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

Информационная безопасность ДБО

ВАЛЕРИЙ ВАСИЛЬЕВ

Системы дистанционного банковского обслуживания (ДБО) как инструмент снижения операционных расходов, повышения эффективности и конкурентоспособности бизнеса банков получают все более широкое распространение в нашей стране. В исследовании агентства CNews Ana-lytics, проведенном в прошлом году, отмечается стабильный рост уровня распространенности ДБО: такие системы используют 94% российских банков из ведущей сотни для обслуживания юридических лиц и 83% — для обслуживания физических лиц. Согласно данным Банка России доступом к своим банковским счетам пользуется несколько миллионов физических лиц.

ОБЗОРЫ

Вместе с тем специалисты по информационной безопасности (ИБ) отмечают низкий уровень защищенности ДБО и большое количество уязвимостей в программном обеспечении, используемом в ДБО-системах, несмотря на увеличение доли профессиональных разработок против самописных.

МВД России сообщает, что растут как количество, так и размеры хищений денежных средств индивидуальных и корпоративных вкладчиков, осуществляемых с использованием ДБО. При этом денег у юридических лиц крадётся в тысячи раз больше, чем у физических.

Ситуация, складывающаяся вокруг ДБО, не оставляет сегодня равнодушными никого из его участников и организаторов — ни клиентов, ни банки, ни правоохранительные органы, ни регуляторов, ни специалистов по ИБ.

В данном обзоре мы постарались рассмотреть специфику организации защиты ДБО, возникающие при этом проблемы и возможные пути их решения с учетом необходимости выполнять нормативные требования к обеспечению безопасности банковских транзакций.

Критерии защищенности систем ДБО

В организации защиты системы ДБО опрошенные нами эксперты рекомендуют исходить прежде всего из экономической целесообразности, т. е. чтобы защита не была дороже защищаемых ресурсов. Хотя есть и более радикальные мнения. Так, Андрей Голов, генеральный директор компании "Код Безопасности", полагает, что критерий защищенности ДБО может быть только один: злоумышленник не должен найти способ совершить хищение денежных средств. Джабраил Матиев, руководитель группы информационной безопасности компании IBS Platformix, также настаивает на том, что необходимо не дать злоумышленнику возможность получить управление чужим банковским счетом, при этом неважно, каким образом это достигается.

Эксперты обращают внимание на то, что средства защиты ДБО не должны доставлять больших неудобств пользователям системы, в первую очередь ее клиентам. В противном случае они просто будут пренебрегать защитой и применять ДБО с нарушением требований к ИБ.

В организации ИБ систем ДБО Алексей Сизов, руководитель группы противодействия мошенничеству Центра информационной безопасности компании "Инфосистемы Джет", рекомендует руководствоваться базовыми критериями защищенности информации: обеспечением конфиденциальности, целостности и аутентичности. При этом целостность информации, как он считает, следует рассматривать не только в отношении платежных поручений, но и применительно к операциям проведения платежа. Аутентичность платежного поручения должна рассматриваться для каждой операции с учетом того, в каком отношении к документу состоит пользователь сервиса ДБО.

Для определения специфических критериев защищенности систем ДБО Евгений Афонин, начальник отдела системной архитектуры компании "Информзащита", предлагает обратиться к документу "Критерии защищенности вычислительных систем ФСТЭК: Автоматизированные системы. Защита от НСД". По его мнению, сформулированные в этом документе положения могут быть успешно применены к системам ДБО. Из основных характеристик защиты ДБО г-н Афонин обращает особое внимание на универсальность мер и средств защиты вне зависимости от методов атак, на возможность адаптации системы защиты в соответствии с изменениями технологий ДБО и бизнес-процессов кредитной организации, а также на способность предотвращать нарушения ИБ автоматически.

Готовым к практическому использованию руководством по обеспечению ИБ в системах ДБО выглядит перечень ключевых критериев защищённости, представленный Сергеем Котовым, экспертом по информационной безопасности компании "Аладдин Р.Д.":

— удобный, интуитивно понятный пользовательский интерфейс;

— доступное и внятное руководство пользователя;

— наличие способов идентификации, альтернативных логин-парольной;

— возможность использования средств аутентификации по выбору клиента (с учётом ограничений, устанавливаемых банком);

— возможность выбора правил и средств доступа к системе;

— промышленная (не "самописная") система ДБО;

— наличие у системы сертификатов регуляторов.

