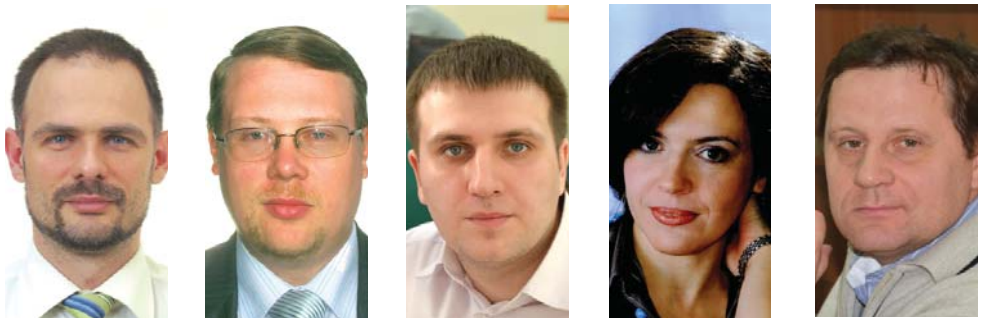
Безопасность электронных финансовых услуг: что нового?

По мере развития рынка электронный финансовых услуг растёт проблема кибермошенничества, преступники становятся все более интеллектуальными, а это значит, что тема обеспечения безопасности сферы электронных денег и платежей нуждается в инновациях. О том, так ли это, и что нового происходит в этой сфере бизнеса мы беседуем с экспертами и участниками рынка Андреем Рябовым, исследователем Научно-исследовательского отдела ЗАО «ОКБ САПР», Дмитрием Романченко, Директором центра технологий безопасности компании IBS, Павлом Головлевым, Начальником управления безопасности Информационных технологий ОАО «СМП Банк», Аленой Зуевой, начальником отдела информационной безопасности и Сергеем Марголиным, коммерческим Директором ООО «Информационные системы».



Павел Головлев, начальник управления безопасности СМП банка • Дмитрий Романченко, директор центра технологий безопасности компании IBS. • Андрей Рябов, исследователь Научно-исследовательского отдела ЗАО «ОКБ САПР» • Алена Зуева, начальник отдела информационной безопасности ООО «Информационные системы» • Сергей Марголин, коммерческий Директор ООО «Информационные системы»

- Какие новые виды атак и опасностей появились, какие ушли в прошлое, какие активизировались, и почему это произошло?

Павел Головлев: Давайте сразу договоримся, что мы обсуждаем только тему «электронные услуги, оказываемые банками», и не будем рассматривать сценарии атак собственно на банки, ведь это большая и отдельная тема, включающая в себя и инсайдерские проблемы, и целевые атаки, и конкурентную борьбу. Комплексные атаки, конечно, существуют, но именно в случае атак на банк. Что же касается атак в области финансовых услуг, то это - массовый рынок, и как любой современный массовый рынок он не терпит сложностей. По мере того, как банки внедряют новые защитные меры, злоумышленники развивают способы противодействия. Поскольку самое слабое звено - это клиентское устройство, то львиная доля атак сосредоточена именно в этом сегменте просто потому, что поверхность атаки больше, следовательно, так проще и быстрее получить профит. Чем десять раз красть по миллиону, оказывается безопаснее и выгоднее миллион раз украсть по 100 рублей. Пока что я не вижу причин для изменения этой тенденции.

Дмитрий Романченко: На мой взгляд, современные атаки, в отличие от прошлых, носят исключительно целенаправленный характер. Они нацелены на получение атакующей стороной определенных выгод: экономического, политического эффекта, влекут репутационные и иные издержки для объекта атаки. Современные акты вторжения всегда интегрированы с элементами социальной инженерии (как в фазе подготовки и осуществления атаки, так и в фазе окончательного эффекта). Сложно выделить состав компонентов ИТ-инфраструктуры банка (или иной организации в цепочке оказания банковского сервиса), которые наиболее часто подвергаются угрозам – здесь работает статистика и правило самого слабого звена. В этой связи, слабым звеном чаще оказываются каналообразующая часть и клиентские устройства. Возможность проникновения через гаджеты в ИТ-систему зависит от многих факторов, и прежде всего от качества кода самого прикладного ПО. На мой взгляд, целесообразно разделить виды атаки на вторжение с целью незаметного проникновения и атаки “вандального типа” (DDoS и прочие). Их схемы и способы проведения могут существенно отличаться.

