний день в домене .рф, который по популярности находится на первом месте в мире среди всех IDN-доменов, насчитывается около 900 тысяч имен. Домен демонстрирует устойчивое развитие и ежегодный прирост на уровне 3-4%. Основным сдерживающим развитие домена фактором является отсутствие возможности использования полностью кириллических адресов электронной почты. Проблема общая для всех кириллических доменов и IDN-доменов в целом. Инициатива регистратур доменов .бел, .укр и .рф подписать петицию в адрес почтовых сервисов и социальных сетей на форуме уже нашла поддержку со стороны регистратур других IDN-доменов», – рассказал директор Координационного центра доменов .ru/.рф Андрей Воробьев.

Участники секции также подчеркнули, что проблемы IDN затрагивают не просто интересы отдельных администраторов доменов, речь идет об интересах десятков миллионов людей, которые пользуются этими доменами. И если существующие сегодня почтовые сервисы и социальные сети не уделят должного внимания этому вопросу, то нишу займут новые компании, которые будут более гибкими.

О росте доли шифрованного трафика говорили участники секции «Информационная безопасность». Интересные цифры привела Маарит Паловирта (ISOC): «86% входящих соединений и 76% исходящих в Google защищены шифрованием. За последние два года очень многие операторы конвертировали свой трафик в зашифрованный». Дмитрий Белявский (ТЦИ) подробно остановился на том, как можно организовать защиту данных при использовании одного из самых популярных интернет-протоколов – DNS. Бенедикт Аддис (Shadowserver) рассказал о том, как работает его компания, занимающаяся вопросами безопасности доменного пространства Великобритании – и оказалось, что схема работы Shadowserver очень похожа на ту, которую в своей работе применяет проект Координационного центра «Нетоскоп». Линда Мюллер (Iron DNS) поделилась опытом внедрения в компании сертификата ISO. О том, как ICANN обеспечивает надежность, стабильность и устойчивость мирового Интернета, рассказал Джон Крейн. Он отметил важность привлечения к этой работе добровольцев из разных стран и пригласил к участию специалистов из России и других стран региона.

Завершился первый день работы TLDCON 2016 заседанием «Международные организации и доменное пространство». Мукеш Чулани (ICANN), Катрина Сатаки (ccNSO) и Леонид Тодоров (APTLD) рассказали о работе своих организаций и о ближайших планах, связанных, в том числе, и со странами СНГ и Восточной Европы. Катрина Сатаки пригласила участников конференции к более активному участию в работе ICANN.

Вечером был ужин в видовом ресторане на горе, куда приходит фуникулер. Рассадка была именная, и гостей я утрамбовывала сразу от входа. Зато все разместились, были накормлены, напоены и даже посмотрели национальные грузинские танцы и послушали песни. С балкона открывался вид на ночной город, горы, окружающие Тбилиси, и невероятно красивую грозу в горах. Позже к этой красоте добавился еще и великолепный фейерверк. Я перемещалась по балкону от одной компании к другой и думала о том,

что надо приехать в Тбилиси еще раз. И никому об этом не говорить!

Второй день начался для меня с традиционной маркетинговой секции. В этом году я хотела немного отойти от вопросов маркетинга и поговорить про IDN-почту, но мои «поклонники» этого не позволили, и пришлось добавлять спикеров с докладами про продвижение доменов и маркетинговые акции.

Участники стали обсуждать проблемы и пути развития интернационализированных доменов. Я предоставила слово главному специалисту отдела прикладных сервисов Технического центра Интернет Игорю Лидину, он рассказал о новом решении, которое позволит создать почту на национальных языках.

Некоторое время назад ТЦИ при помощи статистического портала Statdom.ru, который разработали и поддерживают ТЦИ и Координационный центр доменов .ru/.рф, провели исследование, касающееся поддержки IDN-почты на основных сервисах Рунета. Оказалось, что интернационализированные почтовые адреса поддерживают только 0,4% сервисов обмена почтой в Рунете. «Новый стандарт UTF-8 для поддержки интернационализированных email-адресов разработан еще в 2012 году, но до сих пор основные сервисы Интернета его не поддерживают – за исключением Google, сервис которого Gmail реализовал прием почты с интернационализированных почтовых адресов еще в 2014 году», – рассказал Игорь Лидин. Также он посетовал на то, что, хотя и Координационный центр доменов .ru/.рф, и Технический центр Интернет постоянно обращаются к российским почтовым сервисам с предложением о создании IDN-почты, российские компании реагируют на это предложение без энтузиазма.

Причину такой вялой реакции объяснил представитель "Яндекс.Почты" Алексей Шелковин. Оказалось, что согласно внутренним исследованиям "Яндекса", с национальных доменов поступает только 5,4% всей входящей почты "Яндекса". Это очень небольшой трафик, и поэтому до сих пор вопросу внедрения IDN-почты уделялось не слишком большое внимание. «Но конференция TLDCON показала, что спрос на IDN-почту существует, поэтому, думаю, мы будем работать над этим направлением, чтобы предложить решения пользователям. Многие вещи для внедрения полноценной IDN-почты уже сделаны, поэтому анонс поддержки UTF-8 не за горами. Считаю, что это направление может стать новой точкой роста для "Яндекс.Почты", и надеюсь, что уже на следующей конференции мы сможем представить вам наше решение!» – сказал Алексей Шелковин.

