ОБМЕН ИНФОРМАЦИЕЙ: создание отраслевых центров кибербезопасности

Д.Костров, директор департамента ИКТ NVision Group

В отрасли связи до сих пор не создано единых правил обмена необходимой информацией по проблемам кибербезопасности. Насколько они необходимы и что нужно сделать для решения этой задачи?

Чего нам не хватает

Рассмотрение существующих подходов и "лучших практик" в обеспечении информационной безопасности бизнеса и государства в Российской Федерации позволяет сделать вывод, что уже выстроен порядок сертификации средств защиты по приемлемым требованиям, есть ряд отечественных средств обеспечения безопасности, есть даже "лекала" с наиболее удачных западных систем киберзащиты. Однако есть и проблема – отсутствие так называемых единых баз знаний инцидентов безопасности. Существующее разрозненное понимание процесса обеспечения безопасности основано на работе небольшого количества экспертов (часто альтруистов) на рынке информационной безопасности и их статьях. Именно с данных шаблонов многие интеграторы, а также чуть более "продвинутые" CISO и проводят построение рубежей безопасности.

Из общения с коллегами из департаментов/отделов информационной безопасности предприятий различных отраслей, архитекторами и разработчиками систем (программно-аппаратных комплексов) становится понятно, что у них есть набор средств защиты, правильные настройки этих систем, позволяющие повысить компетентность инженеров учебные центры; есть рынок MSP и "интеграторов на подхвате", но оперативность защиты упирается в проблему получения (обмена) доверенной информации для решения различных проблем в реальном (или почти) времени.

Почему же до сих пор (2015 год) не создано единых правил обмена необходимой информацией по проблемам кибербезопасности в отрасли связи? При обсуждении этого парадокса с представителями подразделений безопасности (информационной, экономической) выяснилось, что:

- нет определенного доверия между самими операторами вследствие конкурентной борьбы;
- обмен существует, но основан на личном доверии;
- регулятор в области связи молчит;
- нет согласованных документов, регулирующих горизонтальные взаимоотношения операторов связи (пример: не подписаны Меморандумы стран-участников РСС о взаимодействии операторов электросвязи в сфере противодействия мошенничеству на сетях электросвязи и о взаимодействии операторов электросвязи и инфокоммуникаций в сфере обеспечения информационной безопасности);
- нет единых международных стандартов/рекомендаций в данной области.

Между тем в условиях взрывного роста кибератак на различные важные (критические) объекты, на "чувствительную" информацию, а также на сети связи в целом и их элементы эталон обеспечения защиты требует нового комплексного подхода при обеспечении приемлемого уровня информационной безопасности.

Представляется, что правильно было бы использовать существующие и разрабатываемые рекомендации Международного союза электросвязи, созданные в рамках исследовательской комиссии 17 (ИК 17), учитывая, что часть стандартов разрабатывали специалисты из Российской Федерации.

На пути к "центру знаний"

Компьютеры и компьютерные сети используются в настоящее время столь же повсеместно, как электричество или водоснабжение. Безопасность инфокоммуникационных сетей и информационных систем, особенно их работоспособность и отказоустойчивость, стала крайне актуальной темой для бизнеса и государства. Уровень развития инфраструктуры сетей связи основных операторов связи Российской Федерации позволяет говорить о наличии у них специализированных подразделений информационной безопасности, противодействия фроду на сетях связи и т.п. У многий компаний созданы операционные центры безопасности (Security operation center – SOC). Такие центры / подразделения выполняют функцию обеспечения информационной безопасности компании или сторонней организации, которая передала на аутсорсинг ИТ-безопасность или ее часть.

Задача SOC – обнаружение попыток несанкционированного доступа к ИТ-инфраструктуре оператора связи, предотвращение попыток вторжения внутрь защищаемого периметра и управление инцидентами ИБ. Управление рисками происходит методом централизованного анализа событий посредством единой системы, состоящей из персонала, специализированных аппаратных средств и программного обеспечения. Как правило, эти системы работают в режиме 24/7. В состав SOC входят подсистемы контроля и анализа журналов всех имеющихся в ИТ-инфраструктуре типов систем, устройств и приложений, деятельности пользователей, межсетевых экранов, систем обнаружения вторжений (IDPS), антивирусов, систем анализа защищенности и т.д., что позволяет из многомилиардного количества событий выделить критичные с точки зрения нарушения правил ИБ, квалифицировать их как инцидент и произвести его обработку.

Также в мировой практике сложилось понятие групп реагирования на инциденты компьютерной безопасности. Существуют различные аббревиатуры, обозначающие такие группы: CERT или CERT/CC (группа оперативного реагирования на компьютерные инциденты или координационная группа), CSIRT (группа реагирования на инциденты компьютерной безопасности), IRT (группа реагирования на инциденты), CIRT (группа реагирования на компьютерные инциденты), SERT (группа оперативного реагирования на инциденты безопасности).

