PC WEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
ФЕВРАЛЬ • 2014 • МОСКВА
http://www.pcweek.ru

Российский рынок ИБ: итоги 2013-го и ближайшие перспективы

ВАЛЕРИЙ ВАСИЛЬЕВ

ОБЗОРЫ

Читатели PC Week/RE, как показал недавний наш опрос, главными движителями рынка средств обеспечения информационной безопасности (ИБ) в нашей стране признают частный бизнес (в данном случае представленный корпоративными пользователями ИБ-средств) и государственные структуры, ответственные за национальную ИБ страны. За каждый из упомянутых сегментов участники опроса отдали примерно по 30% своих голосов. На долю регуляторов, отечественных и международных, приходится соответственно 19 и 6%, и в этом точка зрения участников опроса не совпадает с более расхожим в среде ИТ- и ИБ-специалистов мнением о ведущей роли регулирования в поступательном движении российского рынка ИБ на современном этапе развития информационно-компьютерных технологий (ИКТ).

Именно такой оценки придерживается заместитель генерального директора по развитию компании "ЭЛВИС-ПЛЮС" Сергей Вихорев. Он считает, что российский ИБ-рынок в первую очередь вращается вокруг выполнения регулятивных требований, а ИБ-угрозами корпоративные специалисты по ИБ занимаются в той мере, в какой им позволяют технические и финансовые возможности компании, остаточный принцип корпоративного бюджетирования ИБ и здравый смысл руководителя ИБ-службы.

Трудно объяснить, почему влияние на рынок индивидуальных пользователей ИБ-средств (иными словами, отдельных частных граждан) наши респонденты оценили как нулевое. И это при том, что российский рынок антивирусов для домашнего использования, например, чувствует себя совсем неплохо. Да и в целом вендоры не брезгуют этим сегментом ИКТ-потребителей и нередко именно через него успешно добиваются узнаваемости своих брендов в корпоративной среде.

Наши эксперты констатируют сохраняющиеся на протяжении уже нескольких лет большие различия в уровнях обеспечения ИБ в российских компаниях — от отвечающего лучшим мировым стандартам (в ряде крупных структур государственного и частного секторов, прежде всего имеющих отношение к инфотелекоммуникационной, нефтегазовой и банковской отраслям, где сильнее ощущается влияние отраслевых и федеральных регуляторов) до сильно уступающего среднему уровню ИБ в странах с развитой экономикой (в средних и малых компаниях, для которых стоимость средств защиты и выполнения требований регуляторов автоматически переносит большую часть ИБ-рисков и риски несоответствия регулятивным требованиям в категорию приемлемых).

Знаковые ИБ-события прошедшего года

Курьез, связанный с разоблачениями Эдварда Сноудена относительно размеров слежки со стороны спецслужб США за всем и вся, по сути являющийся для специалистов секретом Полишинеля, тем не менее заставил обывателей задуматься о проблемах информационной безопасности, необходимость которой со вступлением человечества в эпоху Всеобъемлющего Интернета существенно актуализируется уже и на бытовом уровне.

Откровения г-на Сноудена с нежелательной для военных и политиков степенью прозрачности продемонстрировали масштабы и возможные последствия кибервойн, разгорающихся между странами.

Кибервойны провоцируют государства на создание специального рода войск — кибернетических, задача которых состоит не только в противодействии угрозам национальной ИБ, но и во ведении наступательных кибероперациий на территории противника.

Все чаще хакерские атаки используются для дестабилизации политической обстановки, нанесения ущерба как отдельным объектам и субъектам, так и целым странам. Тем правительствам (и даже частным структурам), которые не в состоянии сформировать и поддерживать собственные кибервойска, свои услуги предлагают интернациональные отряды кибернаемников — солдат удачи, владеющих (пусть и не по высшему разряду, как оценивают эксперты) навыками ведения разномасштабных кибербоев.

В подобных условиях Россия не может не готовиться к противодействию современным ИБ-угрозам национального масштаба. В прошлом году, напоминает генеральный директор компании "Код Безопасности" Андрей Голов, по инициативе Совета Федерации РФ был запущен проект разработки Стратегии кибербезопасности России; разрабатывать стратегию формирования киберкомандования начало Минобороны РФ; 15 января 2013-го Президент РФ издал указ № 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации".

Вместе с тем, как подчеркивает Сергей Вихорев, с учетом трансграничной природы киберпреступности и кибертерроризма было бы наивно надеяться, что решить проблему национальной кибербезопасности можно усилиями только нашей страны. Для этого, считает он, необходимы консолидированные действия всего мирового сообщества и создание единого правового поля наподобие действующего морского права.

Впрямую к задачам национальной кибербезопасности относится обеспечение ИБ критически важных объектов (КВО), неотъемлемым ИКТ-компонентом которых являются АСУ ТП. В частности, ФСБ России разработала и опубликовала в прошлом году проект федерального закона "О безопасности критической информационной инфраструктуры РФ". Эксперты отмечают, что в 2014-м ФСТЭК и ФСБ продолжат работу над документами, направленными на регламентирование защиты КВО.

