PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
ФЕВРАЛЬ • 2012 • МОСКВА
http://www.pcweek.ru

ИБ на рубеже 2011–2012 гг.

ВАЛЕРИЙ ВАСИЛЬЕВ

ОБЗОРЫ

Информационная безопасность (ИБ) — одна из немногих высокотехнологичных областей, для которой экономический кризис оказался не тормозом, а стимулом развития. Кому хочется терять секреты своего бизнеса в пору обострения конкуренции и массовых сокращений персонала? Да и госрегуляторы не дали повода российским организациям и предприятиям расслабиться в отношении к защите информации. Закон "О персональных данных", например, по-прежнему многие специалисты признают локомотивом развития ИБ в стране.

Чтобы подвести итоги года и оценить перспективы российского рынка ИБ, мы выделили наиболее четко обозначившиеся за последнее время фокусы в данной сфере и обратились к ИБ-экспертам с предложением высказать свое мнение об их состоянии и возможной динамике.

По наблюдениям руководителя лаборатории защиты информации от внутренних угроз "Лаборатории Касперского" Валерия Боронина, основной темой ИБ в мире в 2011 г. стали атаки на крупные структуры, в том числе и правительственные. Он отмечает, что произошла резкая милитаризация Сети, в некоторых странах были созданы кибервойска, официально разрабатывается кибероружие и легализуется его применение. Заметными стали движения хактивистов, разведывательные действия государственных структур ряда стран, использование кибершпионажа частными компаниями.

С большой вероятностью, по мнению г-на Боронина, можно ожидать атак на промышленные SCADA-системы и обнаружения фактов таких взломов в прошлом. К концу наступившего года, как он считает, даже далекие от ИБ люди начнут понимать, что такое критическая инфраструктура и почему ее необходимо защищать. Он полагает, что возможен прецедент асимметричного ответа на киберугрозу, даже ложную и по неверно идентифицированному автору атаки.

Что же касается российского рынка ИБ, то, как отметил генеральный директор компании "Аладдин Р.Д." Сергей Груздев, его финансовые показатели оказались лучше, чем прогнозировалось: рынок ИБ рос быстрее, чем рынок ИТ, в разы превосходя рост европейского. Объясняет это г-н Груздев реализацией отложенного за время кризиса спроса и зрелостью пользователей в том смысле, что им теперь понятна необходимость защиты данных и связанных с этим рисков.

Вместе с тем г-н Груздев обращает внимание на то, что продолжается и даже усиливается порожденное кризисом некорректное поведение в бизнес-среде: нарушение договоренностей, нечестные тендеры, демпинг и т. п. Острый дефицит технических специалистов некоторые компании, по его наблюдениям, решают переманиванием. Это, как он считает, приводит к "диктату" претендентов на вакансии, необоснованному росту их зарплат, расшатывая в итоге рынок, увеличивая стоимость ИБ-проектов и снижая их качество.

Консолидация корпоративных ИБ-средств и централизация управления ИБ

Прошлый год обозначил проблему управляемости ИБ. Руководитель дирекции ИБ компании R-Style Дмитрий Шумилин считает это следствием увеличения количества применяемых ИБ-компонентов и подлежащих решению ИБ-задач, с одной стороны, и ростом числа объектов защиты, с другой.

Централизация управления средствами ИБ, как говорит начальник управления ИБ компании "Техносерв" Павел Ерошкин, это не просто тенденция — это одно из требований, которое, однако, не всегда выполнимо из-за специфики и разнородности ИБ-средств. При этом он отмечает, что примерно половина всех требований к техническим подсистемам ИБ приходится на сетевую безопасность. Он надеется, что в 2012 г. появятся централизованные интегрированные ИБ-решения, которые будут полностью удовлетворять требованиям регуляторов.

Задача защиты отдельных целевых ИТ-систем, считает г-н Шумилин. переросла в задачу интеграции ИБ-компонентов и построения комплексной системы ИБ. Он отмечает, что вопросы ИБ-интеграции возникают сегодня на всех уровнях — от построения сквозной аутентификации до внедрения систем консолидации логов и корреляции событий. Многие современные системы имеют свой функционал управления инцидентами и одновременно обладают средствами для интеграции со сторонними системами управления безопасностью. По мнению г-на Шумилина, системы управления ИБ-событиями (SIEM) становятся стандартным компонентом, неотъемлемой частью корпоративной инфраструктуры. В результате можно ожидать значительного роста источников событий, генерируемых отдельными ИБ-компонентами, упрощения механизма интеграции и усиления функционала обратной связи. Отвечая на спрос на SIEM, ведущие вендоры могут выпустить бесплатные версии таких продуктов, правда, с ограниченным функционалом.

Лидирующие ИТ-вендоры со своей стороны придают тенденции консолидации большое значение. В подтверждение тому заместитель руководителя отдела информационной безопасности компании "Ай-Ти" Аркадий Прокудин ссылается на недавнее приобретение корпорацией HP компании ArcSight и поглощение корпорацией IBM фирмы Q1Labs. Со своей стороны директор по ИБ Microsoft в России Владимир Мамыкин сообщил, что совсем недавно Microsoft представила на рыке продукт System Center Configuration Manager 2012, который наряду с управлением инфраструктурой сети обеспечивает управление антивирусными средствами.

Консолидация корпоративных систем и унификация используемого программного и аппаратного обеспечения, по мнению аналитика направления ИБ компании "Доктор Веб" Вячеслава Медведева, стали наиболее яркой тенденцией прошедшего года. С этими процессами он тесно связывает спрос на централизованные системы управления инфраструктурой, которые позволяют не только эффективно управлять системами, но и поддерживать непрерывность бизнес-процессов, одновременно сокращая затраты на сопровождение и снижая требования к квалификации обслуживающего персонала. Успешность внедрения таких систем, как он считает, во многом будет определять роль ИТ-руководителей в структуре компаний.

Директор департамента ИБ компании "Энвижн Груп" Дмитрий Соболев отмечает, что в корпоративной среде зреет понимание того, что располагать средствами ИБ недостаточно — ими необходимо грамотно пользоваться, для чего нужны соответствующие процессы и технические ресурсы. Он считает, что в 2012 г. могут быть реализованы знаковые проекты, которые продемонстрируют, как обеспечение ИБ может органично вливаться в бизнес-процессы компании и снижать реальные потери бизнеса.