ИБ-риски, специфичные для ДБО

Риски, связанные с использованием ДБО, эксперты разделяют на те, которые возникают на стороне клиента, и те, что характерны для финансово-кредитных организаций. При этом Сергей Котов подчеркивает, что такие риски специфическими считать не следует, поскольку они актуальны не только для области ДБО.

Для клиентов ДБО характерны кражи и потери средств, применяемых для идентификации пользователей (в том числе ключей формирования электронных подписей платежных поручений), перехват управления вычислительными ресурсами как стационарных, так и мобильных устройств, применяемых для работы с сервисами ДБО, заражение их вредоносными программами, позволяющими нарушать целостность последовательности действий при формировании платежных поручений. Эксперты указывают на то, что ситуация с обеспечением безопасности использования систем ДБО на стороне клиентов усложняется их низкой ИБ-культурой.

На стороне кредитно-финансовых организаций эксперты отмечают недостаточный контроль используемых бизнес-процессов, низкую эффективность взаимодействия банков между собой и с правоохранительными органами, уязвимости в базовом ПО систем ДБО, злонамеренный инсайд со стороны банковских сотрудников, включая администраторов бизнес-приложений и инфраструктуры.

К наиболее сложным и опасным на сегодняшний день атакам на ДБО Андрей Голов относит те, в результате которых происходит подмена платежных документов на этапе их подписания. Во время такой атаки пользователь видит и подписывает один документ, а в банк уходит подложный. Как сообщает г-н Голов, вредоносные программы, лежащие в основе организации таких атак, хакерами разработаны практически для всех наиболее распространенных систем ДБО, а ущерб от этого типа атак сегодня исчисляется десятками миллионов рублей.

Факторы, затрудняющие защиту ДБО

Защита ДБО является задачей комплексной и должна реализовываться как на стороне кредитно-финансовой организации, так и на стороне клиента. И если, как отмечает генеральный директор компании "ДиалогНаука" Виктор Сердюк, на своей стороне провайдер услуг ДБО в состоянии обеспечить желаемый уровень защиты в полном объеме, то на клиентской стороне он может только рекомендовать использовать те или иные механизмы безопасности, ответственность за реализацию которых ложится на клиента.

По наблюдениям г-на Сердюка, большинство успешных атак на системы ДБО проводится через плохо защищенные клиентские места, на которых не выполняются даже базовые требования по защите информации. Он полагает, что отсутствие должного внимания к проблеме защиты информации со стороны клиентов ДБО является одним из основных факторов, затрудняющих эффективную защиту систем ДБО.

В ДБО, как в зеркале, отражаются общие для сервисной модели потребления ИТ проблемы обеспечения ИБ, а именно невозможность для провайдера реализовать и гарантировать требуемую безопасность на стороне клиента, а для клиента — организовать адекватный контроль за качеством услуги (включая ее безопасность) на стороне провайдера. Первый фактор для ДБО играет сегодня более значимую роль, и поэтому клиенты, по мнению экспертов, остаются наиболее уязвимым звеном в обеспечении безопасности ДБО. Второй фактор в основном связан с доступностью сервиса, и возникающие в этой связи проблемы могут быть разрешены сменой ДБО-провайдера.

К факторам, затрудняющим обеспечение ИБ систем ДБО, эксперты относят также высокие требования со стороны клиентов к удобству эксплуатации таких систем. Процедуры получения ключей электронной подписи, их применения, разбор конфликтных ситуаций и т. п. не должны быть сильно обременительными для пользователей.

Использование средств защиты ДБО затрудняется также длительным процессом внедрения, что связано с большой и распределенной клиентской ба-

ПРОДОЛЖЕНИЕ НА С. 17 ▶

Наши эксперты

ЕВГЕНИЙ АФОНИН, *начальник отдела системной архитектуры, "Информзащита"*

АНДРЕЙ ГОЛОВ, *генеральный директор, "Код Безопасности"*

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

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

ВИКТОР СЕРДЮК, *генеральный директор, "ДиалогНаука"*

АЛЕКСЕЙ СИЗОВ, *руководитель группы противодействия мошенничеству Центра информационной безопасности, "Инфосистемы Джет"*

IDM в России. Спрос, предложения, перспективы

В последние два-три года рынок систем управления идентификационными данными (IDM) растет в России в геометрической прогрессии. Это обусловлено целым рядом факторов: увеличением количества используемых в организациях разнородных информационных систем, повышением рисков в связи с многообразием способов распространения информации, переводом бумажного документооборота в электронный и др. Сегодня профессиональное решение для управления доступом необходимо практически любому предприятию с высоким уровнем автоматизации и большим количеством ежедневных кадровых операций. О назначении IDM-решений и о перспективах этого рынка рассказывает руководитель отдела маркетинга компании "ТрастВерс" ***Татьяна Малявина****.*

Татьяна Малявина

Какие задачи решают типовые IDM-системы?