Директор Центра информационной безопасности компании "Инфосистемы Джет" Игорь Ляпунов обращает внимание на произошедшую за год заметную подвижку в вопросах защиты АСУ ТП: приходит понимание реального состояния защищенности этих систем (которые ошибочно рассматриваются как изолированные от Интернета) и последствий ИБ-инцидентов с ними как для их владельцев, так и для окружения; постепенно исчезает пропасть между операторами АСУ ТП и ИБ-специалистами, что подтверждается ростом количества проектов по защите АСУ ТП.

В прошлом году, по наблюдениям заместителя генерального директора компании "Аладдин Р.Д." Алексея Сабанова, заметно активизировалось массовое применение электронной подписи (ЭП). Главным драйвером этого процесса неожиданно выступили торговые площадки — обязательное применение ЭП и неквалифицированного сертификата помогло разрешить ряд юридических и организационных проблем в их работе в России. Объем торгов на них Алексей Сабанов оценивает как самый большой для торговых площадок в мире. Вместе с этим ожидания в отношении применения ЭП в системах электронного документооборота не оправдались: переход на ЭДО активизировался, однако он почти повсеместно реализуется без ЭП.

Важное значение г-н Сабанов придает реализации ЭП на телефонных SIM-картах. Он полагает, что появление и распространение этой технологии способствует построению инфраструктуры открытых ключей (он использует термин "инфраструктура доверия" в этом случае) в области связи и серьезно расширяет пространство доверия. Решения, построенные на этой технологии, создают второй доверенный канал для проведения электронных транзакций с возможностью подтверждения клиентом своих действий.

Осознание экономической целесообразности использования облаков и концепции "принеси свое устройство" (BYOD), согласно наблюдениям директора по информационной безопасности в "Microsoft России" Владимира Мамыкина, уже усилило и продолжает усиливать требования корпоративных заказчиков к обеспечению ИБ этих технологий.

Необходимость оперативно оценивать состояние ИБ (желательно в реальном времени) привела к объединению многочисленных и разнообразных средств защиты в сложные комплексы обеспечения корпоративной ИБ, что, согласно наблюдениям Игоря Ляпунова, резко усилило интерес заказчиков к системам ИБ-аналитики. Спрос на них, как он считает, будет расти и в последующие годы.

Существенно влияющей на рынок ИБ тенденцией, обозначившейся в прошлом году, Алексей Сабанов считает сокращение бюджетов как в государственном, так и в частном секторах. По его мнению, это, с одной стороны, на два-три года затормозит рост объемов рынка ИБ, зато с другой — будет способствовать повышению качества предлагаемых продуктов и решений.

Надвигающееся вступление в силу закона № 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" (означающее переход от 94-ФЗ к 44-ФЗ) усугубит, как считает Алексей Сабанов, практику аукционов с многократным снижением цен, что чревато неадекватностью предоставляемых продуктов и услуг. Выход из этого сложного положения он видит в незамедлительном формировании в сфере ИБ саморегулируемых организаций, которые будут препятствовать работе недобросовестных поставщиков на рынке.

Ландшафт ИБ-угроз

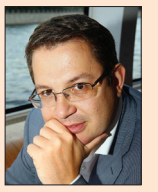
Если, по мнению Сергея Вихорева, сами ИБ-угрозы практически не меняются, то условия их реализации сегодня радикально трансформируются вслед за изменениями, происходящими в ИКТ-инфраструктуре. В первую очередь он обращает внимание на возрастающую гетерогенность современных ИКТ-платформ и рост популярности мобильных средств доступа (в том числе используемых в офисах в рамках программ BYOD) к информационным системам.

Существенное влияние на обеспечение ИБ оказывает расширение сферы применения цифровых технологий. Все чаще

ПРОДОЛЖЕНИЕ НА С. 18 ▸

Наши эксперты

СЕРГЕЙ ВИХОРЕВ
заместитель генерального директора по развитию, "ЭЛВИС-ПЛЮС"

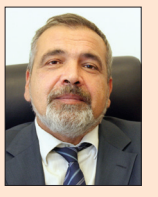


АНДРЕЙ ГОЛОВ
генеральный директор, "Код Безопасности"

ИГОРЬ ЛЯПУНОВ
директор Центра информационной безопасности, "Инфосистемы Джет"

ВЛАДИМИР МАМЫКИН
директор по информационной безопасности, "Microsoft Россия"

ДЖАБРАИЛ МАТИЕВ
руководитель отдела информационной безопасности, IBS Platformix



АЛЕКСЕЙ САБАНОВ
заместитель генерального директора, "Аладдин Р.Д."

ЕЛИЗАВЕТА СПАСЕННЫХ
менеджер по развитию бизнеса, "Информзащита"

Комплексное управление безопасностью: итоги года, планы, ожидания

ТАТЬЯНА МАЛЯВИНА

Несмотря на то что отечественный рынок систем класса IDM (Identity Management) по-прежнему только формируется и многие ИТ-директора еще очень мало знают о профессиональных решениях для управления доступом к информационным ресурсам, вендоры активно развивают свои системы, дополняя их новым функционалом.