Безопасность виртуальных сред

В силу популярности виртуализации руководитель группы информационной безопасности компании IBS Platformix Джабраил Матиев считает вполне закономерным стремление ИБ-вендоров максимально адаптировать свои продукты под использование в виртуальной среде.

Руководитель отдела инфраструктурных решений компании ИНЛАЙН ГРУП Михаил Штарев напоминает, что применение традиционных ИБ-инструментов в виртуальной среде сопряжено с рядом проблем, что для нее требуются специализированные средства. Он считает, что наконец-то этот факт осознан российскими ИБ-потребителями.

По мнению технического директора компании LETA Александра Бондаренко, основной идеей обеспечения безопасности виртуальных сред, в отличие от традиционных, является не выстраивание периметра защиты, а создание защиты "изнутри", защиты каждой отдельной виртуальной машины. Особенно хорошо это видно, когда виртуальные среды мигрируют между физическими серверами из ЦОДа в ЦОД и защита должна мигрировать вместе с ними.

К настоящему времени платформы для построения решений на основе виртуальных сред, как отмечает системный архитектор по информационной безопасности корпорации IBM в России и СНГ Андрей Филинов, переместились из категории уникальных внутренних и специализированных инфраструктур в категорию предложений для открытого рынка, и обеспечение ИБ таких сред перестало быть индивидуальной задачей каждого отдельного внедрения.

По наблюдениям технического консультанта компании Trend Micro Дениса Безкоровайного, в 2011 г. многие проекты по виртуализации на самых ранних этапах уже включали специализированные, адаптированные для виртуальной среды средства защиты. Он считает, что сегодня передовые решения для защиты платформы виртуализации базируются на тесной интеграции с ней и следует ожидать, что поставщики платформ будут расширять возможности интерфейсов взаимодействия своих разработок со средствами защиты. В результате использование специализированных решений для обеспечения ИБ виртуальных сред будет расти.

Ведущий эксперт по вопросам технической защиты информации компании "Код Безопасности" Александр Лысенко обращает внимание на то, что контроль виртуальной инфраструктуры напрямую зависит от уровня контроля над действиями администраторов инфраструктуры, тем более что получить доступ к данным в виртуальной среде гораздо проще, чем в физической.

Выражая мнение большинства экспертов, Дмитрий Соболев отмечает острую потребность в нормативной базе для ИБ виртуальных сред, особенно если учитывать, что защиту зачастую необходимо обеспечивать сертифицированными ФСТЭК и ФСБ средствами.

Директор по развитию бизнеса компании "Информзащита" Андрей Степаненко выразил надежду на то, что российские регуляторы более определенно выскажут свое отношение к обеспечению безопасности виртуальных сред, что позволит как минимум перестать предъявлять к виртуальным машинам требования, аналогичные физическим серверам, а как максимум — учитывать специфические особенности технологии виртуализации при проектировании систем ИБ.

Информационная защита ИТ-сервисов

Облака. Одним из главных факторов, препятствующих распространению облачных ИТ-платформ, являются проблемы с их защищенностью.

Наши эксперты напоминают, что хотя использование облаков повышает эффективность ИТ, социальные сети, электронные госуслуги и многие другие ИТ-сервисы могут быть организованы и без них. Это следует иметь в виду, тем более что, по словам г-на Мамыкина, для публичных облаков ни в одной стране пока не существует методологии оценки их безопасности. В то же время для частных облаков известно, как обеспечить их защиту, так как для них вполне пригодны многие традиционные ИБ-подходы.

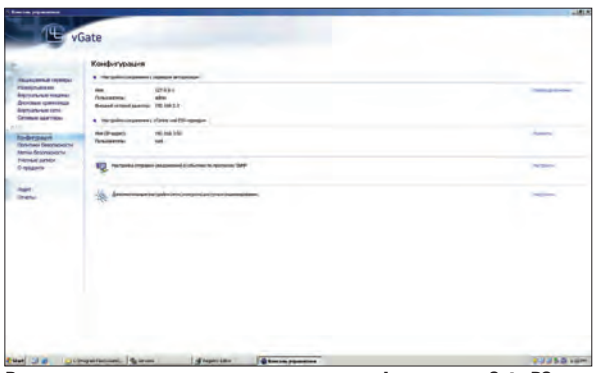
По наблюдениям г-на Бондаренко отраслевые и российские стандарты пока не отражают облачных изменений в ИТ, в то время как за рубежом стандартизацией этого направления в 2011 г. занимались активно: появились такие документы, как NIST-SP-800-144, было организовано (и успело опубликовать ряд документов) сообщество Cloud Security Alliance (CSA) с собственными сертификационными курсами и статусами. В России же пока только появилось (на базе ассоциации RISSPA) представительство CSA.

По мнению руководителя отдела системных инженеров компании Citrix Сергея Халяпина, основная проблема, которую необходимо решить для облаков, заключается в отделении средств управления облачной средой от данных, которые в ней хранятся, чтобы администраторы ЦОДов не могли получать доступ к информации пользователей. Одним из вариантов такого разделения является шифрование данных. При этом следует учитывать тот факт, что с ростом числа пользователей электронных услуг обострится и необходимость в сертифицированных криптографических алгоритмах, в первую очередь при потреб-

ПРОДОЛЖЕНИЕ НА С. 22 ▶

Нужно ли применять специализированные решения для защиты виртуальной инфраструктуры?

Сегодня рынок средств защиты информации (СЗИ) предлагает не так много специализированных решений, способных обеспечить надежную защиту инфраструктуры виртуализации от специфических угроз для этой среды и при этом имеющих сертификаты ФСТЭК России. Тем временем



В консоли управления можно настроить конфигурацию vGate R2

облачные вычисления и технологии виртуализации становятся все более популярными не только среди пользователей этих технологий, но и среди хакеров, инсайдеров и других злоумышленников, все чаще реализующих атаки на такие ресурсы. Очевидно, что для защиты информации в виртуальной среде от несанкционированного доступа, а также для обеспечения соответствия инфраструктуры требованиям законодательства и отраслевых стандартов необходимо применять специализированные СЗИ.

