PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
ОКТЯБРЬ • 2013 • МОСКВА
http://www.pcweek.ru

Информационная безопасность в финансовом секторе

ВАЛЕРИЙ ВАСИЛЬЕВ

ОБЗОРЫ

Финансовый бизнес в России относится к наиболее зрелым в области ИБ. Вместе с тем радикальные изменения в сфере ИТ, связанные с масштабной виртуализацией ИТ-ресурсов, с распространением мобильного доступа, с переходом к облачной ИТ-инфраструктуре как на стороне самих финансовых организаций, так и на стороне их клиентов, заставляют участников финансового бизнеса, охватывающего практически все государственные и частные структуры наряду с частными лицами, использовать новые технологии и средства обеспечения информационной безопасности (ИБ).

Операционная деятельность финансовых структур, связанная непосредственно с деньгами, особенно привлекательна для киберзлоумышленников. Специалисты в области ИБ по-прежнему видят большие проблемы в защищенности дистанционного банковского обслуживания (ДБО). Мошенничество в банковской сфере заставляет банки внедрять дорогие системы борьбы с фродом, наносящим им значительный ущерб.

Деятельность кредитно-финансовых организаций остается в фокусе внимания регуляторов. До сих пор в профессиональной среде продолжается обсуждение положений вступившего в силу закона "О национальной платежной системе". Предполагается, что в ноябре будет опубликована (а с 1 января 2014 г. вступит в силу) новая версия стандарта PCI-DSS.

Опубликованные в августе результаты исследования "Информационная безопасность в российских банках", проведенного аналитическим центром Zecurion Analytics и Ассоциацией российских банков, дают представление о нынешнем состоянии ИБ в кредитных учреждениях страны. Количество банков, выделивших ИБ-службы в самостоятельные структурные подразделения, увеличилось до 64% (против 51% в прошлом году). Однако отдельный ИБ-бюджет имеет лишь 31% банков, у 23% участников опроса ИБ- и ИТ-бюджеты объединены. О дефиците финансирования направления ИБ заявили 38% респондентов.

ИБ финансовых организаций сегодня

Всё, что связано непосредственно с живыми деньгами, всегда было наиболее притягательным для преступников. Но если раньше финансовые организации как центры аккумулирования и поддержки потоков денежных средств были сосредоточены в основном на вопросах физической защиты материальных ценностей, то сегодня, в эпоху перевода денежных активов и платежей в безналичную форму с широким использованием информационно-телекоммуникационных технологий, намного актуальнее для банков стали задачи безопасности информационной.

Поскольку финансовые организации, как напоминает Кирилл Керценбаум, руководитель группы предпродажного сопровождения компании "Лаборатория Касперского", действуют в условиях сильной конкурентции, они стараются оперативно выводить на рынок новые банковские продукты, для чего весьма подходит онлайновая среда, интернет-банкинг. А это порождает новые для банковского бизнеса ИБ-риски и, как следствие, вызывает необходимость разрабатывать и использовать новые ИБ-средства.

Однако несмотря на высокую конкуренцию, согласно наблюдениям Сергея Котова, эксперта по информационной безопасности компании "Аладдин Р.Д.", банки ведут относительно консервативную политику в области внедрения новых ИБ-технологий. Он считает такую стратегию правильной, имея в виду критическую значимость банковского бизнеса для страны, и тем более правильной в нынешних условиях, когда доходы у банков не так велики, как хотелось бы.

Вместе с тем в технологическом консерватизме в области ИБ, о котором говорит Сергей Котов, системный архитектор по ИБ из компании IBM в России и СНГ Андрей Филинов усматривает и отрицательные моменты: поскольку участники рынка ДБО не спешат менять используемые средства защиты на более стойкие, технологии и инфраструктура, используемые сегодня в банках, не всегда способны защитить ДБО от высокотехнологичных атак.

Ссылаясь на статистику, согласно которой более 40% всех ИБ-инцидентов в банках связаны с незаконными операциями через интернет-банкинг, а объем мошенничества в системах ДБО на территории России и СНГ за прошлый год превысил 400 млн. долл., Леонид Плетнев, старший аудитор компании "Информзащита", указывает, что в банках растёт потребность в выстраивании процессов выявления и пресечения мошенничества и во внедрении решений для автоматизации фрод-мониторинга. Особенно рискам, связанным с ДБО, подвержены небольшие финансовые организации, которые только выходят на этот рынок, утверждает Владимир Мамыкин, директор по информационной безопасности компании Microsoft в России. Такие компании в отличие от крупных, как правило, не имеют в своем распоряжении хороших ИБ-специалистов и практически не обладают экспертизой в этой области.