Также в секции приняли участие Евгения Воронко (Hoster.by), Сергей Горбунов (RU-CENTER), Микаэла Круден (Afilias), Марина Никерова (ТЦИ) и Федор Смирнов (Realtime Register).

Вторая секция «Правовые вопросы регистрации доменов» открылась докладом Максима Альзобы (FAITID), который рассказал о том, как решаются вопросы с защитой персональных данных в реестрах доменных имен. Мария Малышева (ТЦИ) представила участникам процедуру безбумажного трансфера для доменов .ru и .рф, которая была внедрена на прошлой неделе. Она подчеркнула, что внедрение электронного трансфера полезно для пользователей и делает домены .ru и .рф более конкурентоспособными на мировом рынке. Также на секции выступили Екатерина Олейник (Arzinger) и Юрий Гончарук (UANIC), которые рассказали о том, как подходят к разрешению доменных споров в украинских национальных доменах .ua и .укр, и об особенностях применения процедуры URS для новых доменов. Эксперт комитета ГД РФ по информационной политике Дмитрий Афанасьев предупредил регистратуры и в первую очередь регистраторов, что сегодня российские (и не только российские) суды начали рассматривать регистратора как ответственного за незаконный контент, который есть на сайте. Это требует от регистраторов внимательнее относиться к поступающим к ним жалобам со стороны правообладателей. Итоги секции подвел вице-президент ICANN Михаил Якушев. Он отметил важность обсуждения вопроса взаимоотношений нормативно-технического регулирования и международного и национального правового регулирования и поиска баланса между ними, а также вопроса защиты персональных данных.

Заключительная секция TLDCON была посвящена рынку вторичных доменов. Андрей Савельев (Домены.РФ) оценил оборот этого рынка в Рунете в 300 миллионов рублей ежегодно. Это достаточно серьезная цифра, которая означает, что для вторичного рынка также необходимы технические решения. Этим занимается Технический центр Интернет, и руководитель проектов DNS ТЦИ Павел Храмцов рассказал о том, в чем состоят особенности организации DNS-сервисов вторичного рынка доменов и построения DNS. Он отметил, что серверы вторичного рынка в три раза чаще подвергаются атакам на DNS, поэтому их лучше разделять с серверами хостинга. Также он рассказал о важной роли, которую играет в работе с вторичным рынком доменов проект «Нетоскоп»: он дает широкие возможности для проверки доменов, предназначенных для продажи на вторичном рынке. Также в секции участвовали Геворг Погосян (Global R) и Александр Щербаков (FAITID).

Вечером гости поехали на экскурсию с дегустацией вина и изготовлением незамысловатой, но от этого не менее вкусной грузинской еды - хлеба, хинкали и чурчхелы. Хотя с дегустацией в Тбилиси, конечно, проблем нет, и дегустировать отличные грузинские вина можно в любом кафе, ресторане или кабачке. В процессе переходов от одного интерактива к другому я и еще несколько человек из оргкомитета решили потеряться: мы дезертировали в отель, где меня ждало мыло душистое и полотенце пушистое, а также халат, тапочки и удобная гостиничная кровать с горой подушек.

Календарь событий: 2016 год

Международные события

28 сентября - 5 октября
APNIC 42,
Коломбо, Шри-Ланка

Встреча APNIC организуется Региональной интернет-регистратурой APNIC, отвечающей за этот регион. Здесь помимо образовательных сессий (первые пять дней) проводится обсуждение технических вопросов и политики администрирования адресного пространства. Встречи проводятся два раза в год, весной совместно с конференцией APRICOT. https://conference.apnic.net/42

17-19 октября
NANOG68,
Даллас, США

Североамериканская группа сетевых операторов (The North American Network Operators Group, NANOG) является одной из самых активных профессиональных ассоциаций в области сетевой архитектуры, конфигурации и технического администрирования сетей в Интернете. Основной фокус NANOG на технологиях и системах, обеспечивающих работу Интернета: систему глобальной маршрутизации, DNS, пиринг и связность. https://www.nanog.org/meetings/nanog68/home

24-28 октября
RIPE73,
Мадрид, Испания

Встречи RIPE проводятся два раза в год и собирают около полутысячи участников для обсуждения вопросов политики распределения номерных ресурсов (IP-адресов и номеров автономных систем) в зоне обслуживания RIPE NCC, сотрудничества, а также технических вопросов, связанных с маршрутизацией, DNS, связностью, измерениями и инструментарием. Встреча длится пять дней и начинается с двухдневной пленарной программы за которой следуют несколько параллельных сессий заседаний рабочих групп. https://ripe73.ripe.net/

3-9 ноября
ICANN 57,
Хайдарабад, Индия

Встречи ICANN проводятся три раза в год в различных регионах земного шара для того, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. https://meetings.icann.org/en/hyderabad57