Одним из таких продуктов является vGate R2, разработка российской компании "Код Безопасности". В конце прошлого года компания объявила о выходе технического релиза новой версии своего продукта с поддержкой VMware vSphere 5, одной из самых современных платформ виртуализации. Помимо поддержки платформы VMware vSphere 5 новая версия продукта отличается расширенным набором встроенных шаблонов (PCI DSS 2.0, CIS VMware ESX Server Benchmark 4, VMware Security Hardening Best Practice 4.1 и др.; всего более десяти шаблонов), предназначенных для контроля выполнения принятых в компании ИБ-политик. Каждый шаблон содержит большое количество политик и настроек, которые позволяют привести виртуальную инфраструктуру в соответствие с необходимыми требованиями безопасности. После принятия администратором ИБ того или иного шаблона все действия администратора виртуальной инфраструктуры контролируются и не могут привести к каким-либо изменениям настроек безопасности, заданных администратором ИБ.

Кроме того, vGate R2 позволяет создать индивидуальный шаблон безопасности на основании принятых в компании регламентов информационной безопасности, то есть компиляцию индивидуальных настроек. Из списка предлагаемых политик для создания индивидуального шаблона компании можно выбрать только те, которые необходимы. Впоследствии можно настраивать отчетность о соответствии выбранному шаблону и получать по требованию или по расписанию отчеты с логотипом компании о состоянии информационной безопасности корпоративной инфраструктуры.

Фактически алгоритм применения политик может выглядеть следующим образом. На базе одного или нескольких шаблонов формируются наборы политик для организации. Затем набор политик назначается для категории или уровня конфиденциальности. Объекту (хост ESX/ESXi, виртуальная машина, сетевой адаптер, виртуальная сеть или хранилище) назначается метка безопасности. При необходимости запускается формирование отчета о соответствии инфраструктуры политикам безопасности. При этом пользователю доступно детальное описание каждого шаблона и ссылка на конкретный пункт руководящего документа.

vGate R2 позволяет установить и централизованно контролировать политики безопасности

Для автоматизированной проверки инфраструктуры виртуализации компании на предмет соответствия политикам безопасности можно использовать бесплатное приложение vGate Compliance Checker, в котором также реализована поддержка платформы VMware vSphere 5. Результаты комплексной проверки, содержащие информацию о соответствии инфраструктуры положениям стандартов, vGate Compliance Checker представит в форме структурированного отчета. Затем на основании этого отчета с помощью vGate R2 эти политики можно установить и централизованно контролировать.

Помимо поддержки платформы VMware vSphere 5 и расширенного набора встроенных шаблонов для контроля выполнения принятых в компании ИБ-политик новая версия vGate R2 также отличается:

- новым интерфейсом для просмотра отчетов;
- поддержкой распределенного коммутатора Cisco Nexus 1000v;
- поддержкой 64-битных систем в качестве платформы для vGate Server;
- улучшенным пользовательским интерфейсом и масштабируемостью;
- поддержкой альтернативного метода лицензирования на базе оплаты за пользование защищенной виртуальной машиной в месяц (по модели SaaS).

Сегодня пользователям платформы VMware vSphere 5 доступен технический релиз новой версии продукта с поддержкой этой платформы и другими функциями, описанными выше. Ожидается, что новая сертифицированная ФСТЭК России версия продукта vGate R2 с поддержкой платформы виртуализации VMware vSphere 5 поступит в продажу в первом квартале 2012 года.

ИБ на рубеже...

◀ ПРОДОЛЖЕНИЕ СО С. 21

лении услуг государственных. Важным аспектом обеспечения безопасности в облаках, отмечает г-н Халяпин, станет отказ от использования привычной парольной аутентификации ввиду ее уязвимости и переход на технологии асимметричной криптографии, т. е. внедрение технологий PKI.

По наблюдениям директора департамента развития и маркетинга компании ЭЛВИС-ПЛЮС Романа Кобцева, те ИТ-директора, которые в той или иной степени используют облачные сервисы, сегодня обеспокоены сохранением только целостности и доступности сервисов, но не их способностью сохранять конфиденциальность информации. Из этого он делает вывод, что для современных пользователей облаков риски нарушения работоспособности информационных систем гораздо выше, чем утечка данных. Организации, для которых конфиденциальность информации приоритетна, пока просто не доверяют облакам.

Основные проблемы продвижения облаков г-н Кобцев видит в правовом поле: провайдеры, как он считает, не готовы подписываться под реальными соглашениями об уровне услуг (SLA), а клиенты не готовы представлять реальную оценку своих активов для подготовки этих SLA. Довершает коллизию несовершенство нашей правовой и в первую очередь судебной системы.

По мнению г-на Филинова, клиенты облачных сервисов доверятся инфраструктуре и поставщику услуг, но вот самые деликатные задачи и, конечно, контроль соблюдения поставщиком оговоренного уровня ИБ корпоративный клиент хочет оставить за собой. Андрей Филинов полагает также, что в продвижении облаков предстоит много новой (по смыслу) работы юридического характера, в то время как программно-технические средства для решения облачных ИБ-задач уже доступны для заказчиков.

Со своей стороны г-н Шумилин подтвердил, что ИБ-вендоры в прошлом году в массе своей заявили о готовности своих продуктов для защиты облачных инфраструктур, в первую очередь это относится к сегменту сетевой безопасности (IPS/IDS-решения, межсетевые экраны) и систем аутентификации.

Основной тенденцией в текущем году при доступе к веб-приложениям, как считает г-н Халяпин, будет поиск удобной для пользователя двухфакторной аутентификации. Дальнейшее развитие, по его наблюдениям, получат решения Web Application Firewall, которые могут контролировать трафик веб-приложений и блокировать вывод на экран нежелательной информации.

Электронные госуслуги. Как отметил г-н Филинов, базовый уровень безопасности в электронных госуслугах уже обеспечивается. Однако, считает г-н Соболев, не стоит сбрасывать со счетов и то, что злоумышленники пока просто не научились использовать доступ к ним в интересах своего обогащения.

Нерешенными признает г-н Филинов вопросы комфортного и быстрого пользовательского доступа к электронным госсервисам. Денис Безкоровайный отметил, что в 2011 г. была заметна тенденция к усилению механизмов удаленной аутентификации пользователей. В результате двухфакторная аутентификация, которая раньше применялась в основном для защиты финансовых транзакций, стала доступной и в других сервисах.

Большинство социальных сетей и крупных порталов стало, по его наблюдениям, привязывать аккаунт пользователя к его мобильному телефону для защиты от автоматических регистраций и для подтверждения подлинности пользователя. "Ростелеком" начал продавать носители с ключами цифровой подписи (ЦП) для доступа к сайтам госуслуг.

