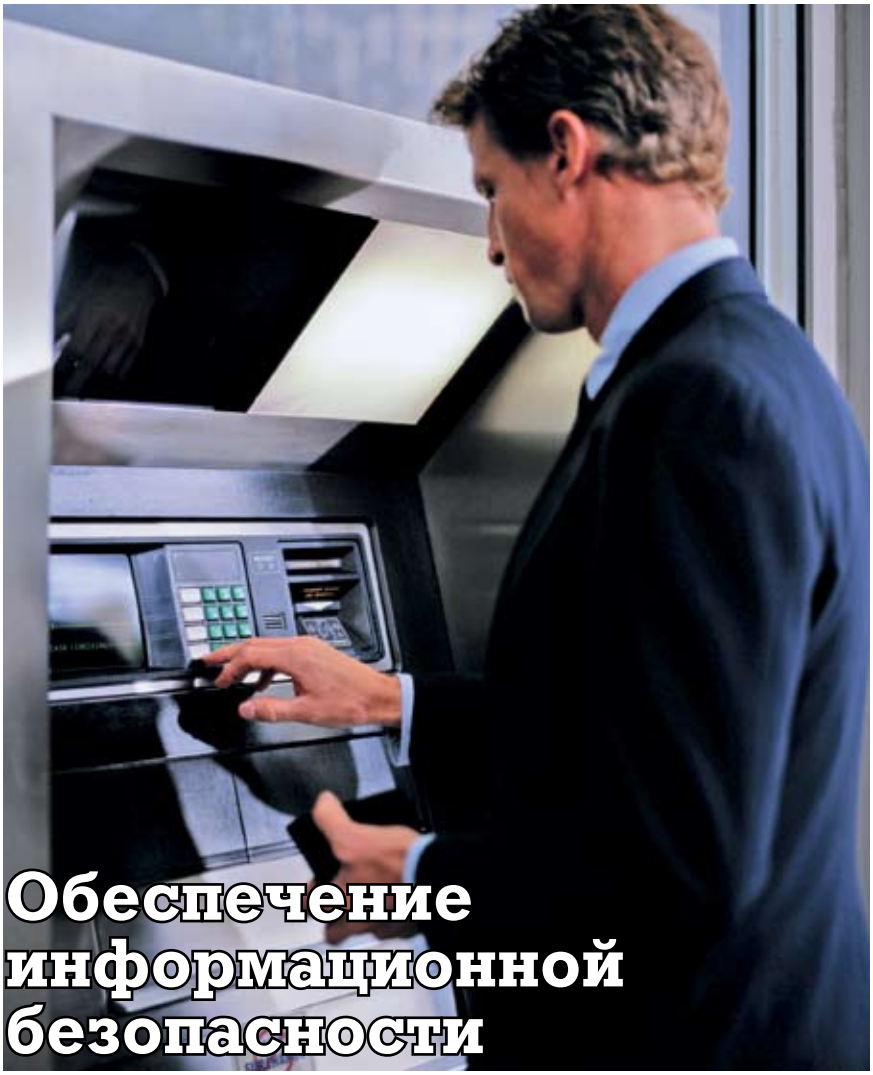

Обеспечение информационной безопасности в условиях интернет-банкинга

Нет большей мудрости, чем своевременность.
Фрэнсис Бэкон

В статье рассматриваются основные угрозы информационной безопасности при использовании в банках систем интернет-банкинга. Приведены рекомендации по предотвращению рассматриваемых угроз, а также положения ряда документов Банка России, имеющих прямое отношение к обеспечению информационной безопасности и поддержанию непрерывности выполнения банковских операций при использовании систем интернет-банкинга.

На протяжении последних 15 лет системы дистанционного банковского обслуживания (ДБО) стали широко применяться в российских кредитных организациях. Их основными достоинствами являются:
• существенная экономия времени за счет исключения необходимости посещать банк лично;
• возможность 24 часа в сутки контролировать собственные счета;
• оперативно реагировать на изменения ситуации на финансовых рынках.