Операторское сообщество уже не первый год обсуждает необходимость создания "третьей доверенной стороны" – центра кибербезопасности. Предполагается, что данный элемент общей безопасности будет "центром знаний" в вопросах информационной / кибербезопасности для операторов связи Российской Федерации. В отличие от других центров, "центр знаний" не устанавливает никаких систем контроля на сетях операторов связи (не нагружает их), а только взаимодействует на основе добровольности, взаимовыгодного сотрудничества и совместного обеспечения устойчивости, целостности и безопасности сети связи общего пользования Российской Федерации. Доверенные операторы связи, используя собственные системы сбора и анализа инцидентов (например, SIEM),

а также методики, разработанные и переданные сообществом специалистов информационной безопасности (используя международный опыт и "лучшие практики"), применяя общеизвестные форматы, направляют информацию в "базу знаний". Формально "база знаний" состоит из: базы инцидентов, базы расследований, базы "лучших практик".

Подобный центр может обеспечить: централизованную координацию вопросов информационной безопасности внутри отрасли связи; централизованную и специализированную систему обработки сообщений об инцидентах и реакции на них; возможность экспертизы и поддержки в процессе быстрого восстановления инцидентов безопасности; возможность взаимодействия в правовых вопросах, сохранение доказательств в случае судебных процессов; сохранение информации о развитии в сфере безопасности; стимулирование взаимодействия клиентов (операторов) по вопросам информационной безопасности (повышение осведомленности). Решаемыми задачами (функциями) должны стать: выявление признаков проведения компьютерных атак, определение их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения, предупреждения и ликвидации компьютерных атак; прогнозирование ситуации в области обеспечения безопасности сетей связи, включая выявленные и прогнозируемые угрозы и их оценку; организация и осуществление взаимодействия между операторами связи, владельцами информационных ресурсов, правоохранительными и другими государственными органами и иными заинтересованными организациями, включая обмен информацией о выявленных атаках и вызванных ими компьютерных инцидентов; обмен опытом в сфере обнаружения и устранения уязвимостей ПО и оборудования; организация и проведение совместных научных исследований в сфере разработки и применения средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак; осуществление мероприятий по обеспечению подготовки и повышения квалификации кадров; сбор и анализ информации о компьютерных атаках и вызванных ими компьютерных инцидентах, включая установление причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы; осуществление мероприятий по оперативному реагированию на компьютерные атаки и последовавшие циденты путем предоставления информации о способах противодействия и устранения угроз; осуществление взаимодействия между операторским центром и центрами, выполняющими аналогичные функции; информирование заинтересованных лиц и субъектов по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Советы непостороннего

При создании межоператорского центра за основу можно взять модель центра на основе международной Рекомендации (разработка Российской Федерации) МСЭ-Т X.800-X.849 – "Руководство по созданию национальных открытых центров сетевой безопасности на протоколе IP для развивающихся стран". Наиболее применимыми форматами получения и обмена информацией об инцидентах с отечественными центрами безопасности могли бы стать форматы X.1500 CYBEX. Положительным фактором стала бы возможность работы с международными CERT при регистрации в FIRST (Forum of Incident Response and Security Teams). Однако, заметим, предполагается, что международное сотрудничество всех российских центров кибербезопасности должно проводиться только через GOV-CERT.

По проблеме мошенничества на сетях связи операторы на основе законодательных актов (которые надо еще разработать) при создании центра должны подтвердить намерения осуществлять обмен опытом и накопленными знаниями в сфере противодействия мошенничеству на сетях электросвязи, в том числе путем оказания помощи в подготовке специалистов в данной области и повышении их квалификации.

Операторы связи и иные заинтересованные организации должны развивать и укреплять сотрудничество в сфере противодействия мошенничеству на сетях электросвязи посредством: отнесения вопросов противодействия мошенническим действиям на сетях электросвязи к приоритетным направлениям деятельности; развертывания и совершенствования автоматизированных систем противодействия мошенничеству на сетях электросвязи; расширения сотрудничества в области противодействия мошенничеству на сетях электросвязи; разработки процедурных мер противодействия мошенничеству на сетях электросвязи и разрешения инцидентов; совместной разработки документов в сфере обеспечения противодействия мошенничеству на сетях электросвязи; принятия организационных и технических мер по обеспечению противодействия мошенничеству на сетях электросвязи, в том числе по внедрению

автоматизированных систем противодействия мошенничеству (при необходимости разработать методику сертификации указанных систем); разработки рекомендаций по уровню квалификации специалистов, реализующих функции противодействия мошенничеству на сетях электросвязи; определения общих требований по расследованию инцидентов, связанных с совершением мошеннических действий на сетях электросвязи; выработки единых подходов (принципов) к анализу технической информации, полученной в ходе расследования инцидентов, связанных с мошенническими действиями на сетях электросвязи.

Для обеспечения информационной безопасности/кибербезопасности операторы связи в рамках своих функций должны соглашаться осуществлять, развивать и укреплять сотрудничество по таким аспектам, как: информирование об инцидентах, в том числе о попытках нарушения информационной безопасности; обмен опытом противодействия угрозам ИБ; предоставление сведений о перспективных решениях; совместная подготовка обобщенных материалов; оказание содействия в подготовке и повышении квалификации специалистов; иные актуальные вопросы в области информационной безопасности.