Сергей Груздев считает запуск портала госуслуг с применением смарт-карт и квалифицированной электронной подписи знаковым событием 2011-го. Этот проект, по его мнению, послужил катализатором дальнейшего развития SaaS и веб-платформ ИТ-сервисов. Он также обратил внимание на появление в прошлом году универсальной электронной карты и на параллельный проект, связанный с созданием карты "Электронное правительство" — платежной карты с сертифицированной ЦП для доступа к порталу госуслуг.

Эмиссия банковских карт "Электронное правительство" с аппаратной реализацией квалифицированной электронной подписи, как сообщил г-н Груздев, была начата в конце прошлого года несколькими банками в Волгограде, Москве и Санкт-Петербурге. Эмитированы работающие карты с банковским приложением международных платежных систем. Начат аналогичный проект с российской платежной системой "Золотая Корона". Появление платежной карты с ЦП, сертифицированной ФСБ, г-н Груздев считает технологическим прорывом в области ИБ банковского сектора и системы госуслуг в электронном виде, поскольку подобных проектов, успешно реализующих объединение двух инфраструктур — платежной и PKI, не существовало.

ДБО. Согласно наблюдениям г-на Филинова, банковские карты перестали быть универсальным и безопасным средством электронных расчетов, в то время как потребность в таких расчетах выросла, и эксперты отмечают активную интеграцию дистанционного банковского обслуживания (ДБО) с социальными сетями и другими онлайновыми сервисами, что усложняет задачи ИБ в ДБО.

Дмитрий Шумилин отмечает, что атаки при удаленном доступе к ИТ-ресурсам становятся более сложными. Наряду с фишингом активизируются такие высокотехнологичные приемы, как "человек посередине" и "человек-в-браузере". Они требуют применения новых средств защиты, способных гарантированно блокировать изменение параметров транзакций, выполняемых на лету.

По мнению г-на Шумилина двухфакторные системы аутентификации должны стать стандартом. Он прогнозирует начало массового применения банковских карт в процессе аутентификации и считает, что это можно реализовать на базе CAP/DPA-технологий или за счет встраивания в карты независимого генератора одноразовых паролей.

Дмитрий Соболев полагает, что настала пора внедрять механизмы поведенческого анализа пользователей ДБО, создавать системы репутационного анализа финансовых транзакций. Он ожидает появления в 2012 г. новых зрелых услуг по защите ДБО и госуслуг.

Одну из таких услуг под названием "АРМ ДБО", позволяющую специалистам провайдера из ситуационного центра реагирования удаленно контролировать степень защищенности программно-аппаратной среды клиента ДБО, вывела на российский рынок компания Group-IB. Как считают представители Group-IB, это поможет осуществлять защиту клиентов от киберугроз, вести сбор информации о ИБ-событиях на стороне клиентов и ее анализ специалистами провайдера.

Однако генеральный директор Group-IB Илья Сачков убежден, что одними лишь техническими средствами обеспечить безопасность клиентского удаленного доступа невозможно. Он считает, что будущее за организационными мерами, и в первую очередь за кооперацией и сотрудничеством участников ДБО. На его взгляд, мож-

но ожидать, что в ближайшей перспективе будут развиваться системы обмена данными между участниками ДБО. Он сообщил, что с прошлого года действует централизованная база данных по мошенническим операциям с использованием систем ДБО, которая, несмотря на малое количество участников проекта (30 банков), заметно улучшила, по оценкам г-на Сачкова, эффективность антифродовых фильтров и тем самым повысила защищенность банков — участников проекта.

ИБ и свободное ПО

С сожалением ситуацию со свободным ПО г-н Медведев характеризует как застойную, выделяя здесь три фактора влияния:

• несовместимость (несмотря на предпринятые в этом направлении усилия) форматов офисных приложений СПО со сложившейся де-факто системой обмена документов;

• отсутствие необходимого количества программных продуктов для бизнеса;

• дороговизна сопровождения.

Являясь приверженцем свободного ПО, он не видит возможности появления в ближайшее время систем, способных потеснить коммерческие программные решения.

Говоря непосредственно о проблемах ИБ в СПО, г-н Бондаренко отмечает потенциальную возможность внесения вредоносного кода, возможность нестабильной работы и, как правило, отсутствие приемлемой поддержки со стороны производителя. По его мнению, массовое распространение (особенно в связи с переводом госсектора на СПО) данных продуктов привлечет к СПО злоумышленников и, как результат, обусловит появление тех же ИБ-проблем, что ныне существуют у проприетарного ПО.

С учётом того, что в большинстве случаев никто за разработанный СПО-продукт ответственности не несёт и непонятно, кто и в какие сроки будет устранять неизбежно появляющиеся ИБ-проблемы, его масштабное использование станет адом для ИБ-специалистов, которым придется регулярно придумывать компенсирующие меры и ждать, когда же сообщество разработчиков разберется с проблемой. По мнению г-на Бондаренко, несколько улучшит положение заметное уже сегодня постепенное появление и распространение продуктов, предназначенных для защиты информации в программных системах, построенных на СПО, но этого, как он считает, явно недостаточно.

Безопасность мобильных конечных точек

В 2011 г. резко обозначилась проблема безопасности мобильных устройств.

Как отметил заместитель генерального директора компании InfoWatch Рустэм Хайретдинов, большинство присутствующих на рынке мобильных устройств создавались для потребительского рынка и не предназначены для принятых в корпоративной среде двухфакторной аутентификации, профилирования пользователей, централизованного администрирования и тому подобных процедур.

По наблюдениям г-на Бондаренко, у большинства организаций сегодня нет возможности контролировать действия пользователей с их мобильными устройствами, когда они находятся за пределами корпоративной сети: какие программы они скачивают, какие сайты посещают, как обращаются с информацией... В итоге риски, связанные с использованием мобильных устройств в корпоративной среде, в 2012-м продолжат стремительный рост. Это потребует распространения на мобильные средства доступа традиционных корпоративных мер защиты конечных пользовательских устройств, что, по оценкам г-на Бондаренко, является непростой задачей. Тем не менее ряд ведущих компаний уже представил на рынке программные продукты, позволяющие решить некоторые из упомянутых проблем.