Бичом ДБО является мошенничество, как инсайдерское, так и внешнее. Правильно выстроенные процессы антифрода, по мнению Леонида Плетнева, позволяют снизить как прямые финансовые потери из-за фрода, так и связанные с ним репутационные риски, повысить доверие клиентов к финансовой организации. Вместе с тем эксплуатация специализированных систем противодействия фроду, как напоминает г-н Плетнев, должна сочетаться с регулярным проведением тестов на проникновение и сканированием на предмет уязвимости, с применением средств контроля целостности, антивирусных программ и прочих привычных ИБ-средств общего назначения.

Андрей Филинов отмечает, что на протяжении нескольких последних лет банки концентрировали свое внимание на ИБ систем и процессов на клиентской стороне, что связано как с ростом интереса клиентов к мобильным приложениям и сервисам, с развитием электронной торговли, с увеличением разнообразия мобильных платформ и степени их использования в повседневной жизни, так и с тем, что безопасность устройств, используемых клиентами для взаимодействия с платежными системами, все еще недостаточна для того, чтобы отказаться от традиционных расчетов.

Сергей Котов отмечает, что большинство банков озабочено борьбой с фродом в основном на своей стороне. В то же время, по его наблюдениям, существуют и нормально работают антифрод-терминалы, эффективно повышающие защищенность и на стороне клиента, однако на их интеграцию в автоматизированную банковскую систему (АБС) потребуется некоторое время (сегодня трудно сказать, сколько, хотя стоимость такой интеграции невелика).

Нынешнюю сосредоточенность банков на противодействии фроду на своей стороне (а не на стороне клиентов) можно признать уместной, так как представитель Банка России, ссылаясь на данные МВД РФ, в своем выступлении на одном из круглых столов, состоявшемся в рамках мероприятия INFOBEZ EXPO'2013, отметил, что в нынешнем году произошли существенные изменения в поведении киберзлоумышленников в кредитно-финансовой среде: они стали смещать фокус атак с клиентской стороны на банковскую.

Одновременно набирающее популярность движение "принеси в офис свое мобильное устройство" (BYOD), как отмечает исполнительный директор InfoWatch Всеволод Иванов, приводит к тому, что ИБ-службам банков все труднее отслеживать и предотвращать инциденты, связанные с утерей персональных данных клиентов, особенно в их привязке к банковской информации. Доступ с широкого спектра пользовательских устройств к банковским данным (если и не на стороне банка, то на стороне клиента) неизбежно ведет к ослаблению контроля над ними.

С распространением мобильных технологий, по мнению Владимира Мамыкина, возросла роль организационной составляющей в обеспечении ИБ, и сегодня необходимо более тщательно обучать сотрудников банков и пользователей систем ДБО правилам работы с информацией, содержащей не только коммерческую тайну, но и персональные данные.

В атаках на ДБО активно используются технологии социальной инженерии, а также внутренние инсайдеры. Поэтому г-н Мамыкин рекомендует вводить в модели угроз финансовых организаций "внутреннего нарушителя", что резко ме-

Наши эксперты

ВСЕВОЛОД ИВАНОВ, *исполнительный директор, InfoWatch*

КИРИЛЛ КЕРЦЕНБАУМ, *руководитель группы предпродажного сопровождения, "Лаборатория Касперского"*

СЕРГЕЙ КОТОВ, *эксперт по информационной безопасности, "Аладдин Р.Д."*

ВЛАДИМИР МАМЫКИН, *директор по информационной безопасности, Microsoft в России*

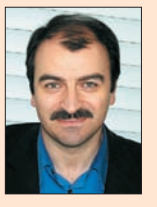
ДЖАБРАИЛ МАТИЕВ, *руководитель отдела информационной безопасности, IBS Platformix*

ВЯЧЕСЛАВ МЕДВЕДЕВ, *старший аналитик отдела развития, "Доктор Веб"*

ЛЕОНИД ПЛЕТНЕВ, *старший аудитор, "Информзащита"*

СЕРГЕЙ СТУПИН, *менеджер по продукту, "ТрастВерс"*

АНДРЕЙ ФИЛИНОВ, *системный архитектор по ИБ, IBM в России и СНГ*



РЕНАТ ЮСУПОВ, *старший вице-президент, Kraftway*

няет ландшафт ИБ в банках и требует изменения общих подходов к обеспечению ИБ, так как использование против такового лишь технических средств защиты, без правильных организационных мер, не может быть эффективным.

По мнению Вячеслава Медведева, старшего аналитика отдела развития компании "Доктор Веб", текущие изменения в ИБ кредитно-финансовых организаций России в наибольшей степени связаны с федеральным законом "О национальной платежной системе". Этот закон, в частности, требует возмещать клиентам финансовые потери, возникшие не по их вине, в том числе и связанные с деятельностью злоумышленников. Мотивированные этими требованиями, банки вынуждены отступать от стратегии здорового консерватизма в ИБ и внедрять системы анализа финансовых операций, усиливать ИБ клиентов.