Наиболее востребованным видом ДБО у клиентов является интернет-банкинг, который позволяет управлять своими банковскими счетами и картами через Интернет в режиме on-line. К уже перечисленным выше достоинствам систем ДБО можно добавить то, что работа с ними не имеет привязки к месту — достаточно иметь доступ к Интернету и web-браузер[1].

Во многих зарубежных источниках интернет-банкинг определяют как способ управления своим счетом через Интернет, то есть делается акцент на операционной составляющей. Но если рассматривать интернет-банкинг с позиций риск-фокусированного надзора, то такой подход не будет учитывать весь спектр возможных рисков.

В письме Банка России от 31 марта 2008 г. № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга» (далее — письмо Банка России № 36-Т) дается более полное определение интернет-банкинга: он определяется как способ дистанционного банковского обслуживания клиентов, осуществляемого кредитными организациями в Интернете (в том числе через web-сайт(ы) в Интернете) и включающего информационное и операционное взаимодействие с ними.

Данное определение является более точным, так как учитывает

Ревенков Павел Владимирович — заведующий сектором Департамента банковского надзора Банка России, кандидат экономических наук.

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

не только операционную, но и информационную составляющую данного вида ДБО. Еще совсем недавно (не более 10 лет назад) в России насчитывалось несколько десятков банков, которые использовали свои web-сайты только в маркетинговых целях, предоставляя клиентам информацию относительно банковских услуг и обслуживания (информационный интернет-банкинг). Но и в этом случае уязвимость web-сайтов была чревата для кредитных организаций различными рисками (например, намеренное искажение представляемой информации). В случае информационного интернет-банкинга на web-сайтах кредитных организаций компьютерные злоумышленники могут размещать ссылки на фальшивые web-сайты, созданные с целью выманивания у клиентов кредитных организаций конфиденциальной информации (сведений о состоянии счетов, паролей и номеров кредитных карт и т.д.) (*рис. 1*).

Рисунок 1

Использование фальшивого web-сайта для выманивания данных по кредитным картам

Кредитные организации вынуждены уделять особое внимание гарантиям безопасности и реализовывать комплексную защиту.

В настоящее время почти все банки предоставляют такую услугу, как операционный (транзакционный) интернет-банкинг, в рамках которого клиенты могут управлять своим счетом через Интернет. Этот уровень интернет-банкинга подразумевает наличие непосредственной связи с сервером и внутренней вычислительной сетью банка или обслуживающей его организации (в случае аутсорсинга). По сравнению с информационным интернет-банкингом у операционного риски намного выше. На вооружении кредитных организаций (КО) должны находиться более сложные средства обеспечения информационной безопасности (ИБ), а также действенные планы обеспечения непрерывности выполнения операций, в том числе при возникновении чрезвычайных ситуаций (пожары, наводнения и т.д.)[2].

Приведем основные угрозы ИБ при осуществлении расчетов с помощью систем интернет-банкинга:

- несанкционированный доступ (НСД) к секретной или конфиденциальной информации как банка, так и клиента;
- подмена собой другого лица с целью уклонения от ответственности, отказа от обязательств либо с целью использования прав другого лица для:
  - а) отправки фальсифицированного электронного сообщения (ЭС) на проведение банковской операции;
  - б) искажения имеющейся информации;
  - в) НСД с помощью фальсификации или кражи идентификационных данных или их носителей;
  - г) фальсифицированной авторизации трансакций или их подтверждения;
- уклонение от ответственности за созданные электронные сообщения;
- фальсификация источника ЭС или степени ответственности (например, заявление о получении некоторого ЭС от другого абонента), хотя на самом деле ЭС было создано самим нарушителем;
- предоставление ложных данных о времени отправки или самом факте отправки ЭС;
- отрицание факта получения ЭС или искажение сведений о времени его получения;
- расширение нарушителем своих полномочий (например, на получение доступа к определенным информационным ресурсам банковской автоматизированной

