Управление рисками

ЭЛЕКТРОННЫЙ БАНКИНГ: УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

П. В. РЕВЕНКОВ,
кандидат экономических наук,
заведующий сектором Департамента банковского регулирования и надзора Банка России
E-mail: rpv@mail.cbr.ru

В статье обосновывается необходимость проведения мероприятий по информационной безопасности в кредитных организациях в связи с распространением мошеннических действий через Интернет и появлением ряда стандартов Банка России по обеспечению информационной безопасности. Рассмотрены организационные меры обеспечения информационной безопасности при применении кредитными организациями технологии электронного банкинга, и приведен анализ проявления источников рисков информационной безопасности.

Ключевые слова: *электронный банкинг, информационная безопасность, риски информационной безопасности.*

Электронный банкинг (ЭБ) – один из самых динамично развивающихся видов дистанционного банковского обслуживания (ДБО).

В силу своих очевидных преимуществ системы ЭБ стали широко применяться в российских кредитных организациях. К их основным достоинствам можно отнести существенную экономию времени за счет исключения необходимости посещать банк лично и возможности 24 ч в сутки контролировать собственные счета, а также оперативно реагировать на изменения ситуации на финансовых рынках.

Имея неоспоримые преимущества в мобильности и простоте в управлении, технологии ЭБ являются еще и постоянным объектом повышенного внимания со стороны мошенников. Больше всего проблем доставляют «спам»[1] и «фишинг» [2].

Жертвой спама стать несложно. Неизвестному отправителю нужно просто знать адреса электронной почты. Существует масса программных средств, которые выискивают в Интернете все последовательности символов, содержащие символ «@». Помимо этого, в Интернете можно нередко встретить сообщения о продаже базы данных с электронными адресами миллионов пользователей, а также программные средства для организации массовых рассылок[3].

Исследовательская компания Radicati Group подсчитала, что в Европе в 2004 г. ущерб от спама составил 9,2 млрд евро, за 2005 г. – 17,1 млрд евро, в 2006 г. – 30,3 млрд евро, а прогнозы на 2007 и 2008 гг. составляли 51,1 и 85,4 млрд евро соответственно [1]. Спам используется и в качестве средства доставки вирусов на компьютеры пользователей Интернет[4]. Например, червь Mimail. E распространяется по

* Настоящая статья выражает исключительно мнение автора и не отражает позиции Банка России.

[1] Спам – самопроизвольная массовая рассылка электронных почтовых сообщений.

[2] Фишинг (англ. Phishing) – это способ мошеннических действий, при котором преступник рассылает множество сообщений по электронной почте в целях получения личной и финансовой информации о потенциальных жертвах для доступа к их банковским счетам и другим важным ресурсам.

[3] В США, Австралии и Великобритании подобная деятельность преследуется в законодательном порядке, и злоумышленнику грозит весьма серьезный штраф или тюремное заключение.

[4] Именно так, к примеру, распространялся известный вирус Sobig.

электронной почте в виде вложенного файла, маскирующегося под ZIP-архив. После активации червь не только приступает к размножению, но и начинает генерировать DoS-атаки[5] на сайты Spews, Spamhaus и Spamcop. Данные проекты занимаются составлением черных списков адресов отправителей спама и их союзников. Можно только представить, сколько забот этот червь принес законопослушным владельцам электронных адресов.

Что касается фишинговых писем, то они приходят якобы от лица банков, платежных систем, онлайн-аукционов, крупных и широко известных интернет-магазинов. Такое письмо создается, форматируется и оформляется таким образом, чтобы выглядеть как отправленное легальным источником. Подделываются не только заголовки письма, но и внешний вид, в него включаются знакомые клиентам банка графические и текстовые элементы, ссылки на реальный сайт. Чаще всего письмо содержит ложную информацию о внезапно возникших технических проблемах на сайте кредитной организации (КО) или платежной системы, в связи с чем якобы возникла необходимость поверки учетных записей и регистрационных данных пользователей.

Получив конфиденциальную информацию, предоставляющую возможность управлять банковским счетом, мошенники начинают тратить деньги клиента на приобретение товаров и услуг, т. е. распоряжаться банковским счетом и кредитной картой по своему усмотрению.

Для противодействия развитию и росту количества афер с использованием фишинговых сообщений в интернете в 2003 г. была создана специальная организация Anti-Phishing Working Group (APWG) [6]. Ассоциация APWG насчитывает более 2 500 членов, свыше 1 600 компаний и агентств, 8 банков, которые входят в десятку крупнейших банков США, четыре крупнейших интернет-провайдера США, сотни производителей и продавцов сетевого оборудования, государственные и частные юридические компании по всему миру.