Компании "ТрастВерс", разработчику решения КУБ, обеспечивающего автоматизированное управление правами доступа, а также непрерывный мониторинг их изменений, удалось многое сделать за прошедший год.

"Была проделана колоссальная работа по отстройке партнерской сети", — отметил менеджер по развитию партнерской сети "ТрастВерс" Артур Салахутдинов. Работа велась в двух направлениях: 1) организация продаж через системных интеграторов, имеющих опыт реализации проектов в области информационной безопасности и управления доступом к защищаемым информационным ресурсам компаний; 2) развитие технологического партнерства.

Технологические партнеры "ТрастВерс" — это разработчики смежных решений. Интеграция наших систем позволяет "ТрастВерс" обеспечить заказчикам решение целого комплекса связанных задач, не распыляя при этом усилия на расширение функциональности, не имеющей отношения к IDM.

В конце 2013 г. КУБ был интегрирован с ITSM-системой "ИнфраМенеджер". Задача состояла в том, чтобы вписать процессы управления доступом к целевым системам и файловым ресурсам в общую схему управления всеми запросами, связанными с ИТ. Напомним, что ITSM-система предназначена для выстраивания процесса обращения пользователей в ИТ-службу за получением каких-либо сервисов: оборудование рабочих мест, замена техники, установка программного обеспечения, предоставление доступа к ресурсам. Интеграция КУБ и ITSM-системы позволяет автоматизировать получение прав и управление доступом через единый портал для обращений пользователей по любым техническим вопросам.

Еще одним стратегически важным решением была интеграция КУБ с продуктом Indeed-ID Enetrprise SSO, избавляющим пользователей от запоминания множества паролей к различным системам. Продукт поддерживает всевозможные способы аутентификации и автоматизирует ввод паролей в используемые приложения. Совместное решение позволило полностью автоматизировать управление учетными данными и правами доступа пользователей. После приема сотрудника на работу и занесения его в кадровую систему для него автоматически создаются учетные записи и пароли во всех целевых системах и выдаются необходимые права доступа. Удобство работы пользователей повышается за счет использования единого пароля.

Для повышения уровня информационной безопасности наших клиентов в конце 2013 г. мы приступили к интеграции КУБ с решениями компании "Крипто-Про", разработчиком средств криптографической защиты информации и электронной цифровой подписи. В результате удалось полностью автоматизировать выдачу и отзыв электронных сертификатов, обеспечить юридическую значимость заявок за счет использования квалифицированной электронной подписи в соответствии с 63-ФЗ и снизить риски компрометации ключей пользователей, используемых для формирования электронной подписи.

В ближайших планах "ТрастВерс" — расширение технологического партнерства с разработчиками SIEM-систем и отраслевых решений.

"В течение года были запущены десятки пилотных проектов по внедрению КУБ на предприятиях среднего и крупного бизнеса различных отраслей, среди которых можно выделить банки, предприятия нефтегазового комплекса, госсектор, производственные холдинги", — рассказал коммерческий директор "ТрастВерс" Даниил Хазов.

Перечислю основной пул задач, стоявших перед нашими клиентами и успешно решенных внедрением КУБ:

- автоматизация предоставления прав доступа к ресурсам;
- реализация механизма согласования доступа в соответствии с применяемым в организациях порядком;
- интеграция с Oracle Identity Manager для усиления информационной безопасности;
- отслеживание изменений целевых систем и сохранение полной истории этих изменений;
- обеспечение юридической значимости действий при предоставлении и согласовании доступа сотрудникам;
- создание матрицы ролевого доступа;
- интеграция с service desk, кастомизированными кадровыми системами и другими используемыми заказчиком приложениями;
- аудит ресурсов на файловых хранилищах, инвентаризация существующих прав доступа и дальнейшее управление ими;
- отслеживание несанкционированных изменений прав доступа и их исполнителей;
- управление настройкой межсетевых экранов и контроль за ними.

"За последний год было выпущено несколько обновлений продукта, в которых появилось много новых возможностей", — заявил менеджер продукта Сергей Ступин. Расширились возможности КУБ по интеграции с информационными системами. Появился долгожданный комплект инструментов разработки (SDK), с помощью которого наши партнеры и заказчики могут самостоятельно разрабатывать коннекторы. Этот функционал значительно ускорит внедрение системы.

Многое сделано для увеличения удобства пользования системой. Например, управлять доступом можно теперь не только с помощью ролей, а выдавая точечный доступ к определенным ресурсам. Это часто полезно, например, при доступе к файловым ресурсам.

Расширились возможности решения по обеспечению информационной безопасности при выдаче сотрудникам базовых прав. Если раньше мы могли назначать роли сотрудникам и связывать их только с должностью, когда все сотрудники на определенной должности получают одинаковые права к ресурсам, то теперь можно связывать роли с подразделениями, группами подразделений, филиалами и т. д. То есть сотрудник получает права на основании своей принадлежности к определенной структурной единице.