Вслед за регулятивными г-н Медведев отмечает еще три фактора, стимулирующие развитие ИБ в банках: переход злоумышленников от действий одиночек к деятельности организованных группировок, имеющих в своем распоряжении широкий набор высокотехнологичных средств для проникновения в ИТ-системы практически любого уровня защищенности; глубокое и широкое проникновение Интернета в сферу финансовых услуг и в быт граждан; снижение стоимости используемых злоумышленниками программных и аппаратных средств, что делает возможным атаки любого уровня сложности.

В Банке России считают, что информационный фон вокруг ИБ-инцидентов в банковской сфере, их освещение в СМИ (несмотря на, мягко говоря, неспособствование этому как со стороны жертв, так и со стороны виновников инцидентов) сегодня в состоянии понуждать кредитно-финансовые учреждения информировать об инцидентах других участников банковского бизнеса, мотивировать их заблаговременно принимать адекватные меры противодействия, повышать киберзащищенность своего бизнеса.

ИБ-риски, актуальные для кредитно-финансовых организаций

Как считают наши эксперты, ИБ-риски, с которыми сталкиваются российские кредитно-финансовые организации, не имеют национальной специфики, и в целом ситуация с ИБ в них соответствует положению дел в ИБ финансовых структур за рубежом.

По мнению Леонида Плетнева, финансовые организации в первую очередь волнуют риски, связанные с прямыми денежными потерями. На них они реагируют остро и стараются по возможности быстро и эффективно их минимизировать. Кроме того, отмечает г-н Плетнев, к числу высокоприоритетных менеджмент банков относит риски, связанные с нарушением требований регуляторов. При этом учитываются как потери из-за штрафов и прекращения профессиональной деятельности вследствие нарушений соответствия регулятивным требованиям, так и потери вследствие реализации угроз, на минимизацию которых направлены требования регуляторов по обеспечению ИБ.

Кстати, как отмечает Всеволод Иванов, размер штрафов за несоблюдение требований регуляторов постоянно растет и сопровождается одновременным усилением контроля регулирующих органов за выполнением этих требований (в частности, касающихся хранения и обработки персональных данных и финансовой информации).

К числу актуальных в последние годы для банков Андрей Филинов отнес риски, сопряженные с использованием устаревших элементов и технологий в составе АБС. Средний возраст российских банков, согласно его наблюдениям, составляет 15—20 лет, их АБС создавались в период, когда заказчики предпочитали разрабатывать прикладное ПО своими силами с использованием наиболее доступных средств, что на ту пору было оправданно. Теперь же эти разработки устарели и стали источником повышенных рисков.

Состояние АБС и других используемых в банках информационных систем, по мнению Кирилла Керценбаума, актуализирует вопросы управления технологическими и операционными рисками. И те и другие г-н Керценбаум связывает непосредственно с рисками ИБ. Современная финансовая организация, по его мнению, представляет собой (или должна представлять) по сути бизнес непрерывного цикла, и роль "кровеносной системы" в нем играют информационные технологии. Информационные системы требуют защиты (однако с учетом доступности) как от внешних, так и от внутренних угроз ИБ, что с неизбежностью увеличивает технологические и операционные риски: перестараться с защитой и превратить работу с информационной системой в трудновыполнимую столь же неверно, как и оставить ее защищенной недостаточно, зато с высоким уровнем доступности. Соблюдать баланс, как подчеркивает г-н Керценбаум, весьма сложно, и наиболее подходящий вариант каждая компания находит для себя индивидуально, выбирая между операционными и технологическими рисками.

Наиболее опасные угрозы для банков (как, впрочем, и для любых других структур) Ренат Юсупов, старший вице-президент компании Kraftway, связывает с человеческим фактором — некомпетентностью или злым умыслом персонала. Исходя из этого он рекомендует прежде всего наладить непрерывный контроль за деятельностью сотрудников. Широкое использование ИТ в банковском бизнесе, по его мнению, делает затруднительным обнаружение в потоке автоматически генерируемых данных последствий ошибок или злонамеренных действий, при совершении которых злоумышленники используют многочисленные уязвимости в информационных системах, обусловленные низким качеством программирования и высокой сложностью самих этих систем.

С человеческим фактором Сергей Ступин, менеджер по продукту компании "ТрастВерс", связывает рост внутренних угроз, обусловленных утечками данных. Их актуализацию можно объяснить как увеличением штата сотрудников (т. е. укрупнением российских банков), так и ростом количества обрабатывающих банковскую информацию приложений, а также уже упомянутым их усложнением.