По данным APWG, в августе 2006 г. по всему миру было произведено 26 150 фишинг-атак. Специалисты объясняют такой рост активности появлением специализированного программного обеспечения, своего рода «наборов юного Фишера». С помощью таких программ даже дилетант легко справится с созданием клона сайта понравившегося банка или платежной системы и размещением его в Интернете.

Учитывая тот факт, что Банк России выпустил уже третью редакцию Стандарта по информационной безопасности «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2008) (далее – Стандарт) и ряд других стандартов по данной тематике[7], можно предположить, что в ближайшем будущем отношение регулятора к состоянию информационной безопасности (ИБ) в кредитных организациях изменится.

Для развития и продвижения стандартов Банка России по обеспечению ИБ было создано Сообщество организаций ABISS, в которое входят уже более 30 кредитных организаций и 6 образовательных учреждений. Цель данного сообщества – способствовать развитию и широкому практическому применению единых стандартов, повышению уровня информационной безопасности организаций финансового сектора и содействию стабильности кредитно-финансовой системы Российской Федерации в целом.

Решать задачу обеспечения информационной безопасности ЭБ необходимо комплексно, на основе правовых, организационных, физических, технических, аппаратно-программных, криптографических и этических мероприятий.

В статье будут рассмотрены только организационные меры (ОМ) обсечения ИБ, так как, по мнению автора, именно от их соблюдения во многом зависит качественное выполнение всех мер, составляющих единый комплекс мер по обеспечению ИБ в КО.

Технологии ЭБ перевели большую часть элементов банковской операции в автоматический режим, но проблема человеческого фактора осталась. В некотором роде она даже усилилась. Если раньше (при ручной обработке первичных платежных документов) работник банка (операционист) принимал документ от клиента, сверял паспортные данные с подлинником и проверял правильность заполнения всех полей в документе, то при применении технологии ЭБ таких контрольных точек стало

[5] DoS-атака (от англ. Denial of Service, отказ в обслуживании) и DDoS-атака (от англ. Distributed Denial of Service, распределенный отказ в обслуживании) – это разновидности атак на вычислительную систему. Цель этих атак – довести систему до отказа, т. е. создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступа к предоставляемым системой ресурсам, либо этот доступ затруднен.

[6] См. сайт: URL: http://www.antiphishing.org.

[7] Все принятые стандарты Банка России по информационной безопасности размещены на официальном сайте Банка России. URL: http://www.cbr.ru или на сайте: URL: http://www. abiss.ru.

значительно меньше и как следствие – появились новые источники банковских рисков. Основными причинами их возникновения являются: виртуальный характер и высокая скорость выполнения банковских операций, общедоступность открытых телекоммуникационных систем и активное участие фирм – провайдеров услуг в проведении операций. Исходя из этого, можно сделать вывод, что значимость человеческого фактора не стала меньше, а в некотором роде даже усилилась, учитывая возможные масштабы денежных потерь.

Вместо взлома замков и физического проникновения в чужие помещения злоумышленники могут осуществлять удаленные сетевые проникновения для сбора, искажения и удаления интересующей их информации.

При определенном подходе сетевые вторжения представляют гораздо меньший риск для взломщиков, чем физическое проникновение, поскольку скрыть свои следы в виртуальном пространстве гораздо легче, чем в реальном мире. Данная ситуация усложняется еще тем, что правоохранительные органы еще не обладают достаточным опытом по расследованию компьютерных преступлений, в отличие от расследования физических краж со взломом, а персонал – необходимыми навыками и соответствующей подготовкой. Следовательно, кредитным организациям необходимо самостоятельно строить защиту своих информационных ресурсов от различного рода компьютерных преступлений. Основу всех мероприятий по обеспечению ИБ составляют ОМ. Они могут применяться для предотвращения угроз, как со стороны внешних злоумышленников, так и со стороны инсайдеров[8].

Процесс выбора ОМ – это творческий, требующий постоянного совершенствования процесс. Но все же основные направления деятельности КО по обеспечению ИБ существуют. Рассмотрим основные их них.