IDM-системы предназначены для автоматизации управления доступом пользователей к информационным ресурсам компании, то есть позволяют создавать, удалять и изменять учетные записи сотрудников в информационных системах в зависимости от кадровых изменений, таких как прием на работу, увольнение, повышение в должности, отпуск, больничный и прочее.

Что ждут руководители отделов ИТ и ИБ от IDM-систем?

В первую очередь — автоматизации. При большом количестве сотрудников в компании ИТ-служба ежедневно завалена заявками, требующими открыть, закрыть или скорректировать доступ сотрудников к информационным ресурсам. При этом для многих компаний ошибочно предоставленные права могут иметь фатальные последствия и привести к утечкам конфиденциальной информации. Как снизить риски таких ошибок? Автоматизировать весь процесс управления правами доступа на основе кадровых изменений путем синхронизации системы кадрового учета и IDM-решения.

Почему IDM-решения часто становятся причиной конфликтов между ИТ- и ИБ-службами компаний?

IDM-решения — это инструмент сотрудников отделов автоматизации. Обычно бизнес-пользователи торопят технических специалистов и настаивают на немедленном предоставлении необходимых для работы прав. И те нередко идут им навстречу, порой нарушая политику информационной безопасности компании. Службы ИБ часто тормозят процесс и вводят довольно сложные, а иногда и избыточные схемы согласования, ведь ответственность за информационную безопасность лежит на них. В IDM-системах процедура контроля доступа реализована как возможность сверки по расписанию. При таком подходе высоки шансы, что неправомерные действия сотрудников будут обнаружены с задержкой или же не будут обнаружены вообще. Запросы, проведенные через IDM в обход процесса согласования, не считаются несанкционированными и никак не фиксируются. Поэтому важно не только обеспечить непрерывный контроль доступа, но и хранить полную историю всех изменений, чтобы при возникновении инцидента иметь возможность оперативно его расследовать.

Как эти вопросы решаются в системе комплексного управления безопасностью (КУБ), разработчиком которой является компания "ТрастВерс"?

КУБ позволяет обеспечить не только процесс согласования и управления правами доступа, но и непрерывный мониторинг их изменений. Система контролирует соблюдение политики ИБ и выявляет несанкционированные изменения настроек информационных систем в режиме реального времени. Эта возможность заложена на уровне архитектуры продукта. Кроме того, система хранит полную историю всех изменений прав доступа, и это решает проблему расследования возникших инцидентов, связанных с информационной безопасностью. Если предприятие имеет географически распределенную структуру, всегда возникает проблема управления сетевым доступом. В КУБ реализована и эта возможность.

А что КУБ дает "айтишникам"? Нет ли у системы перекоса в сторону безопасности?

Одним из результатов внедрения КУБ является формализация политики информационной безопасности. Когда в компании четко выделены зоны ответственности сотрудников за деятельность, связанную с обеспечением ИБ, и действует понятный механизм, определяющий порядок согласования заявок на доступ, учитывающий статусы и роли сотрудников, а также их доступность, у исполнителя гораздо меньше шансов ошибиться. Кроме того, при внедрении КУБ есть возможность полностью автоматизировать процесс выполнения заявок на доступ и таким образом минимизировать риски, связанные с человеческим фактором, и трудозатраты на создание/удаление учетных записей и корректировку прав.

Каково, на ваш взгляд, будущее IDM-систем?

Наши эксперты внимательно изучают тенденции западного и отечественного рынка IDM, который хотя и с небольшой задержкой, движется в том же направлении. В последние пару лет на рынке выделились следующие потребности: необходимость перехода к управлению учетными данными и доступом на основе бизнес-ролей; расширение ареала управляемых данных; развитие возможностей по анализу процесса управления учетными данными и доступом и прогнозирования рисков; реальное обеспечение безопасности и соответствия требованиям регуляторов.

IDM-решения позволяют управлять учетными записями сотрудников, но в них невозможно учесть бизнес-логику компании. Скорее всего, в ближайшем будущем IDM будет обрастать функционалом для создания политики доступа к информационным ресурсам, реализации ролевой модели доступа через бизнес-роли сотрудников, а также для управления жизненным циклом этих ролей. Мы хотим, чтобы наш КУБ соответствовал требованиям рынка и будем развивать его в сторону обозначенных выше направлений.