Воровство клиентской информации банковскими работниками, обслуживающими клиентов, согласно наблюдениям Всеволода Иванова, из отдельных неприятных инцидентов превратилось в обыденность для российских кредитно-финансовых организаций. То, что информацию о клиентах сотрудники, которые (от имени компании!) с ними работают, считают своей собственностью, как отмечает Всеволод Иванов, характерно не только для банковского, но и для российского бизнеса в целом. Многие финансовые организации, например, сталкиваются с тем, что накануне истечения сроков действия полисов страхования, кредитных договоров и т. п. их клиентам начинают звонить конкурирующие компании и предлагать оформить полис у них на более выгодных условиях. Это не что иное, как последствия утечек клиентских данных, которые могут неоднократно передаваться из одной организации в другую.

По этой причине к вопросам ИБ все чаще проявляют интерес руководители бизнес-подразделений банков, которые уже не могут игнорировать связанные с подобными инцидентами потери. Помимо прямого ущерба кражи данных о клиентах несут банку еще и репутационные потери, поэтому их PR-службы и службы маркетинга тоже учатся считать ущерб от подобных инцидентов и становятся заказчиками ИБ-средств противодействия им.

К эффективным способам снижения рисков, связанных с утечками данных, г-н Ступин относит грамотное управление правами пользовательского доступа к ИТ-ресурсам и подчеркивает значимость использования специализированных инструментов — систем идентификации и управления доступом (IDM). Он считает, что процессы управления правами доступа становятся все теснее завязанными на бизнес-процессы банков, что требует более гибких средств управления доступом.

Согласно наблюдениям Сергея Котова, все более глубокое проникновение интернет-технологий в банковский сектор неизбежно. Эти технологии удобны как для банков, так и для клиентов. Они набирают популярность, особенно с учетом низкой плотности населения в нашей стране. Как следствие, наиболее актуальные угрозы для банков тоже перемещаются в Интернет.

Из выступлений на недавнем заседании Правительственной комиссии по использованию ИТ для улучшения качества жизни и условий ведения предпринимательской деятельности можно заключить, что у российских банков на просторах нашей страны остается по меньшей мере 50 млн. потенциальных клиентов, обслуживать которых можно только через Интернет. Перспективы Интернета для банковского бизнеса особенно очевидны, если учесть планы Правительства РФ и ведущих операторов связи страны довести в скором времени охват населения Интернетом до 93%.

Не умаляя положительных результатов интернетизации страны, вместе с тем г-н Котов обращает внимание на отсутствие (как в реалиях, так и в планах) ИБ-инфраструктуры в малых населенных пунктах. Для них, считает он, создание такой инфраструктуры дорого, да и люди там мечтают скорее о дороге до ближайшего райцентра, по которой можно было бы проехать в любое время года. Но, может быть, полагает г-н Котов, с Интернетом (который проложить дешевле, чем построить дорогу) и дорога не так часто будет нужна.

По мнению г-на Котова, для нашей страны насущна возможность работы клиентов с банками из недоверенной среды либо (что дороже) создание замкнутой доверенной среды (или вынесение в такую среду хотя бы критичных операций). Для этого, как он считает, потребуются подходящие по стоимости и простоте эксплуатации средства защиты, позволяющие банку и клиенту взаимодействовать удаленно с нужной степенью защищенности; выдавать их клиентам логично вместе с электронной банковской картой. Такие средства, отмечает г-н Котов, уже есть, но производители систем ДБО пока не спешат встраивать их в свои продукты. Причина проста: дополнительные расходы и небыстрая окупаемость.

Однако, на взгляд г-на Котова, у банков нет сегодня выхода, кроме как работать в этом направлении на перспективу. К этому ситуацию подталкивают закон "О негосударственных пенсионных фондах", стремление правительства страны к ограничению наличных расчетов, наработки, связанные с универсальной электронной картой гражданина РФ, ее банковским использованием и неко-

ПРОДОЛЖЕНИЕ НА С. 21 ▸

От IDM к IAG, или Как не промахнуться с выбором решения для управления доступом

СЕРГЕЙ СТУПИН

Любая организация численностью свыше 200 человек, использующая в работе ряд информационных систем, обеспечивающих ее повседневную жизнедеятельность, рано или поздно сталкивается с необходимостью внедрения системы автоматизированного управления учетными записями. Иначе стоимость поддержки информационных систем, а также риски ошибочного предоставления прав к ресурсам компании чрезвычайно высоки. Речь идет об уже известном на отечественном рынке классе решений — IDM (Identity Management).

В 2012 г. аналитическое агентство Gartner в своем отчете выделило еще один класс решений — Identity & Access Governance (IAG). Давайте разберемся, что это за решения и для каких задач они предназначены.