Алена Зуева: В настоящий момент злоумышленники используют все виды атак. Выбор метода зависит от вида злоумышленника и его возможностей.

Наибольшую опасность, как и вероятность успеха нанести вред, представляет угроза от персонала - инсайдеры. Это может быть как обиженный сотрудник, имеющий доступ к важной информации (вред без извлечения материальной выгоды для себя), так и сотрудники, целенаправленно изучающие узкие места в защите информации. При определенном накопленном знании и низких моральных принципах они могут использовать это для излечения материальной выгоды. Определенный оптимизм внушает уверенность в том, что служба безопасности и служба HR банка стали достаточно требовательны к соискателям.

Сергей Марголин: Весьма значительный риск представляют для себя сами пользователи услуг банка - физические и юридические лица. Низкий уровень защиты, беспечность и общая «компьютерная» безграмотность позволяют злоумышленникам без особого труда воспользоваться чужой электронной подписью и перевести средства с расчетного счета пострадавшего. Часто найти злоумышленника не представляется возможным. Такие организационные меры, как хранение и регулярная смена паролей, хранение электронных подписей на сертифицированных средствах защиты информации (Ру-Токен, Е-токен) в несгораемых шкафах (сейфах), единоличное владение электронной подписью, хранение в тайне паролей доступа в интернет-банк, к сожалению, часто воспринимаются как назойливые советы «чокнутых безопасников».

Алена Зуева: Угрозы проникновения в автоматизированную систему существуют и извне. Общая цель таких атак – получение доступа к конфиденциальной информации, использование полученной информации в собственных целях или искажение информации. Такие проникновения обусловлены избыточностью функций протокола TCP/IP, который служит в настоящее время стандартом межсетевого взаимодействия. Он позволяет сопрягать различные устройства в глобальную сеть Internet и использовать общедоступные каналы связи. В настоящее время все интернет-банки используют защищенные протоколы передачи (SSL-протокол) и шифрование трафика с помощью средств криптозащиты информации при передаче информации по общим каналам связи сети Internet.

- И всё-таки, на какую из сторон приходится наибольший вес угроз и уязвимостей - на сторону клиента банка, на сторону самого банка и его подрядчиков - ЦОДов, телекомпровайдеров?

Павел Головлев: По мере того, как банки внедряют новые защитные меры, злоумышленники развивают способы противодействия. Поскольку самое слабое звено - это клиентское устройство, то львиная доля атак сосредоточена именно там, и причин для изменения этой тенденции нет

Алена Зуева: Если использовать критерий веса угроз как наибольшая вероятность успеха, умноженная на максимальный доход (убыток) от реализации вреда, то рейтинг угроз можно составить следующий:

1. Инсайдеры, работающие в банке – могут нанести самый тяжелый урон автоматизированной системе.
2. Подрядчики банка – ЦОДы, телекомпровайдеры, т.к. многие не обладают достаточным уровнем защиты от распределённых сетевых атак.
3. Клиенты банка.
4. Внешний злоумышленник, имеющий достаточные технические знания и средства для взлома автоматизированной системы, но не обладающий знаниями в политике безопасности в конкретном банке.

- Существуют ли комплексные угрозы: например, атака на клиентский гаджет как способ проникновение в ИТ-систему банка в целом? Расскажите об известных вам прецедентах и их последствиях?

Сергей Марголин: Через клиентский гаджет вскрыть ИТ-систему банка в целом при условии внимательного отношения банка к политике безопасности, разработке организационно-распорядительной документации и соблюдении ее положений, в настоящий момент достаточно проблематично.

Крупные платежные системы, такие как Visa и MasterCard много делают для усовершенствования платежных систем. В частности, международными платежными системами разработан и внедрен новый международный стандарт безопасности PCI DSS (Payment Card Industry Data Security Standard - стандарт безопасности данных индустрии платёжных карт).

Стандарт представляет собой совокупность двенадцати детализированных требований по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организа-

Алена Зуева: Ни одно из существующих решений ИБ не дает 100% защиту от злоумышленников. На сегодня в приложениях для сети Интернет, в мобильных приложениях используются комбинированные методы защиты, что требует от разработчиков усложнения алгоритмов идентификации и аутентификации пользователя интернет-банков. Для банков это означает рост затрат

ций. Принятие соответствующих мер по обеспечению соответствия требованиям стандарта подразумевает комплексный подход к обеспечению информационной безопасности данных платёжных карт.