Психологические меры. Систему ИБ внедряют двумя способами: открытым или закрытым. Если основная цель внедрения системы заключается в выявлении уже действующего канала утечки и определении всех его звеньев (причем не только исполнителей внутри КО, но и заказчиков информации вне ее) – применяется закрытый способ. Как правило, не доводя состава процедур до персонала, внедряют мониторы активности пользователей и контентную фильтрацию почты и Web-трафика.

Если же внедрять систему защиты от внутренних угроз открыто, то за счет психологического фактора можно даже сэкономить. Известно, что при внедрении систем видеонаблюдения для защиты в отдельных помещениях КО можно ставить неподключенные камеры, так как сам факт наличия видеокамеры наблюдения останавливает большую часть нарушителей [2].

Такие меры, как организация более совершенной системы хранения электронных документов, ознакомление сотрудников с новыми регламентами, предание гласности инцидентов, связанных с нарушениями в обеспечение ИБ, в большей части остановят сотрудников, которые имели намерения похитить, исказить, блокировать и уничтожить информационные ресурсы КО.

Права локальных пользователей и стандартизация программного обеспечения. Установив любое специализированное программное обеспечение (ПО), вряд ли можно решить все проблемы, связанные с утечками конфиденциальной информации, поэтому ПО необходимо периодически проверять на возможность преодоления защиты. Кроме постоянного тестирования системы безопасности, необходимо ограничить возможности потенциальных взломщиков. В первую очередь это достигается за счет лишения пользователей прав локального администратора на их рабочих местах[9].

В каждой КО должен быть документ, определяющий список ПО, допустимого к установке на рабочих станциях. Особо внимание следует обращать на желание некоторых сотрудников включить в этот список такие мощные файловые менеджеры, как, например, FAR или Total Commander.

Специфические решения и работа с кадрами. Специфические решения относятся к разряду нестандартных и принимаются индивидуально в каждой отдельно взятой КО. Они могут быть направлены на ужесточение порядка выдачи разрешений на получение информации из баз данных, доступ к которым ограничен в силу конфиденциальности находящейся в них информации. Достаточно эффективным способом является ограничение по объему ежедневных запросов, а для тех, кому необходимо получить больший объем

[8] Инсайдер (Insider) – осведомленное лицо. В узком смысле – держатель акций, исполнительное лицо или директор некоторой компании, который владеет «значительной» долей акций данной компании. В более широком понимании – тот, кто имеет доступ к информации, которая недоступна широкой общественности и существенно влияет на цену акции данной корпорации. См.. *Шарп У., Александер Г., Бейли Дж.* Инвестиции / пер. с англ. М.:ИНФРА-М. 1999.

[9] Чаще всего такая ситуация связана с наличием в КО унаследованного ПО, неспособного работать с операционными системами, поддерживающими удаленное управление.

информации, должны оформлять дополнительную заявку с обоснованием служебной необходимости и т. д.

В указанном стандарте Банка России по ИБ сказано, что «наибольшими возможностями для нанесения ущерба организации банковской системы Российской Федерации обладает ее собственный персонал».

Для успешной работы с персоналом КО необходимо помнить, что залогом эффективности данного процесса является соблюдение принципов последовательности и непрерывности. Привлекать к процессу обучения по вопросам обеспечения ИБ целесообразно всех сотрудников, имеющих отношение к работе с конфиденциальной информацией.

Документарное обеспечение. Все документы можно разделить на три основных уровня применения.

Уровень КО. Это самый верхний уровень в иерархии внутренних распорядительных документов. Начиная с этого уровня, необходимо распространить организационную составляющую системы обеспечения ИБ на все остальные уровни. К этому уровню относятся трудовые соглашения и должностные инструкции, описывающие права и обязанности сотрудников.

Уровень информационной системы. На данном уровне важно определить регламент пользования корпоративной информационной системой и регламент пользования приложениями. Эти документы закрепляют состояние информационной системы, позволяют контролировать запуск потенциально опасных приложений и достичь соответствия корпоративной сети специфическим требованиям для контроля и аудита качества обеспечения ИБ.

Уровень ИБ. На данном уровне необходимо определить модель нарушителя, политику доступа к информации и политику работы с информацией. По сути, именно на уровне ИБ происходит непосредственная работа по контролю и аудиту действий пользователей. Между каждым пользователем, группами пользователей и каждым документом создаются отношения прав, внедряются механизмы журнализации и предотвращения несанкционированных действий.