В связи с ростом требований регуляторов к организации управления доступом помимо задачи автоматизации возникла потребность обеспечить контроль доступа к информационным ресурсам.

Управление правами доступа — задача, имеющая отношение не только к вопросам внутренней автоматизации предприятия, но и к его бизнесу, поскольку она напрямую связана с его бизнес-процессами. Для чего нужно управлять правами доступа пользователей к информационным ресурсам? Чтобы предотвратить утечки стратегически важной для компании информации за счет правильного разграничения прав доступа, распределить ответственность за решения о допуске сотрудников к информации, снизить стоимость эксплуатации ресурсов. Это и есть основные бизнес-задачи.

К сожалению, IDM-решения не способны учесть все особенности бизнес-процессов. В любой организации изменения происходят постоянно: сотрудников принимают на работу, увольняют, переводят с должности на должность и из одного отдела в другой; они болеют, уезжают в командировки, исполняют чьи-то обязанности. И каждое такое изменение влечет за собой корректировку прав доступа к информационным ресурсам.

Но управлять правами доступа лишь на основе кадровых изменений, как правило, не достаточно, ведь необходимость в изменении прав сотрудника не всегда связана с кадровыми перемещениями. Отсюда вытекает необходимость иметь в решении инструмент для самостоятельного запроса прав доступа.

Другая не менее важная задача, выходящая за рамки типовой IDM-системы, — аудит текущих прав доступа. До внедрения IDM-решения в организации уже используется множество целевых систем, таких как ERP, CRM и другие. Необходимо определить, у кого какие права уже есть и соответствуют ли они политике информационной безопасности.

Упомянем еще об одной распространенной проблеме. Допустим, в действующей системе настроили ролевую модель и назначили сотрудникам роли в соответствии с их должностными обязанностями. В любой успешной компании регулярно ведется работа по оптимизации бизнес-процессов, а значит, они постоянно меняются. В связи с вышесказанным нередко возникают ситуации, когда реальные обязанности сотрудника уже не соответствуют ранее настроенной ролевой модели. Если эти изменения не отражены вовремя в IDM-системе, у сотрудника могут возникнуть избыточные права, что повышает риск утечки информации, например, составляющей коммерческую тайну. Избежать таких ситуаций — также задача решений класса IAG. Для этого в них должен быть включён специальный инструмент — процедура сертификации доступа, предполагающая, что владельцы ресурсов, руководители и другие ответственные лица регулярно пересматривают права сотрудников на предмет их соответствия реальным обязанностям, политике информационной безопасности и требованиям регуляторов.

Еще один пример того, как бизнес-процессы влияют на функциональность продуктов по управлению правами доступа. Для снижения коммерческих рисков зачастую желательно, чтобы не было ситуаций, когда выполнение определенной задачи полностью зависит только от одного человека. Например, выставление и оплата счетов. Необходим механизм, позволяющий избегать подобных обстоятельств и своевременно выявлять их, если они все-таки возникли. Опять же это задача IAG.

По прогнозу Gartner, к 2016 г. функциональности IDM и IAG сольются, образовав новый класс решений с расширенной аналитикой в управлении доступом.

Из всего вышесказанного можно сделать следующий вывод: в настоящее время разработчики IDM-решений в ответ на потребности рынка меняют привычный подход к управлению доступом. Фокус внимания смещается от автоматизации администрирования к интеллектуальному управлению политикой доступа на основе ролевой модели. Большое внимание уделяется также возможностям аудита и контроля соответствия политики информационной безопасности требованиям регуляторов.

Компания “ТрастВерс” является разработчиком системы КУБ, которая помимо задач IDM закрывает большинство задач полноценного IAG-решения. В ближайших версиях мы планируем развиваться именно в этом направлении. Уже сейчас у нас есть возможность интегрировать КУБ практически в любые бизнес-процессы заказчика и обеспечить решение всех перечисленных выше задач.

Автор статьи — менеджер по продукту компании “ТрастВерс”.

Найти и обезвредить

ВЯЧЕСЛАВ МЕДВЕДЕВ

Тема компьютерных преступлений не сходит с новостных лент информационных агентств. DDoS-атаки, взломы серверов, утечки конфиденциальных данных и денежных средств по вине инсайдеров и вследствие заражения — перечислять можно долго. Но это новости о событиях — новостей о судебных решениях практически нет. В чем причина?

С точки зрения законодательства все необходимое давно имеется. В главе 28 УК РФ “Преступления в сфере компьютерной информации” содержится целых три статьи: ст. 272 “Неправомерный доступ к компьютерной информации”, ст. 273 “Создание, использование и распространение вредоносных компьютерных программ” и ст. 274 “Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей”.