системы (БАС), создание ЭС в системе интернет-банкинга и т.д.);
• несанкционированное создание учетных записей или изменение (ограничение или расширение) полномочий других пользователей системы интернет-банкинга;
• внедрение в линию связи между другими участниками расчетов в системе интернет-банкинга в качестве активного тайного ретранслятора;
• слежение за особенностями информационного обмена и анализ различных характеристик (объекты и субъекты доступа, время доступа и пр.) передаваемых данных;
• дискредитация защищенного протокола информационного взаимодействия, например, путем разглашения сведений, которые, согласно этому протоколу, должны храниться в секрете;
• изменение функций программного обеспечения (обычно с помощью добавления скрытых функций);
• провоцирование других участников информационного взаимодействия в системе интернет-банкинга на нарушение правил обмена электронными сообщениями, например, путем предоставления неправильной информации;
• препятствование взаимодействию других абонентов, например, с помощью организации DoS-атак[3] или прекращение легального сеанса как якобы нелегального и пр.

Предотвратить проявление вышеназванных угроз можно, только имея слаженную систему обеспечения ИБ.

Сравним два способа связи банка с клиентом:
• по коммутируемой линии, приходящей на модемный пул банковского узла связи;
• по IP-протоколу через Интернет.

В первом случае максимально возможное количество подключений ограничивается техническими характеристиками модемного пула, во втором же — возможностями Интернета, которые могут быть существенно выше. Более того, сетевой адрес банка чаще всего является общедоступной информацией, а телефонные номера модемного пула сообщаются, как правило, заинтересованным лицам. Следовательно, открытость банка, чья информационная система связана с Интернетом, значительно выше, чем в первом случае.

Банк России давно определил проблему обеспечения информационной безопасности как одну из основных составляющих стабильности банковской системы.

В таких случаях возникает необходимость пересмотра подходов к обеспечению ИБ банка. Кредитным организациям, предоставляющим доступ к БАС через Интернет, следует заново провести анализ рисков и скорректировать план защиты БАС с учетом новой «модели нарушителя», а также план поддержания непрерывности выполнения банковских операций, ликвидации последствий, возникающих в случае тех или иных нарушений конфиденциальности, сохранности и доступности информации.

Существует два подхода к проблеме обеспечения ИБ: фрагментарный и комплексный.

Фрагментарный подход нацелен на противодействие четко определенным угрозам в заданных условиях. Примерами реализации такого подхода являются отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т.п.

К достоинствам подобного подхода можно отнести высокую избирательность к конкретной угрозе. Однако есть и существенный недостаток — отсутствие единой защищенной среды обработки информации. Фрагментарные меры ИБ обеспечивают защиту конкретных объектов БАС только от конкретной угрозы. Небольшое видоизменение угрозы ведет к потере эффективности защиты.

Комплексный подход ориентирован на создание защищенной среды обработки информации в БАС, объединяющей в единый комплекс различные меры противодействия угрозам ИБ. Организация защищенной среды обработки информации позволяет гарантировать определенный уровень ИБ, что является достоинством комплексного подхода.

К недостаткам комплексного подхода можно отнести:
• определенные ограничения на свободу действий пользователей информационных ресурсов БАС;
• чувствительность к ошибкам установки и настройки средств защиты;
• сложность управления.

Комплексный подход применяют для защиты информационных ресурсов большого или малого объема, но при этом информация имеет особую важность для ее владельца.

Нарушение в обеспечении ИБ кредитных организаций может нанести значительный материальный ущерб не только банкам, но и их клиентам. Поэтому кредитные организации вынуждены уделять особое внимание гарантиям безопасности и реализовывать комплексную защиту. Комплексного подхода придержива-

ется большинство государственных и крупных коммерческих организаций, так как он охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях, и основан на разработанной для конкретной КО политике безопасности, которая регламентирует эффективную работу всех составляющих комплекса мероприятий по обеспечению ИБ в КО.