Существенно повышена и производительность системы — теперь КУБ может работать с большим объемом данных и обслуживать сотни тысяч сотрудников.

"В 2014 г. мы продолжим работу по совершенствованию системы и повышению удобства пользователей", — поделился планами руководитель отдела развития Дмитрий Прокопенко. В частности, до конца года планируется выпустить версию, позволяющую работать с системой через единый Web-портал, где можно будет не только отправить запрос на предоставление доступа, но и выполнить настройку системы, провести расследование инцидентов.

Поскольку потребность в профессиональных комплексных решениях по управлению доступом и контролю за ним сейчас ярко выражена не только в крупном бизнесе, в планах компании создать линейку решений, адаптированных под сегменты рынка от Huge Enterprise до Medium SMB.

Автор статьи — руководитель отдела маркетинга компании "ТрастВерс".

СПЕЦПРОЕКТ КОМПАНИИ "ТРАСТВЕРС"

Российский рынок ИБ...

◂ ПРОДОЛЖЕНИЕ СО С. 17

мы встречаем такие термины, как "умный дом", "умный город", "Интернет вещей", "Всеобъемлющий Интернет". Цифровые технологии входят во все сферы нашей жизни, в том числе и в управление бытовыми приборами и устройствами. Это требует обеспечения ИБ в ранее несвойственной для нее среде и реализации новых подходов.

Все еще недостаточным признают эксперты уровень безопасности облачных вычислений. Сегодня в этой сфере, по мнению менеджера по развитию бизнеса компании "Информзащита" Елизаветы Спасенных, необходима проработка таких ключевых задач, как управление доступом и учетными записями пользователей и обеспечение защиты данных, размещенных в частных, публичных и гибридных облаках. В целом, считает она, нужно выйти на уровень защищённости, аналогичный внеоблачным ИКТ-средам. При этом особое внимание следует уделять минимизации рисков при миграции в облака и виртуальные инфраструктуры.

Темп роста объемов передаваемых, обрабатываемых и хранимых данных сегодня настолько высок, что, как утверждает Андрей Голов, такие технологии защиты, как шифрование, фильтрация сетевого трафика, VPN, не успевают за ним, и это создает новые проблемы в обеспечении ИБ. В качестве одного из способов их решения (рыночную реализацию которого можно ожидать в ближайшее время) г-н Голов называет криптоакселерацию.

С повышением осведомленности людей в области ИКТ, отмечает Игорь Ляпунов, для компаний ощутимо возрастает число угроз, связанных с высокотехнологичным фродом и злонамеренным инсайдом, которые чреваты как прямыми финансовыми потерями, так и утечкой критически важной информации.

На этом фоне актуализируются и такие задачи, как контроль привилегированных пользователей — руководителей высшего звена и системных администраторов, со злонамеренными и ошибочными действиями которых, согласно наблюдениям г-на Ляпунова, связаны самые серьезные ИБ-инциденты. По его мнению, ИБ-угрозы со стороны собственных сотрудников представляют для компаний более реальную проблему, нежели угрозы внешние.

Владимир Мамыкин напоминает о том, что в апреле 2014 г. останавливается поддержка операционной системы Windows XP, архитектура которой уже не позволяет вносить в нее изменения, адекватные уровню современных угроз. В условиях ухода Windows XP с рынка Microsoft обещает подготовить для ее пользователей рекомендации, которые помогут им обеспечить приемлемый уровень безопасности после прекращения технической поддержки. При этом, как сообщает г-н Мамыкин, безопасность рабочих мест с Windows XP можно будет поддерживать только за счет дополнительных — организационных — мер: отключать такие рабочие места от Интернета и внутренних сетей, резко ограничивать использование на них внешних накопителей.

Как бы ни менялся ландшафт ИБ-угроз, для бизнеса главной мотивацией защиты от них являются не угрозы сами по себе, а связанные с ними ИБ-риски, транслированные в риски для бизнеса. Пользователи ИБ-средств, как отмечает Игорь Ляпунов, часто оказываются в положении догоняющих. Объясняется это просто: совсем не всегда ИБ-вендоры работают на упреждение, а, наоборот, следуют уже сформировавшемуся спросу, да и развертывание средств ИБ является продолжительным процессом. Поэтому он рекомендует внедрять такие решения, которые позволяют в начале их эксплуатации быть хотя бы на полшага впереди актуальных атак.

Регулирование рынка ИБ в 2013 г. и ожидаемые действия регуляторов в 2014-м

Наши эксперты отмечают высокую активность регуляторов в прошлом году, направленную на совершенствование нормативной базы в области обеспечения безопасности национальной платежной системы, персональных данных, государственных информационных систем, АСУ ТП.