Почему вы позиционируете КУБ как IDM-решение нового поколения?

Если резюмировать сказанное, то на сегодняшний день КУБ является единственным на отечественном рынке решением, охватывающим сразу три класса задач: автоматизация, безопасность и управление. На этапе проектирования КУБ задумывался как средство обеспечения информационной безопасности компании, поэтому решение задач безопасности помимо функционала типовой IDM заложено в системе уже на уровне архитектуры. Дополнительно в КУБ реализована такая функциональность, как управление цифровыми сертификатами, программно-аппаратными конфигурациями, сетевым доступом и средствами защиты информации.

СПЕЦПРОЕКТ КОМПАНИИ "ТРАСТВЕРС"

Обзор средств защиты систем дистанционного банковского обслуживания

МАКСИМ ГЛАДКОВ, ВЕДУЩИЙ МЕНЕДЖЕР ОТДЕЛА РАЗВИТИЯ ПРОДУКТОВ КОМПАНИИ "КОД БЕЗОПАСНОСТИ"

Последние 10 лет мы наблюдаем бурное развитие систем дистанционного банковского обслуживания (ДБО). Количество финансовых операций, осуществляемых через такие системы, неуклонно растёт, вследствие чего они попали под пристальное внимание финансовых мошенников.

На сегодняшний день более половины преступлений в кредитно-финансовой сфере приходится на мошенничество в сфере ДБО. По неофициальным оценкам экспертов, оборот российского криминального бизнеса в системах ДБО составляет 500 млн. долл. в год. Объём преступлений в системах ДБО ежегодно возрастает в 2—4 раза. Каждый день в нашей стране происходит 15—20 попыток хищения денежных средств через системы ДБО. Средняя сумма хищения — 400 тыс. руб.

Предоставляя удобный сервис для клиентов, системы ДБО также привели к созданию среды, в которой мошенники осуществляют передачу похищенных денежных средств и в которой обнаружить их гораздо сложнее.

Помимо растущего числа хакерских атак на системы ДБО банковское сообщество испытывает давление и со стороны законодательства. Смысл закона № 161-ФЗ "О национальной платёжной системе" можно выразить одной фразой: во всех случаях хищения денежных средств со счёта клиента банк обязан возместить полную их сумму. Несложно предугадать, что введение данного закона спровоцирует небывалое количество исков о возврате средств со стороны клиентов банка, пострадавших от мошеннических операций в системах ДБО.

В связи с этим банки будут вынуждены снижать риски такого ущерба следующими методами:

- страхование;
- возмещение ущерба от риска, включая выплату штрафа и списание похищенных средств;
- организация защиты, в том числе усиление информационной безопасности;
- перекладывание рисков на клиента, например повышение комиссий и процентов по банковским операциям.

Однако полностью исключить ущерб невозможно, потери у банков и клиентов все равно будут. И объем таких потерь будет только расти.

Сократить подобные риски, угрожающие и банку, и его клиентам, позволит усиление информационной безопасности, которая в зависимости от угроз включает в себя:

- создание доверенной среды на стороне клиента;
- выстраивание процессов противодействия фроду;
- мониторинг транзакций;
- защиту удалённого доступа и т. д.

Теоретически только первый способ может исключить все известные нам виды электронного мошенничества. Все остальные меры снижают вероятность хищения, но не могут предотвратить мошенничество полностью.

Злоумышленники могут применять такие виды атак:

- хищение криптографических ключей;
- "Man in the Middle" (MITM);
- "Man in the Browser", которая является подмножеством MITM-атаки.

До сих пор применяемые на клиентских рабочих местах криптографические токены со встроенным СКЗИ и хранилищем ключевой информации (например, eToken-ГОСТ и Rutoken-ЭЦП) не вполне эффективны, так как могут предотвратить только хищение криптографических ключей. Они не предотвращают атаку MITM, сводящуюся к тому, что злоумышленник получает возможность читать и видоизменять сообщения, которыми обмениваются клиент и банк, причём ни один ни другой догадаться о присутствии мошенника не могут.

Такие атаки можно предотвратить, если вынести функции визуализации документа и формирования ЭП документа в отдельную доверенную среду, которую нельзя атаковать из агрессивной среды, где формируется документ. Под агрессивной средой мы понимаем операционную систему с выходом в Интернет, например Windows 7, в которой работает клиент.