Надежная система обеспечения ИБ не может быть создана без эффективной политики сетевой безопасности, включая отдельные требования по защите информации, входящей в информационный контур ДБО.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:
• законодательного (стандарты, законы, нормативные акты и т.п.);
• административно-организационного (действия общего характера, предпринимаемые руководством КО, и конкретные меры обеспечения ИБ);
• программно-технического (конкретные технические меры обеспечения ИБ).

Меры законодательного уровня особенно важны для обеспечения ИБ. К этому уровню относится комплекс мер, направленных на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям ИБ. Важно не только запрещать и наказывать, но и учить, разъяснять, помогать сотрудникам, в чьи обязанности входит работа с конфиденциальной информацией. Участники информационного обмена, особенно при осуществлении банковских операций через Интернет, должны осознавать важность данной проблематики, понимать основные пути решения соответствующих проблем[4].

Меры административно-организационного уровня. Руководство КО должно сознавать необходимость поддержания режима безопасности и выделять на эти цели соответствующие ресурсы. Основой защиты административно-организационного уровня является политика безопасности и комплекс организационных мер.

К комплексу организационных мер относятся меры безопасности, реализуемые персоналом КО. Выделяют следующие группы организационных мер:
• управление персоналом;
• физическая защита;
• поддержание работоспособности системы обеспечения ИБ;
• реагирование на нарушения режима безопасности;
• планирование восстановительных работ.

Для каждой группы в каждой КО должен существовать набор регламентов, определяющих действия персонала.

Меры и средства программно-технического уровня не менее важны для поддержания должного уровня ИБ, поскольку основная угроза компьютерным системам исходит от них самих: неисправности и выход из строя оборудования, сбои в работе программного обеспечения, ошибки пользователей, а также администраторов сети и администраторов ИБ и т.п.

В рамках современных информационных систем должны быть доступны следующие механизмы безопасности:
• идентификация и проверка подлинности пользователей;
• управление доступом;
• протоколирование и аудит;
• криптография;
• экранирование;
• обеспечение высокой доступности.

В большинстве случаев банковские автоматизированные системы кредитных организаций построены на основе программных и аппаратных продуктов различных производителей. Сегодня нет ни одной компании-разработчика, которая предоставила бы потребителю полный перечень средств (от аппаратных до программных) для построения защищенной БАС. Для обеспечения в разнородной БАС надежной защиты информации требуются специалисты высокой квалифи-

кации, которые должны отвечать за безопасность каждого входящего в нее компонента: уметь правильно настраивать средства защиты, постоянно отслеживать происходящие изменения, контролировать работу пользователей и т.д. Очевидно, что чем разнороднее БАС, тем сложнее обеспечить ее безопасность. Изобилие в корпоративных сетях и системах устройств защиты, межсетевых экранов, шлюзов и VPN[5], а также растущий спрос на доступ к корпоративным данным со стороны сотрудников, клиентов и заказчиков приводят к созданию сложной среды защиты, которой сложно управлять. Отсюда следует, что принятое банком решение безопасности должно гарантировать защиту на всех платформах (при наличии удаленной филиальной сети) в рамках одной КО. Поэтому вполне очевидна потребность в применении единого набора стандартов как поставщикам средств защиты, так и кредитным организациям.

Рисунок 2

Анализ возможных последствий проявления источника риска, связанного с недостатками в обеспечении информационной безопасности в кредитной организации

Криминальный мир явно активизировался в области компьютерных преступлений, что привело к значительному увеличению вредоносных программ и модификации сетевых атак на информационные ресурсы банков.

Стандарты образуют понятийный базис, на котором строятся все работы по обеспечению ИБ, и определяют критерии, которым должно следовать управление ИБ.

Банк России давно определил проблему обеспечения ИБ как одну из основных составляющих стабильности банковской системы. Начиная с 2004 г. регулятор приступил к выпуску общекорпоративных стандартов по ИБ.

С содержанием стандартов Банка России можно ознакомиться на сайте Сообщества пользователей стандартов Центрального банка Российской Федерации по обеспечению информационной безопасности банковской системы Российской Федерации (Сообщество — ABISS) — www.abiss.ru.