Прежде всего они упоминают приказы ФСТЭК России от 11.02.2013 № 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и от 18.02.2013 № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

Прошлой осенью был опубликован проект приказа ФСБ "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

Все эти документы явили собой, по оценкам экспертов, существенное развитие той части нормативной базы, за которую в стране отвечают ФСБ и ФСТЭК. Отмечается, что в настоящее время во ФСТЭК России находится в разработке ряд других документов, в том числе по мерам защиты в государственных информационных системах конфиденциальной информации, не относящейся к государственной тайне.

По оценкам Игоря Ляпунова, публикацию упомянутых документов профессиональная среда встретила со сдержанным оптимизмом: видно, что регуляторы начали стремиться к тому, чтобы их нормотворчество отвечало реальным угрозам, а не оставалось на уровне только "бумажной безопасности". Он выражает надежду, что эта тенденция продолжится, тем более что и на нынешний год этими регуляторами намечен выпуск ряда чрезвычайно важных документов, ожидаемых сообществом.

По мнению Сергея Вихорева, упомянутые документы не являются упрощением или "либерализацией" требований со стороны регуляторов — они изменяют их подход к процессу формирования таких документов: одновременно с предоставлением компаниям свободы самостоятельно формировать состав мер и способов защиты обрабатываемой ими информации резко повышается их ответственность за адекватность выбранных средств. По сути это смена парадигмы формирования требований со стороны федеральных регуляторов.

Если до недавней поры, как отмечает Андрей Голов, разработка нормативных документов в большинстве случаев велась во ФСТЭК исключительно собственными силами внутри ведомства, то теперь к этому процессу все больше и больше привлекают экспертное сообщество, что является важным шагом в поиске золотой середины между требованиями регуляторов и возможностями тех, на кого эти требования распространяются.

Представители ведущих ИБ-компаний и независимые эксперты стали принимать активное участие в деятельности сформированных при ведомствах рабочих комитетов, таких как технические комитеты по стандартизации "Криптографическая ▸

защита информации" (ТК 26), "Защита информации" (ТК 362) и другие. Это дает им возможность на ранних стадиях формирования регулятивных требований высказывать и отстаивать свои позиции перед регуляторами. Изменения регуляторами подхода к разработке своих документов, по оценкам экспертов, заметно повысило их качество и сократило сроки подготовки.

В прошлом году были разработаны проекты актуальных для страны стандартов. В частности, в ТК 362 подготовлено три проекта по стандартам, два из них — по обеспечению информационной безопасности в облаках.

В конце прошлого года Совет Федерации РФ высказал намерения подготовить новую редакцию закона "О персональных данных". Суть изменений, по словам одного из инициаторов проекта сенатора Руслана Гаттарова, заключается в достижении баланса между техническими требованиями и ответственностью за защиту персональных данных (ПДн). Эксперты ожидают, что новая редакция закона снимет многие практические вопросы, связанные с организацией такой защиты.

По мнению Сергея Вихорева, одной из наиболее острых национальных проблем настоящего времени в области ИБ остается отсутствие отраслевых моделей угроз по отношению к ПДн. Разработка таких моделей предписана законом "О персональных данных". Именно на эти модели ориентирована новая система выбора операторами ПДн мер и способов защиты. К большому сожалению, без них ни постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", ни упомянутый выше приказ ФСТЭК России № 21 не могут работать в полную силу.

Благая идея сократить расходы операторов персональных данных на создание эффективной защиты ПДн за счет переложения части бремени на отраслевых регуляторов пока не заработала. Сегодня, как отмечает г-н Вихорев, операторы ПДн вынуждены — в нарушение закона! — и с большими затратами приглашать внешних специалистов для оценки угроз ПДн, так как без этой процедуры выбрать оптимальный состав мер и средств защиты невозможно.

В этом же ряду, на взгляд Сергея Вихорева, стоит и проблема защиты интересов субъектов ПДн. Закон предписывает оценивать возможный вред субъектам ПДн от несанкционированных действий с их персональными данными, что возложено сегодня на операторов ПДн. Но методик проведения таких оценок нет. Вот и получается, что каждый оператор делает это как может. В решении столь сложной проблемы, полагает г-н Вихорев, крайне нужны рекомендации регуляторов.

Как важный шаг вперед расценивает г-н Голов изменения в подходе к сертификации продуктов по линии ФСТЭК. Он упоминает, в частности, новые требования к сертификации систем обнаружения вторжений.

Вместе с тем, говорит он, было бы желательно, чтобы регуляторы пересмотрели подход к аттестации информационных систем. По его наблюдениям, при ныне действующих механизмах аттестации систему нужно переаттестовывать всякий раз при ее обновлении, но при этом не обновляются средства защиты информации, что создает новые проблемы по обеспечению ИБ. Андрей Голов считает, что работу над обеспечением кумулятивных обновлений и технической поддержкой ИКТ-продуктов, используемых в государственных структурах, в части создания методической базы необходимо довести до логического конца. В этом смысле как важную он оценивает инициативу ФСТЭК, которая предлагает приостанавливать действие сертификатов в случаях обнаружения уязвимостей в продукте. Данная инициатива, по мнению г-на Голова, поможет перейти от формального соответствия регулятивным требованиям к реальной безопасности.