Сегодня существуют следующие программно-технические решения, позволяющие обеспечить защиту от всех известных электронных видов атак:

- TrustScreen (криптографические токены второго поколения, токены с дисплеем). Они обеспечивают визуализацию подписываемых документов в доверенной среде, формирование ЭП и неизвлекаемое хранение ключа подписи. Примером могут служить устройства Rutoken PINPad и считыватель смарт-карт SafeTouch;
- MAC-токены, формирующие код подтверждения документа во внешнем по отношению к компьютеру устройстве. Способы ввода полей документа в MAC-токен — ручной с клавиатуры токена, оптический (фотоэлементы), акустический (динамик "бипер" компьютера), проводной (USB). К таким устройствам относятся, например, ActivIdentity Token V2, биометрическая идентификационная AGSES-карта, Vasco DP 835A;
- SIM-карты с "вшитой" электронной подписью. Помимо ЭП SIM-карта может принудительно отображать своё меню на любом мобильном устройстве, что не даст зловредному ПО похитить PIN или помешать доверенному отображению. На данный момент такие SIM-карты не имеют криптографии по ГОСТ и соответственно не сертифицированы по российским стандартам безопасности;
- "ОС в кармане". Загрузка доверенной ОС с USB-токена. Загружаемая ОС не подвержена изменениям, так как каждый раз запускается с Read-Only-носителя. Технология обеспечивает доверенную среду внутри всей ОС. Формирование ЭП и неизвлекаемое хранение ключей происходит на USB-токене. Примером может служить ПАК СОДС "МАРШ!". Однако существует опасность атаки на такую ОС в момент, когда она загружена и работает;
- технология Jinn — инновационная разработка российского вендора, компании "Код Безопасности". По функциям напоминает TrustScreen, но в качестве устройства формирования ЭП и доверенной визуализации используется изолированный от ОС процессор. Отображение происходит на мониторе клиента при монопольном использовании видеокарты компьютера. Таким образом, в рамках одного физического компьютера создаются два полностью независимых вычислительных комплекса — один для ОС пользователя, второй для доверенной среды. Соответственно для применения этой технологии требуется как минимум двухъядерный процессор.

Все описанные выше решения позволяют осуществлять безопасные платежи, гарантированно защищённые от любых известных на данный момент способов электронного мошенничества, кроме прямой, случайной или совершённой по неосторожности передачи злоумышленникам паролей, ключей, токенов и т. д. Выбрать средство защиты для системы ДБО можно исходя из двух критериев: насколько сложно встроить решение в систему ДБО и какое средство защиты представляется более удобным (при этом вопрос юзабилити чаще всего зависит от личного мнения принимающего решение, а не от объективных показателей).

СПЕЦПРОЕКТ КОМПАНИИ "КОД БЕЗОПАСНОСТИ"

Безопасность ДБО: максимальный результат при минимальных затратах

АЛЕКСЕЙ СИЗОВ, РУКОВОДИТЕЛЬ ГРУППЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ КОМПАНИИ "ИНФОСИСТЕМЫ ДЖЕТ"

Защита сервисов дистанционного банковского обслуживания (ДБО) от мошенничества превратилась в одну из важнейших задач кредитно-финансовых организаций. Это обусловлено двумя причинами. Во-первых, высоким уровнем мошенничества: статистика показывает, что его размеры могут достигать 5—10 млрд. руб. в год (и это показатели ДБО только юридических лиц). Во-вторых, ожидаемым вступлением в силу закона № 161-ФЗ "О национальной платежной системе", возлагающего всю ответственность за факты совершения неправомерных операций на кредитно-финансовые компании. Далеко не все банки отмечают высокий уровень потерь со счетов своих клиентов. Однако в настоящее время наблюдается очевидная зависимость: чем крупнее банк, тем чаще он подвергается атакам. В данном случае имеется в виду не только общее количество попыток хищения, но и средняя статистика по каждому клиенту.

От оценки рисков к прогнозируемой защищенности ДБО

Не следует надеяться, что хакер, не сумевший подобрать "отмычку к самой дорогой двери", откажется от своих преступных намерений. Как только одни банки повышают уровень защищенности своих систем, мошенники обращают свои взоры на тех, кто этой задачей еще не озаботился. Поэтому основным критерием, определяющим необходимость повышения уровня защищенности сервисов ДБО, является оценка текущих и прогнозируемых рисков совершения мошеннических действий. Необходимость внедрения новых механизмов защиты становится очевидной, когда оценка таких рисков высока. Если же текущие риски оцениваются как невысокие, нужно использовать различные модели прогнозирования.