К тому же компьютерные преступления, подпадающие под главу 28 УК РФ, зачастую сопровождаются другими преступлениями: нарушение авторских и смежных прав, мошенничество, изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов, уклонение от уплаты налогов с организаций, нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

То есть осудить можно. Остается вопрос о том, почему преступления не доходят до суда. И первая причина — конфликт интересов на всех уровнях, от руководства компаний до системных администраторов.

Руководство компаний-жертв понимает, что даже сам факт расследования может привлечь нежелательное внимание к компании со стороны и клиентов, и надзорных органов. Особенно это относится к руководителям финансовых и банковских учреждений, которые не хотят, чтобы клиенты сомневались в их надежности. А надзорные органы вполне могут заинтересоваться, почему в организации, отчитавшейся о выполнении всех предъявляемых к ней требований, вдруг произошло такое событие.

Плюс традиционное для нашего общества недоверие к правоохранительным органам: если компания расскажет все о своей структуре безопасности — не утекут ли эти данные? К тому же на переданных на анализ компьютерах могут оказаться не только конфиденциальные данные, но и нелицензионное ПО. Возникает логичное желание решить проблему своими силами, подкрепленное нежеланием выносить сор из избы.

Кто может заняться расследованием в структуре компании? Зачастую только системные администраторы. Но они не могут заниматься расследованием преступлений. Во-первых, из-за вышеупомянутого конфликта интересов. Согласно должностным обязанностям первое, что должен сделать администратор при обнаружении инцидента, — закрыть проблему: донастроить файервол, уничтожить вирус, проникший в локальную сеть, и т. д. Но такие действия несовместимы с действиями по расследованию преступлений.

Все мы смотрели детективы и помним, что происходит во время следствия. Сбор доказательств, изучение документов, следственный эксперимент с участием подозреваемого... Для многих является открытием, что в случае компьютерного преступления все идет тем же порядком.

Во-первых, нужно установить факт преступления. Точнее, нужно выделить среди инцидентов, которые ежедневно разбирают администраторы, факты, указывающие на возможное преступление. Но как отличить случай, когда файлы оказались зашифрованы в результате банального заражения, произошедшего по вине администратора, неверно настроившего систему безопасности, от ситуации, когда это случилось по вине инсайдера?

При подозрениях на вредоносную программу сисадмин должен провести проверку на вирусы, уничтожить найденные подозрительные процессы и т. д. Но с точки зрения расследования он тем самым уничтожит все улики. У всех на слуху прецедент, когда в результате несоблюдения процедуры расследования защита смогла подвергнуть сомнению правомерность использования в качестве доказательств изъятых компьютеров — в ходе исследования на файлах компьютеров изменились даты последнего доступа.

Но в большинстве компаний не используются никакие средства аудита системы и уж тем более средства анализа инцидентов. Как в таком случае выделить подозрительный инцидент из огромного потока событий?

Расследование инцидента безопасности может занимать от нескольких дней до нескольких месяцев. И все это время сотрудник, проводящий расследование, будет оторван от текущей работы, и его обязанности придется перераспределять среди других работников. А если штат мал или вообще в компании только один сисадмин?

Возвращаясь к процедуре расследования, отметим, что доказательства нужно собрать так, чтобы избежать искажения информации, в том числе и в ходе технических экспертиз. Т. е. не рекомендуется выключать компьютер, ставший объектом преступления. Или же выполнять на нем какие-либо операции.

Обнаружение, осмотр и изъятие компьютеров и компьютерной информации в процессе следственных действий могут совершаться при следственном осмотре, при обыске, выемке, воспроизведении обстоятельств и обстановки происшествия — эти процедуры известны правоохранительным органам, но известны ли они специалистам компании?

Однако в полиции, как правило, отсутствуют и необходимые специалисты, и надлежащее — весьма дорогое — оборудование.

Выходом из тупика может стать обращение к специальной организации, имеющей возможность сбора и анализа данных. Так, компания “Доктор Веб” производит экспертизу компьютерных инцидентов против конфиденциальности, целостности и доступности компьютерных данных и систем, для совершения которых использовались вредоносные программы и потенциально опасное ПО.

Комплекс мероприятий, составляющий эту услугу компании “Доктор Веб”, включает в себя оперативное реагирование — выезд специалиста для локализации инцидента и обеспечения сохранности электронных доказательств. Специалист производит процедуру изъятия жесткого диска (НМЖД) с ПК, участвовавшего в инциденте, снимает с него аутентичную криминалистическую копию (образ) и оформляет изъятый НМЖД в качестве вещественного доказательства. Все описанные процедуры выполняются в строгом соответствии с требованиями УПК РФ. Также возможен сбор и анализ дополнительной информации, а также текстовых, звуковых, фото-, видеоматериалов, предположительно имеющих отношение к инциденту.