Елизавета Спасенных отмечает, что важным трендом прошлого года в области ИБ стала подготовка российских банков к вступлению в силу положений закона "О национальной платежной системе". Отныне банки обязаны передавать в ЦБ России дополнительные отчеты, соответствующие разработанным ЦБ формам. Эти отчеты должны способствовать повышению безопасности банковской среды нашей страны.

Ряд тенденций развития информационной безопасности в 2014 г. в телекоммуникационном сегменте, как напоминает Елизавета Спасенных, определил вступившие в силу в декабре 2013-го поправки к закону "О связи". Кроме того, значимыми для телекоммуникационных компаний с прошлого года стали изменения в законодательстве, касающиеся блокировки веб-ресурсов. В связи с этим у операторов связи возросла потребность в средствах анализа трафика, позволяющих осуществлять более удобную для абонентов и более точную блокировку запрещенных веб-страниц.

Грядущие технологические проблемы и прорывы

Руководитель отдела информационной безопасности компании IBS Platformix Джабраил Матиев свои главные технологические ожидания в области ИБ связывает с реализацией требований современных законодательных актов, т. е. регулирование, по его мнению, есть и будет основным драйвером технологического развития российского ИБ-рынка.

Наиболее надежными и экономически эффективными способами защиты от современных и будущих ИБ-угроз Сергей Вихорев считает сквозной контроль целостности среды обработки информации и полное шифрование данных. Не случайно в последних документах ФСТЭК России, напоминает он, среди мер защиты информации особо отмечена доверенная загрузка средств её обработки.

Однако, как отмечает г-н Вихорев, контроль целостности и надежное хранение ключевой информации могут базироваться только на аппаратных компонентах информационных систем. Вместе с тем развитие информационных технологий и потребность в компактных и высокопроизводительных средствах доступа к данным стали причиной того, что производители этих средств отказываются от использования традиционных, давно обкатанных интерфейсов для подключения внешних устройств в пользу интерфейсов нового поколения (таких как форм-фактор M.2).

По мнению Сергея Вихорева, в силу этого обстоятельства использовать сертифицированные аппаратные модули доверенной загрузки и электронные замки, которые отработаны на протяжении уже нескольких лет и сегодня представлены на рынке, затруднительно на мобильных автоматизированных рабочих местах, построенных на базе современных компьютеров, из-за технологического отставания этих сертифицированных решений.

Поэтому рынок ждет таких средств защиты этого класса, которые позволят обеспечить доверенную загрузку мобильных компьютеров за счет использования резидентного компонента на базе его аппаратной платформы, защищенную работу пользователей и конфиденциальность информации при работе с корпоративными ресурсами и выходе с этого же компьютера в Интернет.

Елизавета Спасенных, отчасти соглашаясь с изложенным выше мнением Джабраила Матиева, а отчасти усматривая иные стимулы развития ИБ-технологий, отмечает, что потребность в новых средствах защиты у российских ИБ-пользователей появляется как в связи с необходимостью выполнения новых требований и рекомендаций регуляторов, так и ввиду желания сделать приемлемыми для себя новые