Требования стандарта распространяются на все компании, работающие с международными платёжными системами Visa и MasterCard. В зависимости от количества обрабатываемых транзакций, каждой компании присваивается определённый уровень с соответствующим набором требований, которые они должны выполнять. В рамках требований стандарта предусматриваются ежегодные аудиторские проверки компаний, а также ежеквартальные сканирования сетей.

Высокая вероятность захода злоумышленника в систему Интернет-банка или осуществления платежа с помощью Интернет-магазина может быть при компрометации пароля доступа в Интернет-банк (программы-закладки на компьютере пользователя, хранении пароля доступа на стикере на мониторе и т.п.), передоверия своей банковской карты другому лицу, передача по открытым системам номера карты, дата истечения срока действия и CVC-кода. К примеру, эти данные могут запросить отельеры Европы по телефону или факсу при бронировании номеров в гостинице.

- Каковы уровень и динамика спроса на решения в области защиты информации разных типов: электронные ключи, QR-мидлетов, другие аппаратные средства, антивирусы (в том числе, встраиваемые в пользовательское ПО), другие виды (пожалуйста, укажите, какие)? Каковы достоинства и недостатки существующих решений?

Павел Головлев: Абсолютного решения - так называемой "серебряной пули" не существует. В современных условиях необходимо очень тонко сегментировать клиентскую базу и применять в каждом сегменте решения, наиболее адекватные поставленной бизнес-цели и риск-аппетиту. В этом контексте необходимо признать, что спроса со стороны самих клиентов пока нет, и не предвидится, так как любая мера безопасности – это, в первую очередь, снижение удобства. А спрос со стороны конкретного банка появляется и будет появляться только при наличии чисто экономических причин для возникновения такого спроса именно в этом банке.

Дмитрий Романченко: Область технологий информационной безопасности активно развивается, и ответ на этот вопрос – повод к отдельной дискуссии. При выборе способов и технологий ИБ всегда приходится искать баланс между удобством клиента и приемлемым уровнем безопасности. На текущий момент наблюдается существенное увеличение количества систем ДБО, использующих двухфакторную систему аутентификации. Широкое распространение получили одноразовые пароли, высылаемые на телефон клиента. Необходимо отметить и важные активности лидеров платежной индустрии Visa и MasterCard по переходу исключительно на чип-карты, и полный отказ от использования карт только с магнитной полосой. Данная активность существует в виде четкого плана с жесткими сроками. Это предполагает полную замену парка устаревших банкоматов. К сожалению, далеко не все российские банки готовы следовать подобным требованиям.

Алена Зуева: Нужно понимать, что ни одно из существующих решений не дает 100% защиту от злоумышленников. На сегодня в приложениях для сети Интернет (Интернет-банки), в мобильных приложениях (мобильный интернет для смартфонов), используются комбинированные методы защиты: разделение каналов получения паролей входа в интернет-банк (login, password хранит пользователь, подтверждение по разовому паролю через SMS, номеру мобильного телефона или карт-ридера), принудительные смены пароля для пользователя, аудит сложности подбора нового пароля. Это требует от разработчиков интернет-банков усложнения алгоритмов идентификации и аутентификации пользователя интернет-банков. Для банков это влечет развертывание и поддержание удостоверяющих центров на серверах банковской автоматизированной системы.

- Следовательно, растут затраты на обслуживание и разработку ПО…

Алена Зуева: Да, настоящий бум переживают сертифицированные средства криптографической защиты информации (электронные ключи). Это вызвано, с

одной стороны, низкой ценой устройства, высокой степенью надежности от копирования информации с устройств Ру-токен (Е-токен). Минусы в небольших размерах устройства (он же главный плюс), а значит, его достаточно просто потерять. Также устройства часто путают с обычным flash-накопителем и забывают в USB-портах.

Сергей Марголин: Отмечу, что рынок QR-мидлетов и карт-ридеров не так сильно распространен в России. Возможно, это вопрос будущего. А вот необходимость покупки и обновления антивирусных программ у пользователей уже выработана. Сейчас мяч на стороне разработчиков ПО – актуальными являются снижение цены антивируса с одновременным повышением его надежности, своевременное обновление баз знаний по различным вирусам, сервисная поддержка пользователей. С точки зрения развития, следует обратить внимание на пользователей мобильных приложений Интернет-банков и своевременную поставку антивирусного ПО для смартфонов.