Хранение физических носителей. Достаточно эффективным способом является анонимизация носителей. Сотрудники, имеющие доступ к носителям, не знают, на каком носителе какая информация записана, они управляют только анонимными номерами носителей. Те сотрудники, которые знают, на каком носителе находится какая информация, в свою очередь, не должны иметь доступа к хранилищу носителей. Другой не менее эффективный способ – шифрование информации при резервном копировании. Даже если информация будет вынесена или скопирована – потребуется некоторое время на ее расшифровку. Нельзя забывать и про замки, открывающиеся только двумя ключами, находящимися у разных сотрудников и т. д.[10].

Система мониторинга работы с конфиденциальной информацией. Система мониторинга работы с конфиденциальной информацией должна постоянно наращиваться функционалом и аналитическими возможностями. Развиваться она может в двух направлениях.

Первое направление – интеграция систем защиты от внутренних и внешних угроз. Инциденты последних лет показывают, что существует распределение ролей между внутренними и внешними злоумышленниками, поэтому объединение информации из систем мониторинга внешних и внутренних угроз позволит обнаруживать факты таких комбинированных атак. Одной из точек соприкосновения внешней и внутренней безопасности является управление правами доступа. Любые заявки на получение доступа к ресурсам, не предусмотренным служебными обязанностями, должны немедленно приводить в действие механизм аудита работы с этой информацией.

Другое направление развития системы мониторинга внутренних инцидентов с конфиденциальной информацией – построение системы предотвращения утечек. Алгоритм работы такой системы тот же, что и в решениях по предотвращению вторжений. Сначала строится модель нарушителя, по ней формируется «сигнатура нарушения», т. е. последовательность действий нарушителя. Если несколько действий пользователя совпали с сигнатурой нарушения, прогнозируется следующий шаг пользователя, если и он совпадает с сигнатурой – подается сигнал тревоги. Например, был открыт конфиденциальный документ, часть его была выделена и скопирована в буфер, затем был создан новый документ и в него было скопировано содержимое буфера. Система предполагает: если дальше новый документ будет сохранен без метки

[10] С развитием технологий RFID и GPS, возможно, появится решение, при котором внедренные в каждый носитель радиометки будут сигнализировать о попытках вынести его за пределы хранилища и даже посылать сигналы об их местонахождении.

Анализ проявления источников рисков ИБ в КО

«конфиденциально» – это попытка похищения. Еще не вставлен USB-диск, не сформировано письмо, а система информирует администратора ИБ, который принимает решение: остановить сотрудника или проследить дальнейший путь направления данной информации.

Примерно в таком же объеме необходимо разрабатывать меры по каждому направлению деятельности, входящему в состав комплекса мер по обеспечению ИБ КО, в том числе и для системы ЭБ (см. рисунок).

На примере приведенного анализа источников рисков, связанных с недостатками в обеспечении ИБ системы ЭБ, показано, что все они приводят к возникновению типичных банковских рисков (см. рисунок). Последствия проявления банковских рисков несут определенные убытки, причем не только количественные, которые выражаются в конкретной денежной сумме, но и качественные, которые приводят к падению рейтинга банка, ухудшению отношений с клиентами и деловыми партнерами.

Очевидно, что лучше заранее минимизировать банковские риски путем обдуманного выбора всех необходимых мероприятий для обеспечения ИБ системы ЭБ. Многие источники банковских рисков можно предотвратить при правильной организации всех процессов, входящих в этапы жизненного цикла системы ЭБ[11].

В заключение необходимо отметить, что обеспечение ИБ – процесс непрерывный. Угрозы ИБ не только постоянно изменяются, но и исходят от хорошо подготовленных программистов и специалистов в области информационных технологий. Сегодня многие банки в связи с не самым лучшим периодом в развитии мировой экономики приняли решение о сокращении расходов на обеспечение ИБ, а криминальный мир – наоборот, чувствуя слабость в этой области, ответил «изобретением» новых видов вредоносного кода и способов мошенничества. Поэтому любой банк, стремящийся работать стабильно и иметь хорошую репутацию, должен обеспечить надежную защиту своим информационным ресурсам.

Список литературы

1. *Грень И. В.* Компьютерная преступность. Минск: Новое знание. 2007. 413 с.
2. *Скиба В. Ю., Курбатов В. А.* Руководство от внутренних угроз информационной безопасности. СПб.: Питер. 2008. 320 с.

[11] Речь идет об основных этапах жизненного цикла любой автоматизированной системы: планирование, внедрение, эксплуатация, сопровождение и модернизация. В ряде случаев этих этапов может быть как больше, так и меньше. Все зависит от уровня детализации жизненного цикла системы.