Заместитель директора центра ИБ компании “Инфосистемы Джет” Евгений Акимов тоже отметил, что в 2011 г. активизировались работы по организации защищенного доступа к информационным ресурсам и контроля утечек для мобильных устройств. По его словам, практически все крупнейшие производители систем защиты заложили в свои решения адаптацию мобильных устройств к системам и шлюзам доступа, возможность централизованного распространения ИБ-политик на них и управления ими.

Решением задачи доступа с мобильных устройств, по мнению г-на Халяпина, может стать комбинирование технологий безопасного клиентского доступа с системами виртуализации десктопов и приложений. Он полагает, что в 2012 г. этот подход распространится, в том числе на хранение и обмен данными между пользователями. Применение облачных технологий хранения и обмена данными в рамках корпоративной инфраструктуры позволит реализовать обмен информацией как между пользователями, так и между различными устройствами одного пользователя, что также поможет избежать присутствия на разных устройствах одного пользователя различных версий документа и утечек данных при потере устройства.

Эксперты считают, что оптимальным вариантом для офисного использования являются изначально спроектированные для этого специализированные мобильные ОС и устройства, которых становится все больше. Реалии российского рынка, очевидно, приведут к появлению отечественных программных разработок, позволяющих обеспечить в этом сегменте соответствие требованиям бизнеса и законодательным нормам в области защиты информации.

Расследование преступлений в сфере ИТ

Согласно наблюдениям г-на Сачкова, прошедший год показал, что направление расследований компьютерных преступлений необходимо развивать как самостоятельную сферу ИТ-отрасли. Он считает, что невозможность защититься только техническими мерами подтолкнула как государство, так и бизнес к решительным проактивным организационным действиям. Государство, отмечает он, провело значительную законодательную работу в сфере борьбы с киберпреступностью. Например, поправки в 28-ю главу УК РФ ужесточили ответственность за преступления в сфере ИТ, внесли ряд дополнительных квалифицирующих признаков. Однако то, что для подготовки поправок не были привлечены эксперты в области ИБ, привело к тому, что только что принятый документ уже требует доработок.

Особо г-н Сачков отмечает активность правоохранительных органов в 2011 г., завершивших ряд громких мероприятий: ликвидацию кардерской фабрики в Подмосковье, аресты интернет-мошенников Степанова и Глотова, судебный процесс против “короля спама” Куваева и др. Он считает их знаковыми, демонстрирующими киберпреступникам, что пора безнаказанности завершается.

Он обращает также внимание на рост активности коммерческих организаций, пострадавших от рук компьютерных злоумышленников. Эти организации все чаще выступают инициаторами расследований инцидентов, обращаясь как в правоохранительные органы, так и к независимым компьютерным криминалистам.

Вячеслав Медведев считает, что после установки систем защиты от утечек компании должны внедрять системы контроля действий пользователей, с тем чтобы формировать доказательную базу при возникновении ИБ-инцидентов. Однако, по его прогнозам, в наступившем году не ожидается широкого выхода на рынок таких ре-

ПРОДОЛЖЕНИЕ НА С. 24 ▶

Опыт "Доктора Веб" по внедрению корпоративных продуктов в 2011 г.: госструктуры и сфера образования под защитой

Ушедший год запомнился не только ожидаемым ростом числа угроз, но и качественным изменением систем информатизации предприятий в самых разных сферах экономики России. Как известно, информатизация сама по себе сразу не приводит к созданию эффективных систем информационной безопасности. Причин тому много. Так, ориентация на использование нелицензионного ПО не просто не позволяет применять многие наработки вендоров, оптимизирующие бизнес-процессы, но, самое главное, не дает возможности внедрить те же серверные продукты — ведь взломанных версий таких решений в сети нет. На это накладывается и почти полное отсутствие опыта у людей, организующих такие сети. Однако со временем до служб информационной безопасности и рядовых системных администраторов все больше доходит простая истина: внедрение лицензионного антивирусного ПО сразу избавляет от массы проблем, с которыми можно столкнуться в будущем.

Компания "Доктор Веб" и ее корпоративные продукты уже много лет занимают ведущие роли в коммерческом и государственном секторах. Нельзя не заметить, что информатизация и переход на лицензионное ПО в различных сферах российской экономики только идут на пользу этому антивирусному разработчику. Среди крупных внедрений Dr.Web в 2011 г. легко отметить проекты в сфере образования, которые оказались крайне успешными. Так, летом 2011-го компания "Доктор Веб" с радостью сообщила о внедрении продуктов из своего корпоративного комплекса Dr.Web Enterprise Security Suite в школах Республики Татарстан. Проект впечатляет своей масштабностью, ведь в единую сеть защиты по нему планируется включить сразу 40 000 рабочих станций и серверов.

"На данный момент (речь об августе 2011 г.) антивирус Dr.Web защищает 16,5 тыс. рабочих станций — и эта цифра растет с каждым днем. Для управления инфраструктурой антивирусной сети используется Центр управления Dr.Web Enterprise Security Suite с выделенным сервером базы данных PostgreSQL на ОС Linux, — рассказывает Камиль Курамшин, специалист Центра информационных технологий Республики Татарстан. — С сервера Dr.Web Enterprise Security Suite осуществляется установка антивируса на рабочие станции, а также контролируется обновление антивирусных баз. Процесс развертывания антивирусной инфраструктуры проходит гладко и без сбоев".

Столь масштабному внедрению продуктов Dr.Web в школах Татарстана предшествовала одна весьма интересная социальная акция, запущенная "Доктором Веб" в сотрудничестве с оператором телекоммуникационных услуг "ЭР-Телеком". Это проект "Защити на отлично", в рамках которого более 100 школ в нескольких российских городах получили возможность бесплатно подписаться на тарифный пакет "Dr.Web Премиум", предлагаемый в рамках услуги "Антивирус Dr.Web" (поставляемой на базе интернет-сервиса Dr.Web AV-Desk). Этот пакет позволяет ограничить доступ юных пользователей сети Интернет к нежелательному контенту и обеспечить безопасность школьных компьютерных сетей.