Андрей Рябов: Мы исходим из того, что, токены, защищенные ключевые носители, электронные замки, модули доверенной загрузки, средства разграничения доступа, VPN, межсетевые экраны и т.п. позволяют обеспечить достаточный уровень защищенности только в комплексе. Но если есть хотя бы одна функция, связанная с безопасностью, - изделие нуждается в сертификации. А когда изделие сертифицировано, кто, за исключением горстки специалистов, поймет, что оно обеспечивает не «безопасность», а приемлемое выполнение только одной (или нескольких) функций?! Защита подменяется имитацией защиты. Имитация - проблема эпохи.

Не решает проблему и подключение к недоверенному компьютеру устройства электронной подписи, подписывающего и отображающего платежку. Да, если это устройство простейшее, его можно исследовать, зафиксировать его состояние и считать доверенным. Но проблема в том, что его функциональность будет слишком узкой (в силу простоты). Значит, использовать его будет неудобно. А если функциональность сделать близкой к привычной, которую предоставляют компьютеры, тогда и все проблемы компьютеров перенесутся на это устройство. И снова о доверенности придется забыть.

Еще один сюжет: в 2012 году один известный вендор представил новое устройство, позволяющее использовать на платформе iOS (iPhone/iPad) смарт-карты с сертифицированной российской криптографией. Утверждается, что смарт-карта и ридер

для iPad/iPhone дают возможность использовать квалифицированную электронную подпись в системах электронного дистанционного обслуживания, интернет-банкинга, при работе с электронными государственными услугами и пр.

- Как оценить, насколько это соответствует действительности?

Андрей Рябов: Обратимся к положениям Федерального Закона «Об электронной подписи» № 63-ФЗ. В соответствии с ч.2 п.4 ст.5 «для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии 63-ФЗ». В соответствии с п.4 ст.10 участники обмена при использовании квалифицированной ЭП «обязаны использовать СЭП, получившие подтверждение соответствия требованиям ФЗ-63». В соответствии с п.5 ст.8. ФСБ РФ устанавливает требования к СЭП и осуществляет подтверждение соответствия СЭП установленным требованиям. Требования к СЭП устанавливаются Приказом ФСБ РФ № 796 (далее – Приказ).

- Но ведь рассматриваемая смарт-карта в настоящий момент не имеет документов, подтверждающих соответствие требованиям к СЭП?

Андрей Рябов: Однако отсутствие документов еще не говорит об отсутствии соответствия, а говорит лишь о том, что оно не подтверждено.

- А соответствует ли анонсированный продукт требованиям Приказа?

Андрей Рябов: Смарт-карта может выполнять функции СКЗИ, хранилища ключевой информации, можно на смарт-карту загрузить Java applet для выполнения прикладных задач. Но для выполнения п.8 и 9 Приказа необходимо выполнять визуализацию подписываемого/проверяемого документа, подтверждение создания подписи, просмотр того, что подпись создана.

Данные функции могут реализовываться программными и аппаратными средствами, с которыми штатно функционируют средства ЭП – среда функционирования. В данном случае – это либо прикладное ПО, либо Web-браузер, функционирующие на устройствах Apple с ОС iOS. То есть iPad/iPhone с операционной системой iOS в рассматриваемом случае будут являться компонентами среды функционирования СЭП.

В соответствии с Приказом, средства ЭП и среда их функционирования, должны противостоять угрозам, представляющим собой целенаправленные действия с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемой средствами ЭП информации или с целью создания условий для этого – атаки.

Например, для средства ЭП класса КС1 (класс с наименьшими требованиями по информационной безопасности) среда функционирования, с которой они штатно должны функционировать, для прохождения оценки соответствия в системе сертификации ФСБ по требованиям Приказа, должны противостоять таким атакам, как внесение несанкционированных изменений в компоненты среды функционирования, в том числе с использованием вредоносных программ; проведение атак на программные и аппаратные компоненты среды функционирования.

- Каковы методы противодействия таким атакам?

Андрей Рябов: Методами противодействия этим атакам могут служить применение сертифицированных решений для защиты от НСД (наложенные СЗИ или сертифицированная ОС), контроль целостности критических важных файлов, которые не должны изменятся в процессе работы; применение антивирусных средств.

На сегодняшний день сертифицированных средств защиты информации для операционной системы iOS, которые могли бы противостоять приведенным выше атакам, нет, а вопросы, связанные с механизмами безопасности, интегрированными в iOS, остаются открытыми.