ПРОДОЛЖЕНИЕ НА С. 20

Государственные информационные системы: безопасность данных на особом контроле

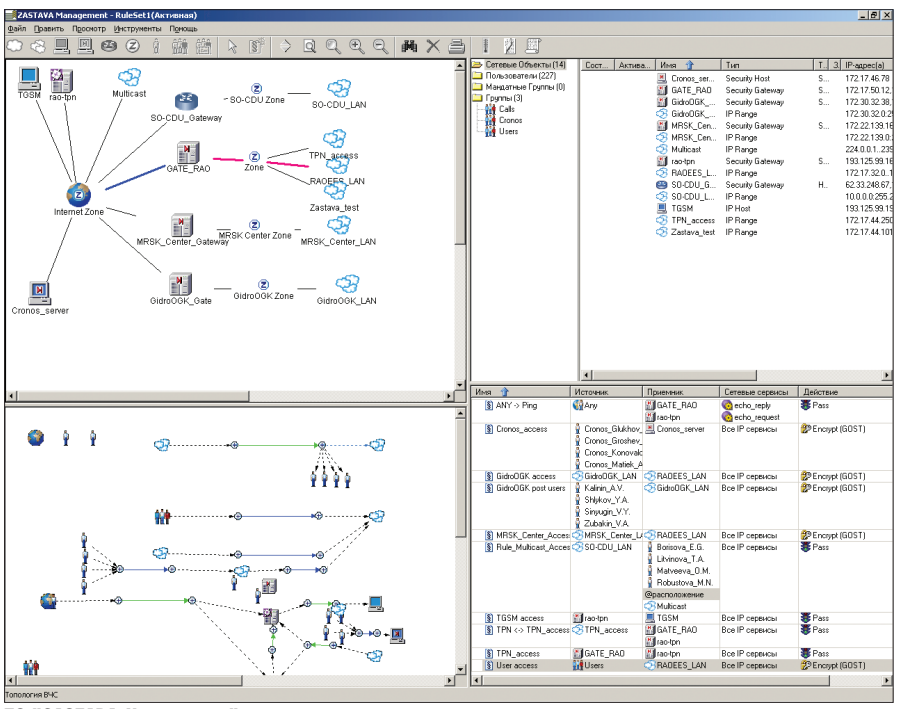
ИГОРЬ ШИТОВ

Для российской ИТ-отрасли 2013 год стал без преувеличения знаковым. Была опубликована "Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 — 2020 годы и на перспективу до 2025 года". Совет Федерации разработал стратегию кибербезопасности России, а в январе 2014-го началось её общественное обсуждение. Эти два программных документа чётко указывают на то, что государство выбрало свой вектор развития в области ИТ. Госорганы активно поддерживают данное направление, становясь не только разработчиками руководящих документов, но и потребителями самых масштабных и интересных решений.

Однако 2013-й стал и годом атак на информационные ресурсы. Компания Cisco в своём отчете "Cisco 2014 Annual Security Report" отмечает, что количество зарегистрированных атак в прошлом году значительно превысило этот показатель за предыдущие годы. Теперь их объектами становятся не только корпорации и частные лица, но и государственные информационные системы (ГИС). Спектр мотивов таких атак — от хактивизма до наступательных действий в кибервойнах.

Государственные органы непосредственно не занимаются коммерческой деятельностью, но размер их информационных систем и ценность информации, обрабатываемой в них, зачастую даже превосходят эти показатели для крупных коммерческих структур. В проведённом исследовании B2B International отмечено, что средний размер ущерба от одного инцидента в сфере ИБ для крупной компании можно оценить в 25 млн. рублей. А общий ущерб для государства даже сложно представить!

В России основными руководящими документами по информационной безопасности государственных информационных систем в 2014 году будут "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (приказ ФСТЭК России от 11 февраля 2013 г. № 17) и "Требования и методы по обезличиванию персональных данных государственными и муниципальными органами" (приказ Роскомнадзора от 5 сентября 2013 г. № 996). В феврале 2014-го приказом ФСТЭК России планируется введение в действие методического документа "Меры защиты информации в государственных информационных системах", который будет разъяснять порядок выполнения требований, установленных приказом № 17. Кроме того, ФСТЭК ведёт разработку единого методического документа, устанавливающего порядок моделирования угроз для безопасности информации независимо от вида обрабатываемой в ГИС информации ограниченного доступа (за исключением государственной тайны). Пока такая методика разработана только для персональных данных.



ПО "ЗАСТАВА-Управление" — мониторинг в реальном времени

Давайте попробуем разобраться, какие же меры защиты регулятор считает приоритетными для государственных информационных систем. Для этого нужно обратиться к 17-му приказу. Состав мер защиты (что нужно делать) получается очень обширным: идентификация и аутентификация субъектов и объектов доступа; управление доступом субъектов доступа к объектам доступа; ограничение программной среды; защита машинных носителей информации; регистрация событий безопасности; защита от вредоносного кода; обнаружение (предотвращение) вторжений; контроль (анализ) защищённости информации; защита среды виртуализации; защита технических средств; защита систем связи и каналов передачи данных, обеспечение целостности и доступности информационной системы и информации.

Среди перечисленных одной из самых важных задач является именно обеспечение сетевой безопасности для ГИС. Это обусловлено прежде всего огромной территориальной распределённостью таких систем и масштабом происходящих изменений. Ярким примером тут может служить проект полного перевода органов госвласти на электронный документооборот к 2017 году. Региональные госструктуры тоже не отстают и строят территориально распределённые ИС, причём их проработка и зрелость зачастую даже выше, чем у федеральных систем. И все эти системы предъявляют самые строгие требования к защите каналов связи.

У нашей компании есть значительный опыт работы с государственными заказчиками. На протяжении последних лет мы решили многие задачи по проектированию систем защиты информации для ГИС, запуску и модернизации технических подсистем ИБ и их технической поддержке. Нашими заказчиками стали Банк России, ФСТЭК, ФНС, Росфинмониторинг, Росреестр, Комитет информатизации и связи г. Санкт-Петербурга, Правительство республики Татарстан. Реализуя эти проекты, мы смогли выделить несколько задач, решение которых должно быть приоритетным при обеспечении сетевой безопасности.

Однако при реализации крупных федеральных и региональных проектов мы столкнулись с важной задачей централизации управления защищённой сетью. Этого требует не только территориальная удалённость подразделений, но и не всегда достаточная компетенция персонала, обслуживающего системы на местах. Вторая важная задача — организация защищённого доступа удалённых (мобильных) пользователей к информационным ресурсам органов госвласти. Это особенно актуально для сотрудников, часто выезжающих в командировки, проводящих выездные проверки и инспекции.