Как показала практика, российские границы не смогли сдержать образовательные проекты компании "Доктор Веб", которые, как оказалось, могут быть успешно реализованы и за рубежом. Об этом свидетельствует стартовавшая осенью 2011 г. крупная поставка продуктов Dr.Web в учебные заведения Японии. Образовательная система этой технологически развитой страны получает надежную антивирусную защиту в рамках совместного проекта "Доктора Веб" и CHIeru, ведущего японского поставщика ПО для школ и вузов. Эта компания сотрудничает более чем с тысячью учебных заведений на архипелаге. Свыше 270 000 учащихся пользуются поставленными ею решениями. В рамках сотрудничества компаний "Доктор Веб" и CHIeru школы и вузы Японии получают в свое пользование продукты Dr.Web для Windows, Linux, Mac OS X и мобильной платформы Android. Специально для этого проекта была разработана система лицензирования продуктов Dr.Web, которая учитывает специфику образовательной системы Японии. Так, начальным, средним и старшим школам партнеры предложили безлимитную лицензию на продукты Dr.Web, которые могут быть установлены на школьных компьютерах и серверах, а также на личных компьютерах преподавателей и их смартфонах под управлением ОС Android. Для высших учебных заведений Японии предназначены пользовательские лицензии, обеспечивающие защиту личных компьютеров и смартфонов студентов и преподавателей.

Наряду с начальным и средним образованием корпоративные решения Dr.Web активно поставляются и в высшие учебные заведения. Так, стоит упомянуть о внедрении продуктов корпоративного комплекса Dr.Web Enterprise Security Suite в Северо-Западном институте управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации. Поставку лицензий для защиты 740 рабочих станций, 43 серверов и 40 почтовых шлюзов осуществила компания "Инфогрупп". Другое крупное внедрение осени 2011 г. — защита 1500 рабочих станций в Ижевском государственном техническом университете (ИжГТУ).

"ИТ-инфраструктура вуза децентрализована, поэтому нашей задачей было предоставление сервиса антивирусной защиты для пользователей корпоративной сети, — говорит инженер-программист отдела информатизации ИжГТУ Раис Ахкямов. — Установка сервера и подготовка необходимых скриптов не заняли много времени. Особо хотелось бы отметить высокий уровень обнаружения вредоносного ПО, широкий диапазон настроек антивирусных агентов, централизованные обновления и отменный уровень сопутствующего сервиса".

Компания "Доктор Веб" и ее партнеры не забыли и о крупных госструктурах, которые в большинстве своем успешно используют антивирусные продукты Dr.Web. Так, в конце 2011 г. о продлении лицензии на антивирусные продукты Dr.Web сообщил Аппарат Государственной думы Федерального собрания Российской Федерации.

Как отмечает ведущий консультант отдела информационных технологий Управления документационного и информационного обеспечения Аппарата Государственной думы Елена Григорьева, антивирусные продукты Dr.Web защищают рабочие станции депутатов Госдумы и гражданских служащих Аппарата с 2000 г. "В 2010—2011 годах для защиты рабочих станций, подключенных к компьютерной сети Государственной думы, в рамках исполнения государственного контракта был внедрен программный комплекс Dr.Web Enterprise Security Suite. Еще во время тестовых испытаний мы ощутили преимущества, которые давал Центр управления. Удаленная проверка, лечение инфицированных объектов и обновление антивирусных баз стали легкими и нагядными для администратора, — отмечает г-жа Григорьева. — Пригодилась возможность синхронизации времени".

Чем же порадует "Доктор Веб" в наступившем году? Традиционно, выпуская свои решения, компания "Доктор Веб" стремится не просто обеспечить антивирусную защиту, но и решить проблемы пользователей. Например, основным путем проникновения вирусов в сеть любой организации служат, как известно, ее сотрудники. Как правило, они работают не только в свое официальное рабочее время, но и в дороге (используя мобильные устройства и планшеты) и дома. В связи с этим необходимо не просто защитить сеть, но и создать некую сферу безопасности — настоящее облако. Где бы ни хранились и ни обрабатывались данные, где бы ни находился сотрудник компании — он и его устройство должны быть защищены от любых типов угроз. Об этом мало кто знает, но антивирусные решения всегда разрабатывались как облачные — задолго до того, как понятие облаков стало активно продвигаться на рынок. Это позволяет легко выполнить описанную задачу. Пример внедрения Dr.Web в школах Японии — одно из первых внедрений в соответствии с новой концепцией безопасности, которой предстоит стать одним из элементов цифрового будущего, основанного на понятии свободы творчества и раскрытии всех возможностей, которые предоставляют современные технологии.

В наступившем году специалисты компании продолжат совершенствование хорошо известных продуктов и технологий. Если прошедший год был ознаменован выходом нового антивирусного ядра, имеющего поистине революционные характеристики, то наступивший 2012-й должен быть отмечен аналогичным качественным скачком в характеристиках пользовательских и корпоративных решений, построенных на этом ядре. Уже в ближайшее время выходит обновление продуктовой линейки Dr.Web Enterprise Security Suite. Оно позволит существенно поднять уровень детектирования новейших угроз и одновременно снизить нагрузку на компьютеры пользователей. Как известно, законодательство требует использования всеми компаниями сертифицированных решений. В связи с тем, что процесс сертификации занимает более полугода, перед клиентами стоит проблема выбора между сертифицированными решениями, собранными довольно давно, и несертифицированными, но включающими новейшие разработки. Компания "Доктор Веб" решает данную проблему с помощью так называемого инспекционного контроля — и уже скоро её клиенты получат сертифицированную версию, обновленную до современного уровня.

ИБ на рубеже...

◀ ПРОДОЛЖЕНИЕ СО С. 23

шений и роста их популярности. С достаточной долей вероятности рост внимания к подобным системам, по его оценкам, можно отнести на следующие два года.

Чтобы поймать современного финансового мошенника или грамотного ИТ-нарушителя, надо, как отметил г-н Филинов, изучить и сопоставить гигантские объемы данных мониторинга системы и операций. Поэтому логично в 2012 г. ожидать роста интереса к средствам класса business intelligence с точки зрения их использования в аналитической деятельности при расследовании ИТ-преступлений.

Регулирование ИБ

Основным событием 2011 г. в области государственного и отраслевого регулирования ИБ стало принятие поправок к закону "О персональных данных". По общему мнению экспертов, изменения в 152-ФЗ и других законах, а также принятие нескольких новых, также относящихся к регулированию ИБ, обозначили основную тенденцию — усиление госрегулирования в этой области.

Вместе с тем в прошедшем году, согласно наблюдениям г-на Медведева, не наблюдалось массового внедрения систем защиты, соответствующих законодательным требованиям. Причины этого он видит в дороговизне, сложности и избыточности таких систем для большинства компаний.