Антивирусных продуктов для мобильных устройств Apple тоже нет, а ряд атак именно на те системы, для применения в которых анонсируется рассматриваемый продукт, в наше время как раз реализуется с помощью шпионского ПО. Например, подмена платежных реквизитов в XML-документе при отправке его на подпись в системах ДБО.

- То есть, если рассматривать связку устройств «смарт-карта и ридер + устройство Apple», атака как раз приходится на компонент среды функционирования СЭП – кеш Web-браузера устройства Apple?

«

Сергей Марголин: Инноваций требует область хранения персональных данных в части усиления ответственности за утечки, принудительной аттестации систем обработки персональных данных и, как следствие, рост предложений программно-аппаратных средств по защите информации

Андрей Рябов: Да, поскольку нельзя противодействовать атакам на приложение или Web-браузер, которые являются компонентами СФ СЭП и отвечают за функции визуализации подписываемой информации и другие предусмотренные п.8 и 9 Приказа, нужно признать, что они функционируют в недоверенной среде и подвержены атакам.

- Стало быть, для использования квалифицированной ЭП в системах ЭДО, интернет-банкинга и пр. – недостаточно только применения «связки» смарт-карты и ридера?

Андрей Рябов: Необходимо также, чтобы СЭП и среда функционирования удовлетворяли требованиям Приказа для соответствующего класса СЭП, а средства СЭП были сертифицированы по требованиям Приказа.

- То есть неназванный вами вендор, выпустив ридер для мобильных устройств Apple, создал не СЭП для iOS, а технические предпосылки для использования смарт-карт в качестве хранилища ключевой информации и СКЗИ на iPad/iPhone?

Андрей Рябов: В основе безопасности всегда должна лежать доверенная среда. Это нужно хорошо понимать.

Андрей Рябов: Токены, защищенные ключевые носители, электронные замки, модули доверенной загрузки, средства разграничения доступа, VPN, межсетевые экраны и т.п. позволяют обеспечить достаточный уровень защищенности только в комплексе. Но если есть хотя бы одна функция, связанная с безопасностью, - изделие нуждается в сертификации. А когда изделие сертифицировано, кто, за исключением горстки специалистов, поймет, что оно обеспечивает не «безопасность», а приемлемое выполнение только одной (или нескольких) функций?! Защита подменяется имитацией защиты. Имитация - проблема эпохи

Павел Головлев: Категорически не согласен! Начнем с того, что мне до сих пор никто так и не ответил на вопрос: «А зачем при проведении платежей использовать квалифицированную подпись?». Сертифицированные средства в подавляющем большинстве случаев защищают хуже, чем несертифицированные, по ряду объективных причин, главные из которых - технологическое отставание,

Павел Головлев: От нарушений дисциплины не защищает ничего. Невозможно полагаться только на технические решения. Необходимо учить и клиентов, и сотрудников банков правилам «компьютерной гигиены». «Деньги в компьютере» это такие же деньги, как и в кошельке, поэтому компьютер надо беречь так же как кошелек

невозможность адаптации под бизнес-процессы и потребности клиента, абсолютно неадекватная цена, а также полное отсутствие ответственности производителя. А чаще всего, необходимых бизнесу «здесь и сейчас» сертифицированных средств, как было отмечено выше, просто нет и не предвидится.

Среди двадцати девяти актуальных защитных мер для систем ДБО, выработанных рабочей группой практиков банковской безопасности, нет ни слова о сертифицированных средствах. Они, конечно, могут применяться, но на рынке также есть гораздо более эффективные несертифицированные средства. Связки смарт-карты и ридера, действительно, может быть недостаточно, но отказываться от нее только потому, что она несертифицирована, просто неразумно.

Сертификация в наших условиях – не панацея, а не более чем дополнительная фискальная нагрузка на бизнес, имеющая, в целом, отрицательную эффективность и создающая для клиентов ложное ощущение безопасности.

Также необходимо понимать, что создание доверенной среды на стороне клиента - это практически неразрешимая задача. Никто не будет передавать деньги лотошнику за стаканчик мороженого через банковскую ячейку. Эффективность использования на компьютере клиента средств контроля целостности операционной системы и программных компонентов, оцененная экспертами, составляет чуть выше восьми процентов в контексте снижения риска. А вот насильственное навязывание подобных решений является серьезной головной болью для банков.