Оценка таких рисков не всегда является сложной задачей. Допустим, с 1 января 2014 г. вступают в силу все положения № 161-ФЗ в той редакции, что зафиксирована на данный момент. В этом случае риски будет нести банк. Объемы денежных средств, размещаемые на банковских счетах, к примеру, юридических лиц редко оказываются менее 1 млн. руб. Следовательно, результатом 10—20 успешных атак станет прямой убыток банка в размере около 1 млн. долл.

Описанный пример наглядно иллюстрирует необходимость повышения защищенности сервисов ДБО. Это комплексная задача, требующая применения решений, которые можно разделить на два сегмента. К первому относят механизмы защиты на стороне клиента (от токенов до модных сейчас средств обеспечения целостности среды), а ко второму — создание независимых инструментов контроля, не зависящих напрямую от клиента или его желания соблюдать "лучшие практики" в сфере ИБ. К таковым относятся различные системы fraud-мониторинга.

Внедрение любого из приведенных средств должно осуществляться исходя из прогнозируемого повышения защищенности каналов ДБО после внедрения. Его определяют на основании показателя, демонстрирующего изменение вероятности успешной реализации атаки.

Практика: три шага к снижению рисков мошенничества

Для обеспечения достаточного уровня защищенности на стороне клиента недостаточно только внедрения новых технологий. Нужно контролировать, насколько клиенты банка соблюдают требования к выполнению комплексных мер по использованию и администрированию этих средств, что сложно реализуемо. Это значит, что система fraud-мониторинга является если не достаточным условием повышения защищенности каналов ДБО, то уж точно необходимым. Её использование должно максимизировать уровень защиты клиентов и их финансовых активов при одновременной минимизации убытков и затрат на внедрение.

Решение этой задачи можно разбить на несколько шагов. Во-первых, необходимо определить канал обслуживания клиентов, наиболее подверженный мошенничеству. Для одних организаций это ДБО юридических лиц, для других — интернет-банкинг физических лиц, для третьих — процессинг пластиковых карт. Наиболее приоритетное направление определяется на основе совокупных данных о развитости того или иного сервиса, о его доле во всей операционной деятельности банка, об ограничениях на использование и о практике претензионных обращений клиентов.

На втором этапе среди общей массы клиентов выделяют наиболее высокорисковые группы. Все клиенты разные: одни заботятся о безопасности, другие не очень или не всегда, третьи обладают большими остатками на расчетных счетах, четвертые дифференцируют средства между различными банковскими продуктами. Группы наибольшего риска выделяются на основании как формальной оценки (по остатку на счете), так и статистики зафиксированных обращений клиентов по фактам мошенничества. А выявление наиболее характерных признаков (возраст, положение в обществе, сфера занятости или вид бизнеса и пр.) позволит эффективно строить карты риска для всей клиентской базы. Практика внедрения решений в крупнейших банках России показывает, что источником 90% всех рисков для крупных и средних банков является 25—30% клиентской базы. Поэтому внедрение системы fraud-мониторинга не всегда должно быть "атакой по всем фронтам" зафиксированного мошенничества, часто оно является поступательным движением минимизации рисков "от большого к меньшему" и "от хорошего к лучшему".

Третий шаг — внедрение решения fraud-мониторинга. По нашим оценкам, на это требуется в среднем не менее шести месяцев. Необходимо помнить, что если такое решение не внедрялось вообще, поскольку на текущий момент риски минимальны, то в случае резкого роста этих рисков их нельзя будет быстро компенсировать. Если же полнофункциональное решение внедрено у ограниченной группы пользователей (в группе высокого риска), то его можно масштабировать в кратчайшие сроки. Фактически это превращается в уже достаточно проработанный проект по модернизации системы, требующий существенно меньше времени.

***

Системы fraud-мониторинга — продукты комплексного внедрения, имеющие ощутимую стоимость и требующие достаточного количества ресурсов (как временных, так и человеческих). Их необходимость и высокая эффективность доказываются практикой использования в ведущих мировых и российских банках. Основные показатели успешности проекта — окупаемость решения или значительное снижение рисков мошенничества — могут достигаться и при поэтапном развитии проекта по внедрению системы fraud-мониторинга. При этом становится возможно получить максимальные результаты за минимальные деньги и в кратчайшие сроки.