Автор статьи — ведущий аналитик отдела развития компании “Доктор Веб”.

Информационная...

ПРОДОЛЖЕНИЕ СО С. 19

торые иные аспекты. Часть забот с обеспечением ИБ в этой схеме могут принять на себя операторы мобильной связи (техническая возможность создания такой инфраструктуры доказана).

Факторы, затрудняющие организацию ИБ в кредитно-финансовых структурах

Среди наиболее важных факторов, затрудняющих организацию ИБ в кредитно-финансовых структурах, наши эксперты выделили финансовый, человеческий и технический аспекты, которые тесно переплетаются один с другим.

Так, Леонид Плетнев, усматривая главную проблему в ограниченности ИБ-бюджетов, отмечает, что главная задача руководителя ИБ-службы часто сводится к обоснованию перед руководством необходимости вложений в ИБ в терминах, понятных бизнесу. Например, доказать актуальность системы DLP можно, позиционируя ее не как решение для борьбы с утечками данных, а как инструмент оценки лояльности персонала. На неумение технических специалистов объяснить бизнес-руководству, как уровень защищенности влияет на функционирование бизнес-процессов, в результате чего снижается авторитет ИБ-службы и осложняется ее работа, обращает внимание и Вячеслав Медведев. Он отмечает также недостаточную компетентность банковских ИБ-специалистов, что приводит к ошибкам в оценке рисков и неверному выбору средств защиты, несмотря на доступность информации об уровне современных угроз и наличие адекватных средств защиты. Так, по его наблюдениям, ИБ-специалисты нередко забывают о системах резервного копирования и разграничения и контроля доступа.

Констатируя, что человеческий фактор по-прежнему остается узким местом любой ИБ-системы, Джабраил Матиев, руководитель отдела информационной безопасности компании IBS Platformix, отмечает, что работу банковской ИБ-службы значительно затрудняет отсутствие централизованной комплексной политики повышения осведомленности в области ИБ пользователей финансовых услуг.

С другой стороны, ИБ-службам банков сегодня приходится иметь дело с системами высокой сложности, причем Ренат Юсупов отмечает низкую адаптивность существующих ИБ-средств к новым угрозам. Это позволяет злоумышленникам умело эксплуатировать архитектурные изъяны аппаратуры и программного обеспечения, нередко имеющего низкое качество, а также создавать и продавать универсальные, профессионально разработанные платформы для взломов. По оценкам г-на Юсупова, профессионализм взломщиков сегодня настолько высок, что последствия их проникновения в ИКТ-среду обнаруживаются спустя длительное время. Критические уязвимости, как он подчеркивает, лежат на уровне микропроцессоров, архитектуры, низкоуровневых кодов инициализации систем, где их практически невозможно обнаружить привычными средствами.

Для того чтобы противостоять подобным угрозам, считает г-н Юсупов, средства защиты должны строиться на таких принципах, как превентивность, непрерывность, интеграция средств защиты уже на уровне проектирования "железа" и ПО, адаптируемость к работе против новых угроз, приоритет безопасности над основным функционалом. По его мнению, эти средства уже есть на российском рынке.

Сложность современных ИБ-решений нередко требует от обслуживающих их специалистов высокой ИБ-квалификации и компетенций в смежных специальностях и должностных обязанностях. Это уровень ИБ-директора, а таковых в России сегодня мало. В результате, как отмечает г-н Иванов, на российском рынке появились и так называемые ложные системы: вендор приписывает своему продукту функции, которых в нем нет, а ИБ-специалист оказывается недостаточно компетентен, чтобы распознать обман. По описаниям ложные и полноценные системы выглядят одинаково, но стоят по-разному: не понеся никаких трат на разработку полноценного функционала, поставщик ложной системы получает возможность демпинговать. При прочих равных (на бумаге) качествах заказчик, разумеется, выберет более дешевую. Убедившись в том, что система не решает возложенных задач и не имея достаточной компетенции, чтобы разобраться в истинных причинах этого, заказчик разочаровывается в целом классе решений, что тормозит развитие соответствующего направления ИБ.

Средства и способы защиты, считает Кирилл Керценбаум, должны находиться в постоянном движении вслед за изменением и переоценкой рисков, что требует значительных вложений в ИБ-решения. Однако не каждый бизнес-руководитель понимает эффективность данных вложений, ведь посчитать реальные потери от ИБ-инцидента можно только тогда, когда он в действительности произошел. Поэтому именно ущерб от случившихся ИБ-инцидентов чаще всего становится стимулом выделения средств и внедрения новых ИБ-систем.

Изменить ситуацию поможет формирование в России института ИБ-руководителей (ИБ-директоров), способных донести до бизнес-заказчиков последствия реализации ИБ-угроз как угроз для бизнеса.