Алена Зуева: может быть в данном примере следует различать программные и аппаратные средства? Программные (СКЗИ) должны быть сертифицированы, сертификацией занимается ФСБ и все, что рассказал Андрей Рябов – истина. Аппаратные же (или технические средства) по последним веяниям ФСТЭК (приказ ФСТЭК №21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных») ч.I п.4 говорит об оценке соответствия. В данной трактовке собственник информационной системы (в нашем случае – банк) вправе сам решать какие средства защиты от несанкционированного доступа он будет применять: сертифицированные или прошедшие соответствие по уровню безопасности. Если же банк является государственным, то он обязан использовать только сертифицированные средства защиты.

Андрей Рябов: Уточню ещё раз, что отсутствие сертификата (и подтверждения оценки соответствия) не говорит о том, что требования безопасности не выполняются. О том, что они не выполняются, я сделал вывод, основываясь на совсем других посылках, которые были подробно изложены. Не вижу смысла комментировать мнение о том, что требования регуляторов надуманы и завышены. Все серьезные безопасники считают требования регуляторов слабыми, отстающими от реальных хакерских атак, и в своих средствах защиты предусматривают и те защитные механизмы, которые практически необходимы, но не отражены в требованиях. Есть и другой подход - имитация выполнения требований. Об этом я тоже сказал.

А вот с тем, что создание доверенной среды на машине клиента на период работы с банком - это практически нерешаемая задача – не могу согласиться. Такие решения на отечественном рынке есть, и они сертифицированы, и имеют положительный опыт интеграции с системами «Клиент-Банк». Это средства обеспечения доверенного сеанса связи. Мы называем эту технологию "Серебряной пулей для хакера".

- Что можно сказать о сопровождении и поддержке средств защиты на текущий момент? Изменились ли издержки банка как пользователя, клиента банка как пользователя, и поставщика решения? Чьё бремя стало тяжелее? Как урегулируются потери при наступлении инцидента?

Павел Головлев: К сожалению, поставщики решений сейчас не отвечают ни за что, но при этом обладают чрезмерно хорошим аппетитом, сложившимся под влиянием очень крупных заказчиков. Поэтому распределение издержек между банком и клиентом, а также урегулирование инцидентов – исключительно вопрос стратегии и тактики управления рисками конкретного банка.

Дмитрий Романченко: В связи с расширением ландшафта угроз и частоты инцидентов информа-

ционной безопасности, а также в связи с развитием рынка современных «тяжелых» решений, пока что затраты банков только растут. В свою очередь, поставщики решений несут издержки, связанные с адаптацией своих продуктов к новым требованиям и прохождением сертификации. Развитие аутсорсинга рынка функций ИБ пока находится на недостаточном уровне, как в силу технических проблем, так и в силу организационно-правовых (к примеру, непонятно, как распределять компенсацию в случае инцидента ИБ между банком и сервис-провайдерами). Рынок страхования рисков ИБ также находится в зачаточном состоянии. Очевидно, что издержки в каком-то объеме перекладываются на клиента.

- Как соблюсти баланс в соотношение безопасности и мобильности, эксплуатационных качеств и стоимости владения для пользователей? Какие средства максимально защищают бизнес от нарушений пользовательской дисциплины – небрежности пользователя при вводе, хранении паролей, хранении аппаратных устройств защиты и т.п.?

Павел Головлев: Надо считать риски, сегментировать клиентов, продукты и услуги, обеспечивать многовариантность решений. Абсолютного решения не существует: то, что хорошо для одного банка может быть абсолютно неприменимо для другого. То, что устраивает одного клиента, может совершенно не нравиться десятку других. Единственное, о чем можно сказать с уверенностью, это то, что от нарушений дисциплины не защищает ничего. Мы, наверное, единственная страна, в которой каждую весну со льдин спасают одних и тех же рыбаков. Невозможно полагаться только на технические решения. Необходимо учить, учить и еще раз учить и клиентов, и работников правилам «компьютерной гигиены». «Деньги в компьютере» это такие же деньги, как и в кошельке, поэтому компьютер надо беречь так же как кошелек.

Лично мне импонирует решение, когда ключи подписи системы «Клиент-Банк» хранятся на той же карточке, на которой хранятся личные средства директора или бухгалтера. Безопасность таких ключей гораздо выше, но и сопутствующих проблем по управлению ключевой инфраструктурой больше. Не каждый может себе позволить такое решение.