6-8 ноября
28-й форум EURO-IX,
Краков, Польша

EURO-IX является ассоциацией точек обмена трафиком (IXP), координирующей различную коллективную деятельность между участниками и предоставляющей информационные услуги, такие как база данных IXP по всему миру. Два раза в год EURO-IX организует встречу участников и всех, кому интересны вопросы обмена трафиком, создания и обслуживания IXP. Это прекрасная возможность обменяться опытом, расширить свою профессиональную сеть и установить новые деловые отношения. https://euro-ix.net/members/forums/29th-euro-ix-forum/

13-18 ноября
IETF97,
Сеул, Южная Корея

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов в области Интернета. В основном работа в IETF производится в многочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100).
http://ietf.org/meeting/97/index.html

6-9 декабря
IGF 2016,
Гвадалахара, Мексика

Internet Governance Forum (IGF) представляет собой форум для обсуждения проблем управления Интернетом. Это многосторонний институт, созванный по решению Генерального секретаря ООН в 2006 году, который с тех пор проводится ежегодно. В дискуссиях принимают участие представители частного сектора, правительств, гражданского общества и технического сообщества.
http://www.intgovforum.org/multilingual/content/igf-2016

В России

21 октября
Санкт-Петербург,
КДЦ«Club House»

Secure IT World 2016

5-я юбилейная конференция по информационной безопасности. В программе: вступительная часть «Тенденции мира Информационной безопасности. Защита АСУТП КВО», тематические сессии «Информационная безопасность как сервис» и «Особое мнение».
http://www.event-house.ru/content/secure-it-world-0

8-10 ноября
Якутск,
СК «50 лет Победы»

Информационные технологии. Телекоммуникации. Безопасность

6-я межрегиональная специализированная выставка. Информационно-коммуникационный сектор Республики Саха (Якутия) является растущим сегментом региональной экономики. В Республике активно внедряются современные технологии предоставления услуг связи. Мероприятие проводится при поддержке Правительства Республики Саха (Якутия) и стало важным и продуктивным деловым событием для региона.
http://www.ses.net.ru/index.php/calendar/322-svyaz-yakutsk-2016

В Москве

18-19 октября,
Swissotel Красные Холмы

Capacity Russia & CIS 2016

Вот уже 12-ый год Capacity Russia & CIS является крупнейшей встречей исполнительных руководителей телекоммуникационных компаний России, СНГ и зарубежных стран. http://www.capacityconferences.com/Capacity-Russia-CIS.html

20 октября,
АЗИМУТ Отель Олимпик

Международный Форум «Современная инженерная инфраструктура. Вокруг Автоматизации. Вокруг ЦОД. Вокруг Сетей»

На мероприятии будут раскрыты все вопросы, связанные с проектированием, построением и эксплуатацией современного дата-центра и всех элементов его инфраструктуры, а также с организацией современных проводных/беспроводных сетей и автоматизацией производственных и бизнес-процессов. http://moscow-bis-2016.ciseventsgroup.com/

1-3 ноября,
Экспоцентр на Красной пресне

RIW 2016

Russian Interactive Week является главным ежегодным выставочно-конференционным событием отечественной отрасли высоких технологий. Конференционная часть RIW 2016 охватывает все современные темы развития Рунета. http://riw.moscow/

7-8 ноября,
Сколково

Highload++

Профессиональная конференция разработчиков высоконагруженных систем. Конференция пройдет в этом году уже в десятый раз и соберет 2500 участников. Мероприятие направлено на обмен знаниями о технологиях, позволяющих одновременно обслуживать многие тысячи и миллионы пользователей.
http://www.highload.ru/

17-18 ноября,
Москва, КЗ Космос

ZeroNights 2016

Ежегодная международная конференция, посвященная практическим аспектам информационной безопасности. ZeroNights рассказывает о новых методах атак и угрозах, показывает возможности для нападения и защиты, предлагает нестандартные методы решения задач ИБ. http://2016.zeronights.ru/

24-25 ноября,
Холидей Инн Лесная

Broadband Russia Forum 2016

За последние шесть лет Форум стал основным местом встреч регуляторов и первых лиц операторских компаний, трибуной для всех, кто внедряет инновации в ИКТ-отрасли.
http://www.comnews-conferences.ru/ru/conference/bb2016

1 декабря,
Центр международной торговли

Пиринговый форум MSK-IX

Крупнейшая ежегодная встреча участников интернет- и телеком-рынка. Форум проводится с 2005 года, с каждым годом собирая все большее число профессионалов.
http://peering-forum.ru/

MSK IX

WWW.MSK-IX.RU

+7 (495) 737-9295

9
ГОРОДОВ

35
ПЛОЩАДОК
ДЛЯ РАЗМЕЩЕНИЯ

600+
УЧАСТНИКОВ

ПОДКЛЮЧЕНИЕ
до **100** Гбит/с

ТРАФИК
2,0+ Тбит/с

18
УЗЛОВ DNS-СЕТИ

Интернет изнутри

2016