Как считает г-н Акимов, большинство компаний для выполнения регуляторных требований по ИБ стремятся получить положительное заключение о соответствии (сертификат, аттестат и т. п.), которое отражает состояние ИБ компании на определенный момент времени. Такой подход, по его мнению, приводит, как правило, к созданию большого количества подсистем ИБ и появлению "зоопарка" средств защиты, предназначенных для выполнения требований различных нормативных актов.

Что касается отраслевого регулирования, то, как отметил г-н Акимов, можно ожидать, что разработки стандартов и рекомендаций по ИБ, которые велись такими структурами, как Инфокоммуникационный союз, Банк России, НАУФОР, РСА, НАПФ, продолжатся и будут закреплены законодательно.

Как напоминает руководитель направления ИБ компании КРОК Михаил Башлыков, наступивший год — выборный, поэтому можно ожидать появления новых требований к компаниям, может поменяться структура организаций, которые отвечают за контроль систем ИБ. Вместе с этим наши эксперты отмечают усиление и даже ужесточение регулирования ИБ.

Развитие направления соответствия регулятивным требованиям, по мнению г-на Акимова, подталкивает компании к переходу от выполнения отдельных конкретных требований к ИБ к выстраиванию систем обеспечения комплексного соответствия, позволяющих учитывать сразу набор нормативных актов и стандартов. Такой подход позволит создавать системы эффективного контроля соответствия и выстраивать прозрачные взаимосвязи между внутренними процессами ИБ и внешними нормативными требованиями, тем самым обеспечивая постоянную готовность компании к эффективному для себя выполнению требований ИБ-регуляторов.

"Необходимость в ИБ-интеграции продиктована сложностью ИБ-проектов"

Зеленоградскую компанию "ЭЛВИС-ПЛЮС" можно считать старожилом российского ИТ- и ИБ-рынка: в конце 2011-го она отметила свой 20-летний юбилей (www.pcweek.ru/business/article/detail.php?ID=135505). В последнее время компания активно развивалась и, по предварительным данным, в 2011 г. по обороту вышла на показатель 1 млрд. руб.

Своими оценками текущей ситуации на рынке информационной безопасности (ИБ), итогов развития интеграционного направления в этой области за прошедший год, а также перспектив в сфере ИБ на ближайшее будущее поделился генеральный директор "ЭЛВИС-ПЛЮС" ***Виктор Лебедев****.*

Виктор Лебедев

К каким изменениям рынка системной ИТ-интеграции привела тенденция заниматься обеспечением ИБ непосредственно в ходе ИТ-проектов, по возможности интегрируя средства защиты в ИТ-инфраструктуру, а не внедряя наложенные решения через специализированные ИБ-проекты?

Включение требований ИБ в ИТ-проекты сделало такие проекты комплексными. Помимо технического усложнения это, как правило, увеличивает число участников как со стороны заказчиков (их интересы в проекте представляют разные структуры — в первую очередь, учитывая специфику рассматриваемых проектов, это ИТ- и ИБ-службы), так и со стороны исполнителей, что усложняет проекты организационно. На стороне заказчиков, как правило, управление проектом в целом не ведется, и этим вынуждены заниматься мы — интеграторы.

Успех проекта теперь зависит от взаимодействия привлеченных к его выполнению ИБ-интегратора и ИТ-интегратора. Если же решение задач ИБ заказчик делегирует исключительно ИТ-интегратору, то от его компетентности в области ИБ зависит результат проекта в целом.

В любом варианте актуальной является способность генерального подрядчика грамотно управлять проектом. В практике нашей компании, например, есть ИБ-проект, в котором количество привлеченных (узкоспециализированных) субподрядчиков достигало пяти компаний.

Какой из двух упомянутых сценариев сегодня встречается чаще?

Крупные ИТ-интеграторы имеют собственные специализированные ИБ-подразделения, что позволяет им многие проекты выполнять своими силами . Однако кризис 2008 г. привел к тому, что некоторые интеграторы стали избавляться от непрофильных активов, в результате чего их ИБ-подразделения подверглись существенным сокращениям. Таким образом, начал формироваться пул специализированных ИТ- и ИБ-интеграторов, не стремящихся к расширению своих компетенций на смежные области и способных выполнять в кооперации ИТ-проекты любой сложности.
В основном же выбор сценария ИТ-проекта зависит от доверия заказчика к привлеченному исполнителю. У каждой структуры заказчика, заинтересованной в успехе проекта, есть свои профессиональные и партнерские предпочтения, и они с гораздо большей готовностью привлекут те компании, с которыми знакомы по совместной работе. Эти компании уже знают особенности инфраструктуры заказчика, его методы, технологии, системы защиты, а потому априори имеют возможность оказаться эффективными исполнителями проекта.

Кто же он такой — российский интегратор информационной безопасности? Каков его бизнес-портрет?

Необходимость в ИБ-интеграции продиктована прежде всего сложностью обеспечения ИБ в современных условиях. Задачи создания систем защиты информации сегодня ничуть не проще создания систем информационных. Говорить об ИБ-интеграторе вообще трудно. Легче составить представление о них, обсуждая конкретные проекты — разработку документации, консалтинг, создание конкретной ИБ-системы и т. п. Если у заказчика есть потребность в таком проекте, то круг исполнителей, способных его выполнить, в стране известен довольно точно. Среди них — и крупные ИТ-интеграторы со своими ИБ-подразделениями, и универсальные, и узкоспециализированные ИБ-интеграторы. Проводить между ними жирную разделительную черту я не стал бы.

Что же касается некоторых общих черт, присущих всем ИБ-интеграторам, то прежде всего давайте отметим, что каждый из них работает на ИБ-рынке. Рынок этот я характеризую как довольно закрытый и регулируемый намного сильнее, чем ИТ-рынок в целом. У него есть свои специфические требования, свои регуляторы, лицензиары и лицензиаты, есть регламенты использования на стороне заказчика конкретных подсистем защиты.

Те компании, которые взаимодействуют со всеми участниками ИБ-рынка — заказчиками, регуляторами, производителями, интеграторами — и которые в состоянии наиболее полно выполнить все вышеупомянутые требования, я бы и назвал ИБ-интеграторами.

ИТ-интегратор, как правило, сильно уступает ИБ-интегратору в вопросах взаимодействия с регуляторами — он не всегда может компетентно объяснить, чем продиктовано то или иное нормативное требование. Чаще всего он занимает такую позицию: сформулируйте свои требования сами — и я их выполню. Компетентность ИБ-интегратора позволяет ему корректировать требования заказчиков в целях повышения эффективности ИБ-проекта.