Дмитрий Романченко: Клиент должен иметь возможность определять свой баланс между удобством пользователя и приемлемым для него уровнем безопасности. Если система ДБО не будет достаточно гибкой в этом вопросе, то это может негативно повлиять на удовлетворенность клиента предоставляемыми услугами. Но вести «просветительскую» работу с клиентом необходимо. Уровень «компьютерной грамотности» населения, к сожалению, оставляет желать лучшего. Поэтому необходимо объяснять клиентам важность вопросов ИБ и даже склонять их к соблюдению правил информационной безопасности. Этому могла бы способствовать практика удаленного аудита компьютера клиента и взимания дополнительных комиссий в случаях, если клиент не выполняет требования к информационной безопасности.

С другой стороны, для определения требуемого уровня безопасности важно понимать возможности и цели нарушителя. Если речь идет о преступных группировках, то ситуация одна. Если речь идет о возможностях государства (в том числе иностранного), либо их использования преступными (коррумпированными) сотрудниками, то ситуация совсем иная. Раскручивающийся в настоящее время скандал с прямым доступом Агентства Национальной Безопасности США к серверам Microsoft, Google, Apple, YouTube и других наглядно показал цену защиты указанных сервисов, технологий. А, соответственно, и мобильных устройств производства указанных компаний или использующих соответствующее ПО. Так что в любом случае надо понимать приемлемость рисков для клиентов.

Сергей Марголин: Здесь работает общий принцип охраны информации – комплекс мер по охране по стоимости не должен превышать стоимость самой информации. Максимальную защиту принесут только комплексные меры – организационные, программные, дисциплинарные. И меры должны пересма-

Дмитрий Романченко: Область технологий информационной безопасности в банковском секторе активно развивается. На текущий момент наблюдается существенное увеличение количества систем ДБО, использующих двухфакторную систему аутентификации и иные защитные механизмы: к примеру, широкое распространение получили одноразовые пароли, высылаемые на телефон клиента. Лидерами индустрии платежных карт (Visa, MasterCard) реализуется дорожная карта по полному отказу от использования “нечипованных” карт только одной с магнитной полосой. Это предполагает полную замену парка устаревших банкоматов, к чему готовы далеко не все российские банки.

триваться и обновляться не реже чем один раз в 3 года (общая оценка безопасности информационной системы). По конкретному направлению меры могут пересматриваться и чаще, например смена пароля может осуществляться каждые три месяца.

- Каков оптимальный портфель решений для обеспечения безопасности электронных финансовых услуг для банка и для его клиента? Какова его средняя цена владения? Каковы бюджеты и сроки проектов для корпоративных заказчиков?

Павел Головлев: Рецепта не существует, как не существует стандартного решения. Каждое решение должно быть уникальным и учитывать все аспекты бизнеса банка и его риски. Рабочая группа, в которую входят эксперты из нескольких банков, уже разработала несколько моделей угроз для различных областей деятельности банков, содержащих как оценку актуальности угроз, так и оценку эффективности различных защитных мер как в целом, так и в отношении конкретных угроз. Из этих моделей видно, что общая эффективность самой эффективной защитной меры в системах ДБО чуть выше 40%. В области карточного бизнеса этот показатель в два раза ниже, но и выбор защитных мер значительно богаче. Соответственно, защитные меры должны комбинироваться для снижения риска до приемлемого уровня с учетом того, что оптимальная стоимость решения должна составлять 10-15% уровня исходного риска. При этом необходимо не забывать об иных затратах, сопутствующих внедрению любой защитной меры, таких как затраты на интеграцию с существующими бизнес-процессами, на сопровождение, реагирование на инциденты, корректировку параметров автоматизированных систем, логистику и т.п.

Дмитрий Романченко: Стоимость портфеля для клиента оценить сложно, так как указанная цена может быть спрятана в стоимости отдельных технических средств (электронные ключи, антивирусное и прочее ПО), в стоимости банковских продуктов, в стоимости страхования по отдельным продуктам, условиям покрытия рисков информационной безопасности.

Стоимость для банка складывается из стоимости решений (оборудование и ПО, стоимости поддержки, стоимости внешнего сервиса). Стоимость продуктов одного и того же класса может существенно отличаться. Типовой набор, приведенный в различных российских и западных стандартах, примерно совпадает (PCI DSS, требования по безопасности в развитие ФЗ-161, СТО БР ИББС, 21 приказ ФСТЭК от 2013 года и проч.). Это большой список, включающий в себя до 20 необходимых функций информационной безопасности и соответствующих решений.

- Какие инновации просматриваются в перспективе для включения в продукты класса ДБО в целях обеспечения безопасности электронных финансовых услуг?