Доверенные операторы связи на основе взаимных интересов и принципов равноправия: принимают организационные и технические меры по обеспечению информационной безопасности собственной сети электросвязи; разрабатывают методики (принципы) анализа технической информации, полученной в ходе исследования инцидентов ИБ; не препятствуют обмену сведениями об инцидентах, если это не противоречит российскому законодательству; проводят работы по подготовке своих специалистов в области информационной безопасности и повышения их уровня квалификации.

Хотелось бы отметить, что в рекомендации МСЭ-Т X.1500 описаны методы обмена информацией о кибербезопасности. Эти методы могут использоваться по отдельности или в том или ином сочетании, в зависимости от требований или случая, для того, чтобы повысить уровень кибербезопасности путем согласованного, комплексного, глобального, своевременного и гарантированного обмена информацией. В них не накладываются обязательства по обмену информацией, а также не рассматриваются средства получения и конечное использование информации. Обмен информацией о кибербезопасности (CYBEX) является одним

из элементов обеспечения уверенности и безопасности при использовании ИКТ.

Что касается методов, используемых для обмена информацией, то ожидается, что организации электросвязи получат информацию, которая позволит им принимать решения и меры, направленные на существенное повышение уровня конфиденциальности, целостности и доступности глобальных средств и услуг электросвязи/ИКТ; получат информацию, способствующую безопасному процессу сотрудничества и безопасному управлению, благодаря которым повышается уровень гарантии при обмене информацией между организациями; обеспечат согласованный подход к управлению и обмену информацией о кибербезопасности на глобальной основе; повысят осведомленность о кибербезопасности и улучшат сотрудничество в целях снижения влияния киберугроз, кибератак и вредоносного программного обеспечения.

Предлагается применять такие шаблоны, как: описание "общеизвестные уязвимости и незащищенность (CVE); система оценки общеизвестных уязвимостей (CVSS); перечень общеизвестных слабых мест (CWE); система оценки общеизвестных слабых мест (CWSS); открытый язык описания уязвимостей и оценки (OVAL); расширяемый формат описания списка проверки конфигурации (XCCDF); перечень общеизвестных платформ (CPE); перечень общеизвестных конфигураций (CCE); формат обмена результатами оценки (ARF); описание общих событий (CEE); формат обмена описаниями инцидентов (IODEF); перечень и классификация общеизвестных схем атак (CAPEC).

Если продумывать состав центра, то можно предположить, что в него войдут: центр компетенций, центр анализа и сбора, база "знаний".

Следует также учесть, что в соответствии с решением руководства 8 Центра ФСБ РФ и согласно Указу № 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ", все полномочия по созданию данной системы, разработке методики обнаружения атак, обмену информацией между госорганами об инцидентах ИБ, оценке степени защищенности критической информационной инфраструктуры возложены на ФСБ. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (сокращенно СОПКА) представляет собой единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации. Кроме того, в соответствии с решением Совета безопасности России создать центр реагирования на инциденты информационной безопасности в финансовой сфере, который будет называться FinCERT, а также решением Центрального банка к концу мая 2015 года создать центр реагирования на инциденты для оперативного сбора и обмена информацией о попытках несанкционированного вывода денежных средств из банков, предполагается использовать мировой опыт создания подобных формирований на основе трехуровневой модели.

При создании межоператорского центра надо продумать правила обмена с существующими и создаваемыми в России центрами. ■

Кольчугинские кабельщики работают на импортозамещение

29–30 мая во Владимире состоялся третий экономический форум "Владимирская область — территориальный центр импортозамещения". Это главное событие в деловой жизни региона, постоянным участником которого является АО "Электрокабель" Кольчугинский завод" (входит в "Холдинг Кабельный Альянс").

Одним из главных мероприятий форума стала выставка товаров владимирских производителей, а также предприятий из Волгоградской области. В числе стратегических задач форума – формирование в регионе сети отраслевых центров импортозамещения, и завод "Электрокабель" должен войти в число предприятий, которым предстоит стать ключевыми игроками Центра импортозамещения для нефтегазового комплекса.

Кольчугинский завод выступил партнером круглого стола "Внедрение успешных практик устойчивого развития как важный фактор обеспечения импортозамещения и улучшения инвестиционного климата". Выступая на мероприятии, Алексей Прохоров, директор АО "ЭКЗ", отметил: "Мы зачастую не импортозамещаем, а импортоопережаем. Уже сегодня "Холдинг Кабельный Альянс" предлагает потребителям кабели, не уступающие, а порой и превосходящие по эксплуатационным характеристикам импортные аналоги".

В своем докладе А.Прохоров подчеркнул, что только за последний год силами холдинга разработано более 200 новых изделий в рамках программы импортозамещения в таких сегментах, как судовые кабели, кабели для горнорудной отрасли, нефтегазовой промышленности, линий электропередачи, оптические кабели.

По информации АО "Электрокабель" Кольчугинский завод"