Можно ли утверждать, что упомянутая выше тенденция обеспечивать ИБ непосредственно в ходе ИТ-проектов нивелировала остроту противоречий между требованиями ИТ и ИБ?

У заказчика противоречия между ИТ- и ИБ-направлениями рождаются как противоречия между его службами ИТ и ИБ, возникающие при формулировании требований к параметрам систем и режимам их эксплуатации. Идеальная с позиций ИТ информационная система обеспечивает доступ ко всем своим ресурсам для всех, а мнение об идеальной системе у ИБ-специалистов диаметрально противоположное.

Помимо принципиальных, я бы сказал, диалектических противоречий в требованиях со стороны этих двух служб к назначению ИТ есть и куда более прагматичные и, кстати, превалирующие аспекты, как, например, борьба за бюджеты, которые у заказчиков уже разделены.

Что же касается рынка в целом, то тут идет борьба за коммерческие интересы между участниками рынка, в том числе между ИТ- и ИБ-интеграторами. У каждой стороны своя объективная и субъективная аргументация собственных преимуществ в борьбе за заказчика.

Эту коллизию всякий раз разрешает сам заказчик — именно он определяет, какой должна быть реализуемая система. Невозможно не упомянуть, что на позицию заказчика влияет регулирование ИБ. Сегодня это в первую очередь закон "О персональных данных".

Спрос на системы защиты персональных данных породил немало недобросовестных, недостаточно компетентных фирм, которые тем не менее тоже называют себя ИБ-интеграторами. Поскольку закон "О персональных данных" затрагивает миллионы компаний, большая часть которых не имеет должного опыта в области защиты информации, нередко подобных квазиинтеграторов воспринимают как гуру. Их присутствие на рынке приводит к появлению эрзац-продуктов и эрзац-услуг, так как только квазиинтеграторы могут выполнять заказы по диктуемым ими демпинговым ценам, которые ниже среднерыночной себестоимости. В результате у заказчиков, идущих у этих "гуру" на поводу, оказываются измененными привычные бизнес-процессы, а защиты как не было, так и нет.

Чего же все-таки в регулировании ИБ больше — плюсов или минусов?

Упомянутый закон уже несколько лет является основным драйвером рынка, поэтому отношение к нему со стороны интеграторов очевидно положительное. С позиций заказчиков, оценка влияния этого закона неоднозначна. С одной стороны — требования закона являются ограничением и обременением для бизнеса и поэтому воспринимаются негативно. С другой стороны, давайте посмотрим как на пример на требования к оформлению налоговой отчетности. Компании к ним давно привыкли, а собственники бизнеса научились использовать эту отчетность для оценки состояния дел. Нечто похожее происходит в отношении требований к защите информации.

Упомянутый закон во многом уже соответствует Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Это упрощает для российских компаний международное общение, в том числе и трансграничную передачу данных. Ну а внутри страны, отвечая за соблюдение конституционных прав граждан, государство просто обязано принимать меры к защите этого рода личной информации.

Есть мнение, что закон навязывает способы защиты персональных данных. Я так не считаю. Операторам персональных данных следует грамотно различать, что от них требуется для выполнения закона, а что только рекомендуется. Так, в законе говорится об оценке соответствия его требованиям. А ее можно проводить несколькими способами: декларацией, приемо-сдаточными испытаниями и сертификацией. Есть из чего выбирать. Однако нужно грамотно оценивать трудоемкость и стоимость каждого способа в каждом конкретном случае. Вполне может получиться, что без использования сертифицированных средств оценка соответствия системы защиты персональных данных окажется столь же сложной и дорогой, как ее сертификационные испытания. Опыт показывает, что использование сертифицированных средств для заказчика выгоднее во всех аспектах. Кстати, сегодня на рынке доступны самые современные ИБ-средства, сертифицированные в соответствии с требованиями этого закона.

Однако повторю: оптимальный способ оценки соответствия зависит от конкретной ситуации у конкретного заказчика. В практике нашей компании есть созданные нами системы защиты персональных данных, от аттестации которых заказчик отказывался, ограничиваясь только нашей декларацией ее соответствия требованиям закона "О персональных данных", и после этого успешно проходил проверку Роскомнадзора.

Как правило, при проверках заказчики сами взаимодействуют с регуляторами. Вместе с тем по их просьбе мы тоже можем подключаться к проверкам — помогаем им обосновать свою позицию вплоть до обращений в прокуратуру.

Среди клиентов "ЭЛВИС-ПЛЮС" более 40% относятся к госсектору. Что-нибудь изменилось за прошлый год в работе с ними по направлению ИБ?

Во-первых, нужно отметить, что для госорганизаций основным драйвером в области ИБ сегодня является не закон "О персональных данных". Вместо него эту задачу выполняет ряд постановлений и указов руководства страны, определяющих порядок межведомственного взаимодействия и оказания государственных услуг в электронной форме (на которую, согласно указу президента страны, госструктурам надлежало перейти с июля прошлого года). Они вызвали очень интересные процессы в области обеспечения ИБ в государственных организациях и предприятиях, наиболее примечательные из которых относятся к защите не закрытой, а открытой информации — обеспечению ее достоверности и доступности. Ведь известны случаи изменения содержимого страниц даже на президентском сайте.

При оказании госуслуг в электронном виде, когда персональные данные граждан начинают передаваться по различным ведомственным локальным сетям и Интернету, предстоит решить задачу соответствия закону "О персональных данных" межведомственного документооборота. Не менее остро стоит проблема технологического и организационного согласования ведомственных информационных систем между собой. Известно, что построены они в том числе и в сфере обеспечения ИБ, на базе совершенно разных продуктов и разными интеграторами.

Если говорить об изменениях в области ИБ в госсекторе, то в силу упомянутых причин ИБ-проекты там стали масштабнее и существенно превышают по объемам проекты в коммерческих организациях. На ИБ в госструктурах сказывается также длительное недофинансирование ИБ-направления, в результате чего они сильно отстали от коммерческих фирм и многие ИБ-задачи там приходится решать с нуля. Да и проблема с ИБ-кадрами в госструктурах стоит острее, нежели в частном бизнесе. К тому же изначально отношение к защите информации в государственном секторе было более формальным: на первом плане выполнение требований регуляторов, а не борьба с реальными утечками информации.