ИБ финансового сектора и регуляторы

Согласно результатам упомянутого выше исследования "Информационная безопасность в российских банках", 77% банков страны недовольны деятельностью регуляторов в финансовой области и оценивают ее как чрезмерно суровую, не способствующую реальной защите информации, а только усложняющую ее. При этом 93% респондентов заявили о том, что проверили состояние своей ИБ на соответствие стандарту СТО БР ИББС, но только 16% участников исследования смогли это соответствие подтвердить. При этом у 91% соответствие требованиям регуляторов играет роль движителя реализации ИБ-проектов, и всего лишь в 34% кредитных организаций повышение ИБ рассматривается сегодня как конкурентное преимущество.

Налицо, как констатирует Всеволод Иванов, противостояние "бумажной" безопасности, навязываемой регуляторами, и реальной ИБ, обусловленной требованиями бизнеса как такового. Он считает, что о своей ИБ банки должны думать сами, и главным драйвером в этой области для них должны быть финансовые потери, которых можно избежать с помощью ИБ-решений. При этом г-н Иванов не отрицает полезности некоторых рекомендаций и требований регуляторов и призывает использовать их.

В настоящее время, как считает Леонид Плетнев, финансовые организации в России сконцентрированы на выполнении следующих законов и стандартов:

- стандарт индустрии платежных карт PCI DSS;
- №161-ФЗ "О национальной платежной системе";
- №152-ФЗ "О персональных данных";
- стандарт Банка России СТО БР ИББС-1.0—2010.

Эти документы определяют более восьмисот требований к российским кредитно-финансовым учреждениям. Во избежание лишних затрат руководство должно наладить эффективное управление соответствием требованиям регуляторов. Учет дублирующих требований, снижение затрат на реализацию актуальных требований, контроль непрерывности процессов обеспечения ИБ, успешное прохождение аудитов и проверок в отведенные сроки — вот основные задачи, на которые ориентированы сегодня банки с точки зрения требований регуляторов при обеспечении ИБ.

По мнению Леонида Плетнева, в условиях постоянно меняющегося законодательства, неизвестных сроков выхода нормативных актов, уточняющих законы, коллизий и размытых требований в регулятивных документах руководители некоторых банков занимают выжидательную позицию. Большая же часть финансовых организаций, стремясь к реальной защите бизнеса, следует риск-ориентированной модели обеспечения ИБ. При этом неадекватные, по мнению бизнеса, требования даже крупные финансовые структуры зачастую реализуют формально, с единственной целью избежать штрафных санкций со стороны внешних контролирующих органов.

Отмечая очевидные тенденции к повышению общего уровня ИБ в кредитно-финансовой области и напрямую связывая их с новыми ИБ-требованиями и усилением контроля со стороны регуляторов, Джабраил Матиев одновременно констатирует, что зачастую эти требования не учитывают специфику современных ИТ-инфраструктур и процессов, из-за чего снижается уровень соответствия им, поскольку банки не успевают за регулятивными новациями.

Как считает Ренат Юсупов, нормативная база должна определять только общие принципы построения ИБ, подходы и критерии оценки, а приведение их в соответствие с актуальным уровнем угроз должно оставаться за банками и определяться тем, какие технологии и продукты они выбирают. По его мнению, российская нормативная база сегодня переходит именно на эти принципы, и когда этот переход завершится, можно будет оценить её адекватность ИБ-угрозам и требованиям бизнеса. Он отмечает также, что в настоящее время банковские ассоциации успешно договариваются с государством о комфортных условиях для адаптации своих ИТ- и ИБ-систем к новым требованиям регуляторов.

Влияние нормативных требований на банковский бизнес Кирилл Керценбаум оценивает по большей части положительно, отмечая достаточность и полезность регулирования финансовой сферы в России. Стандарт СТО БР ИББС, по его мнению, является одним из лучших российских отраслевых ИБ-стандартов и включает в себя большое количество прозрачных и своевременных норм, позволяющих наладить в финансовом учреждении высоконадежную и эффективную ИБ-систему как технически, так и организационно. От других стандартов и регулятивных норм СТО БР ИББС выгодно отличает, считает он, постоянная адаптация под самые современные регулятивные требования и угрозы, характерные для отрасли, что позволяет финансовым организациям быть более гибкими и быстро подстраиваться под требования рынка.

Андрей Филинов оценивает регулирование кредитно-финансовой среды в России в целом как достаточное, корректное и адекватное с точки зрения традиционных банковских услуг. Однако, отмечает он, требуется более оперативное развитие нормативной базы ИБ в отношении сервисов платежей, предоставляемых небанковскими структурами, такими как операторы связи, электронные деньги, электронная торговля, сети платежных терминалов.