СПЕЦПРОЕКТ КОМПАНИИ "ИНФОСИСТЕМЫ ДЖЕТ"

Информационная...

◀ ПРОДОЛЖЕНИЕ СО С. 14

зой ДБО-систем. Внедрение системы защиты может приводить к значительной модификации самих систем ДБО в целом. К управлению системами ДБО пока привлекают в основном специалистов службы ИТ, игнорируя ИБ-службу, что также не способствует безопасности ДБО-услуг.

Виктор Сердюк полагает, что для эффективного противодействия атакам на системы ДБО помимо использования современных средств и методов защиты необходимо налаживать более тесное взаимодействие между банками, правоохранительными органами, регуляторами, а также компаниями, работающими на рынке защиты информации. В настоящее время эта задача, по его наблюдениям, решается путем создания специализированных профессиональных ассоциаций и рабочих групп, в рамках которых обсуждаются проблемы защиты систем ДБО и возможные пути их решения.

Поскольку конкуренция на рынке услуг ДБО ощущается уже весьма остро, стоимость для клиента защиты как дополнительного сервиса не должна быть высокой. В противном случае повышается срок самоокупаемости ДБО-систем, что не стимулирует банки рассматривать ИБ как конкурентное преимущество в сфере услуг ДБО.

ИБ-методы и ИБ-продукты для защиты ДБО

Согласно наблюдениям Виктора Сердюка, на ИБ-рынке имеется достаточно широкий спектр решений, которые позволяют обеспечить эффективную защиту систем ДБО. Наряду с традиционными межсетевыми экранами, антивирусами, системами обнаружения атак и т. п. есть и специализированные продукты, к которым он относит инструменты усиленной аутентификации, системы мониторинга банковских транзакций с целью выявления мошенничества, а также средства создания доверенной среды ДБО. Кроме этого он отмечает, что некоторые российские компании, работающие на рынке ИБ, начали предоставлять консалтинговые услуги по проведению аудита информационной безопасности ДБО-систем. В рамках такого аудита проверяется устойчивость системы к возможным атакам злоумышленников, а по результатам формируется отчет с описанием выявленных уязвимостей и рекомендациями по их устранению.

По мнению Сергея Котова, была, есть и будет необходимость в разработке и использовании принципиально новых методов и продуктов для обеспечения безопасности ДБО, которые должны следовать за развитием сервисов ДБО и технологий, используемых киберпреступниками. Разработчикам систем ДБО и ДБО-провайдерам он рекомендует уделять внимание не только функциональности систем, но и безопасности их использования. На первый план в защите ДБО должно, как он считает, в скором времени выдвинуться страхование ИБ-рисков кредитно-финансовыми учреждениями (но не клиентами).

На взгляд Евгения Афонина, инструменты, необходимые для обеспечения защиты ДБО, уже придуманы, и задача заключается в том, чтобы их правильно использовать. Большей эффективности, утверждает он, можно добиться за счет риск-аналитического подхода, если положить его в основу управления информационной безопасностью ДБО. Повысить уровень защиты систем ДБО, по его мнению, можно, применяя поведенческий анализ действий пользователей и профилирование выполняемых ими транзакций.

Как полагает Алексей Сизов, в краткосрочной перспективе для защиты ДБО нужно сосредоточиться на средствах защиты клиентской среды. К ним он относит механизмы интеллектуального реагирования на факты мошенничества и инструменты усиленной аутентификации пользователей, подтверждающие легитимность операций ДБО. В настоящее время на стороне ДБО-провайдера для этого используют как специализированные системы антифрода, так и настройки на отработку событий, связанных с мошенничеством, системы управления информационной безопасностью (СУИБ).

В среднесрочной перспективе, по мнению г-на Сизова, внимание будут уделять механизмам защиты и контроля программного обеспечения систем ДБО, а также контролю действий обслуживающего персонала (сотрудников банков, аутсорсинговых компаний и т. д.).

Андрей Голов наиболее эффективным подходом к обеспечению безопасности ДБО считает внедрение защиты внутри самой ДБО-системы. На его взгляд важно, чтобы используемые средства криптозащиты ДБО и критичные части самой системы ДБО функционировали в единой защищённой среде. Однако если обеспечивать неизвлекаемость ключевой информации в каком-либо отдельном носителе, то необходимо, чтобы и криптографические операции тоже выполнялись в этом носителе, и визуализация информации защищаемых процессов была реализована на нём же. При пакетной обработке транзакций, когда невозможно выполнить ее визуализацию, г-н Голов рекомендует использовать такие приемы, как "белый список" надёжных получателей, управление рисками выполнения операций и т. п.