Павел Головлев: В общем-то, в особых инновациях необходимости нет. Было бы желание и возможности адекватно и к месту применять то, что уже есть. При этом ощущается острая потребность в «демократизации» ценовой политики поставщиков решений. В этом свете лично мне нравится новый продукт «PayControl» компании «СэйфТек». В сегменте для физических лиц, и даже малого и среднего бизнеса, – очень достойное решение.

Сергей Марголин: На мой взгляд, инноваций требует область хранения персональных данных в части усиления ответственности операторов персональных данных за утечки, принудительной аттестации систем обработки персональных данных и, как следствие, рост предложений программно-аппаратных средств по защите информации. Как пример можно привести постепенный переход от карт с магнитной полосой на чиповые карты и расширение использования виртуальных карт.

Дмитрий Романченко: Существенный вклад в обеспечение безопасности систем ДБО может внести анализ «платежного профиля» клиента. Интересным способом защиты от «фишинга» является персонализация интерфейса системы под клиента. Перспективным направлением является использование новых способов аутентификации (например, на основе биометрических данных). Однако основная инновация, которая может радикально изменить ситуацию, это совместные действия банков, интернет и сервис провайдеров в построении сквозных интегрированных систем обеспечения ИБ со сквозными бизнес-процессами в данной области. Это позволит создать такую глубину стека технологий безопасности, которая будет сложно преодолима даже для хорошо вооруженного злоумышленника, а значит, снизит частоту успешных инцидентов ИБ и, соответственно, потери. Более того, данный подход позволит разумно распределить риски (и покрытие по ним) между различными участниками ДБО. Это позволяет надеяться, что в итоге выиграет клиент.

- Эксперты утверждают, что Россия находится в списке лидеров по количеству сотовых телефонов и других электронных гаджетов, но и на первых

позициях по объему наличных платежей. Готовы ли отечественные банковская и платежная индустрии к взрывному росту электронных платежей, если таковой случится, с точки зрения безопасности электронных финансовых услуг?

Павел Головлев: Я не вижу причин для взрывного роста электронных платежей. Для проведения электронных платежей необходимо не столько наличие гаджета у плательщика, сколько заинтересованность и возможность приема таких платежей получателями. А эти процессы регулируются совсем иными и, зачастую, совсем не технологическими обстоятельствами. В этой сфере сейчас идет нормальный эволюционный рост, и банковская индустрия с ним вполне справляется, более того – всеми силами старается его стимулировать, так как считает недостаточным. При этом, в течение 2010-2012 годов удельный риск в системах ДБО по всей банковской системе оценивается стабильно - в одну копейку на каждую тысячу рублей в обороте. В карточном бизнесе в 2011году он подрос в полтора раза по сравнению с предыдущими годами, и стабилизировался на уровне пятнадцати копеек на ту же тысячу рублей. Основную опасность представляет именно революционное насаждение новых технологий и продуктов. Зачастую, при разработке этих продуктов и технологий вопросы безопасности не просто не рассматриваются, а сознательно игнорируются, так как устанавливаются иные критерии эффективности. В этом контексте индустрия безопасности всегда будет выступать в роли догоняющего, и главной задачей является недопущение ситуации, когда разрыв станет критическим.

Дмитрий Романченко: Готовы ли банки? Если ответить кратко, то не готовы. Но это следует воспринимать дифференцированно по отношению к различным категориям финансовых институтов и инструментов, различным банкам. Инвестиции крупных банков в ИБ вполне ощутимы, и ситуация существенно улучшилась по сравнению с ситуацией пятилетней давности. Но сохраняется неравенство по уровню ИБ между крупными банками, средними и мелкими, между центральными офисами и филиалами, между различными видами платежей (карточные платежи, клиент-банк, электронные деньги и проч.).

Алена Зуева: Хочется верить, что Россия постепенно улучшает свои системы банковского и платежного обслуживания. Также улучшаются магистральные каналы связи, идет бурное строительство оптоволоконных и спутниковых линий связи. В России есть опыт построения больших автоматизированных систем и сделаны большие финансовые вложения для закупки нужного оборудования.

Сергей Марголин: В России много талантливых программистов и инженеров, которые все больше работают внутри страны. Решения, которые уже имеются, на мой взгляд, доказывают, что справиться с взрывным ростом электронных платежей России вполне под силу.

С точки зрения безопасности, необходимо учитывать ошибки при построении как коммерческих систем массового обслуживания, так и государственных информационных систем (ГАС «Выборы», ЕГЭ, «Пенсионного фонда»), анализировать и не допускать их повторения.