Практика и количество внедрений показывают, что для решения задач сетевой безопасности как нельзя лучше подходят VPN/FW-продукты, в том числе и из линейки "ЗАСТАВА", разработчиком которых является компания "ЭЛВИС-ПЛЮС".

Одно из ключевых преимуществ семейства продуктов "ЗАСТАВА" — гибкость масштабирования системы. Сейчас в промышленной эксплуатации находится корпоративная сеть с общим числом узлов более 10 000 (филиалы, удалённые подразделения и региональные представительства, удалённые пользователи), а технологических ограничений на количество узлов просто нет. Администраторы, работающие с системой каждый день, также отмечают удобство и продуманность централизованного управления из одной географической точки в режиме реального времени с помощью продукта "ЗАСТАВА-Управление". Они могут гибко настраивать правила VPN/FW, вести мониторинг работы всей системы, проводить диагностику и анализ логов, удалённо обновлять VPN/FW-агенты. При этом есть одна интересная особенность: вместо одного глобального центра можно создать целую иерархию центров управления. На каждом уровне иерархии администраторы будут обладать только ограниченным, заранее определённым набором прав в рамках своего территориального сегмента.

Решения семейства "ЗАСТАВА" совместимы с различными операционными системами и аппаратными конфигурациями, в том числе отказоустойчивыми, что обеспечивает высочайшую надёжность системы. Кроме этого наша компания предлагает широкий выбор программно-аппаратных комплексов, которые прошли предварительное тестирование и на которых обеспечена максимальная производительность VPN/FW "ЗАСТАВА".

В каждый проект для ГИС наша компания привносит не только те или иные технические решения, но и экспертизу. Мы сознаём, что разобраться в большом количестве появляющихся нормативных документов бывает очень непросто, поэтому периодически организуем специализированные семинары и вебинары для сотрудников служб ИТ-органов госвласти. Мы всегда открыты к диалогу и готовы делиться своими знаниями с отраслью. Задать вопросы, а также найти анонсы ближайших мероприятий вы всегда можете на сайте компании "ЭЛВИС-ПЛЮС".

Автор статьи — руководитель направления компании "ЭЛВИС-ПЛЮС".

СПЕЦПРОЕКТ КОМПАНИИ "ЭЛВИС-ПЛЮС"

Российский рынок ИБ...

◂ ПРОДОЛЖЕНИЕ СО С. 19

ИБ-риски. Сегодня, считает она, многие ИБ-вендоры стремятся занять открывающиеся ниши в новых направлениях ИБ. Однако полностью удовлетворить требования регуляторов и заказчиков у новаторов пока не получается. Так, по ее мнению, на рынке еще явно недостаточно сертифицированных средств для защиты виртуальных инфраструктур.

Вместе с тем г-жа Спасенных ожидает выхода на рынок принципиально новых решений для защиты виртуальных сред, что стимулируется широким распространением виртуализации, а также ростом популярности облачных технологий. Она полагает, что производители средств виртуализации и их технологические партнеры в скором времени заявят о разработках, связанных с развитием встроенных в гипервизор средств защиты, в которых, возможно, будут широко применяться технологии программно конфигурируемых сетей.

Ключевую технологическую проблему сегодняшних дней в области ИБ Игорь Ляпунов видит в том, что системы ИБ при их возрастающей сложности плохо управляемы и не дают реальной картины происходящего в защищаемой среде. В то же время оперативно получать достоверную информацию об инцидентах и адекватно реагировать на них — вот главная задача службы ИБ. Именно поэтому, считает он, в настоящее время растет спрос на решения класса Security Information and Event Management и Security Intelligence. Рынок уже предлагает достаточное количество средств, предназначенных для решения таких задач, и заказчикам, по мнению г-на Ляпунова, остается лишь вовремя развернуть их у себя и правильно эксплуатировать.

Андрей Голов указывает, что все еще ждет своего решения задача обеспечения юридической значимости электронных документов. Она превратилась в проблему для многих российских министерств и ведомств, потому что серьезно тормозит внедрение там передовых технологий и в конечном счете мешает переходу на удобные способы электронного обмена данными.

По мнению г-на Голова, российские производители по-прежнему заинтересованы в том, чтобы регуляторы четко определили свою позицию в вопросах экспорта российских ИКТ-разработок. Тот путь, который реализован сегодня, — получение экспортных разрешений от ФСТЭК и ФСБ — он оценивает как забюрократизированный настолько, что выполнение связанных с его прохождением организационно-технических процедур практически невозможно.

Как считает Андрей Голов, сложившаяся в этой области практика серьезно мешает нашим разработчикам заявить о себе на потенциально привлекательных для них рынках Юго-Восточной Азии и Латинской Америки, нынешнюю конъюнктуру которых он определяет как благоприятную для появления и закрепления на них российских ИБ-продуктов. Он полагает, что наши ученые и инженеры все еще в состоянии поддерживать паритет компетенций с главными иностранными конкурентами в области математики и криптографии. При надлежащей поддержке государства эти направления могли бы войти в (короткий) список ведущих отраслей российской экономики.