По мнению г-на Голова, подходы к обеспечению ИБ в системах ДБО нужно пересматривать, двигаясь в двух направлениях. Во-первых, часть системы банк — клиент следует поместить в доверенную среду, которая реализуется вне операционной системы на защищенном внешнем носителе. Это должно обеспечить целостность и неизменность платежных документов во время их подписания.

Подобный подход может упереться в стоимость решения. Банк, по оценкам г-на Голова, готов потратить на защиту одного клиентского средства доступа к системе ДБО не более ста долларов. Это заставляет ИБ-разработчиков идти на компромиссы, в частности применять решения класса Trusted Screen, представляющие собой аппаратные устройства размером с ладонь с сенсорным экраном, в доверенной среде которых подписывается документ и отображаются платежные данные. К недостаткам этого подхода Андрей Голов относит необходимость применять дополнительное устройство, а также дорогие токены и смарт-карты со встроенной криптографией.

Второй компромиссный вариант защиты платежных документов от фальсификаций, рассматриваемый г-ном Головым, представляет собой тонкий или доверенный клиент, разворачиваемый на клиентском компьютере в виде виртуальной машины, на которой создается доверенная среда для просмотра и подписи платежных документов. Такое решение не требует дополнительных устройств, кроме доверенного носителя. Однако пользователь, работая с системой ДБО в такой среде, сильно ограничен, так как система "не видит" ресурсов рабочей стации и не может с ними работать.

По словам г-на Голова, совмещение упомянутых выше двух подходов позволяет обойти их недостатки. Суть такого совмещения заключается в том, что до загрузки вычислительной системы клиентского рабочего места некоторые ее ресурсы (одно ядро процессора, часть памяти и ресурсов видеокарты и т. д.) занимается микрокодом доверенной среды и пользовательскими ключами. После выполнения этой процедуры стартует загрузка операционной системы компьютера, которая теперь "не видит" "изъятых" у нее ресурсов и не может к ним обращаться. Благодаря этому никакие вредоносные программы не в состоянии перехватить критические данные, которые загружены в сформированную таким способом доверенную среду.

Когда в системе ДБО проводится банковская транзакция, внедренный микрокод переключает компьютер в доверенную среду, отображает документ на экране компьютера, затем формирует электронную подпись и возвращает управление операционной системе. Как подчеркивает Андрей Голов, предлагаемая технология отличается надежностью, низкой стоимостью, не требует дополнительных устройств для совершения операций и визуализации.

Регулирование ДБО

Самым значимым в области регулирования ДБО в России является принятый 27 июня 2011 г. федеральный закон № 161-ФЗ "О национальной платежной системе". Его появление, как считает Джабраил Матиев, свидетельствует о серьезных намерениях нашего государства в регулировании функционирования платежных систем, и одним из результатов создания национальной платежной системы станет повышение общей защищенности систем ДБО. Андрей Голов подчеркивает, что разработка и корректировка закона проходит в тесном контакте госрегуляторов, производителей средств ИБ и специалистов служб безопасности банков.

Однако Алексей Сизов оценивает состояние регулирования и контроля исполнения требований регуляторов в сфере ДБО нашей страны как зачаточное. По его мнению, выдвинутые в законе "О национальной платежной системе" требования являются необходимыми для регулирования обращения платежей в стране. Вместе с тем закон получил ряд серьезных замечаний со стороны банковского сообщества, которые повлекли за собой необходимость его корректировки и уточнений. В результате госрегуляторами принято решение на год (до января 2014-го) отсрочить вступление в силу девятой статьи закона, определяющей порядок возмещения клиентам денежных средств, которые были задействованы в банковских операциях, совершенных с использованием электронных средств и без согласия клиента, в том числе через системы ДБО.

По мнению Виктора Сердюка, с развитием российской регулятивной базы будет усугубляться ответственность кредитно-финансовых организаций за возможные финансовые потери их клиентов, связанные в том числе с атаками на системы ДБО (и отложенная на год статья рано или поздно начнёт работать), и усилятся требования к защите информации в кредитно-финансовых компаниях, в том числе в отношении систем ДБО. Так, Банк России уже ведет разработку специализированных нормативных документов по информационной защите, среди которых можно назвать стандарт Банка Росси СТО БР ИББС и Положение Банка России 382-П от 9 июня 2012 г. о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке контроля со стороны Банка России за соблюдением этих требований.