Для специалистов подразделений риск-менеджмента, контроллинга, службы внутреннего контроля и других подразделений, в чьи функции входит управление рисками, вопросы обеспечения ИБ представляют интерес и с точки зрения возникновения дополнительных источников рисков. В определенной степени недостатки в обеспечении ИБ могут мешать эффективному развитию КО, снижать ее конкурентоспособность и надежность, приводить к незапланированным расходам, а также вызывать неуверенность у сотрудников в защите их личных сведений и информации о характере выполняемых ими работ.

Все перечисленные в начале статьи угрозы ИБ по сути своей являются компонентами отдельных типичных банковских рисков [1].

В целом схема анализа возможных последствий проявления недостатков в обеспечении ИБ должна выглядеть следующим образом: факт наличия определенного недостатка, возможные последствия и возникновение ситуации, при которой банк не сможет выполнять свои обязательства перед клиентами (*рис. 2*).

Такие схемы анализа должны быть включены во внутренние методи-

ки КО по оценке рисков, связанных с недостатками в обеспечении ИБ. Для разработки подобных схем анализа целесообразно привлекать аналитиков, сотрудников информационно-аналитического подразделения и службы безопасности.

В заключение хотелось бы отметить, что последствия экономического кризиса привели в ряде кредитных организаций к сокращению финансирования мероприятий, направленных на обеспечение ИБ. В то же время криминальный мир явно активизировался в области компьютерных преступлений, что привело к значительному увеличению вредоносных программ и модификации сетевых атак на информационные ресурсы банков. Очевидно, что противостоять преступлениям такого рода может только адекватная защита, в противном случае потери от компьютерных преступлений могут быть непредсказуемо велики.

ПЭС 11067/23.05.2011

Примечания

1. Web-браузер — приложение на компьютере, которое обеспечивает доступ к web-страницам в Интернете. Web-браузер запрашивает, загружает и отображает web-страницы при переходе с одного интернет-сайта на другой. Сегодня в России самым популярным web-браузером является Internet Explorer.

2. По вопросу поддержания непрерывности и (или) восстановления деятельности КО, нарушенной в результате непредвиденных обстоятельств, Банком России 5 марта 2009 г. было выпущено указание № 2194-У «О внесении изменений в Положение Банка России от 16 декабря 2003 г. № 242-П „Об организации внутреннего контроля в кредитных организациях и банковских группах“», которое содержит рекомендации по структуре и содержанию плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности кредитной организации в случае возникновения непредвиденных обстоятельств.

3. DoS-атака (от англ. Denial of Service — отказ в обслуживании) и DDoS-атака (от англ. Distributed Denial of Service — распределенный отказ в обслуживании) — это разновидность атак на вычислительную систему. Цель этих атак — довести систему до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам либо этот доступ затруднен.

4. В качестве одного из последних примеров разъяснительной работы можно привести письмо Банка России от 2 октября 2009 г. № 120-Т «О мерах безопасного использования банковских карт», в приложение к которому регулятор разработал памятку для держателей банковских карт с описанием основных правил, позволяющих обеспечить максимальную сохранность банковской карты, ее реквизитов, ПИН и других данных. Следование этим правилам позволит снизить возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате товаров и услуг, в том числе через Интернет.

5. VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Источник информации: ru.wikipedia.org.

Использованная литература

1. Письмо Банка России от 23 июня 2004 г. № 70-Т «О типичных банковских рисках».

2. Скиба В.Ю., Курбатов В.А. Руководство от внутренних угроз информационной безопасности. СПб.: Питер, 2008.

3. Грень И.В. Компьютерная преступность. Минск: Новое знание, 2007.

4. Деднев М.А., Дыльнов Д.В., Иванов М.А. Защита информации в банковском деле и электронном бизнесе. М.: КУДИЦ-Образ, 2004.

5. Ревенков П.В., Дудка А.Б., Сычев А.М., Пеленицын А.М. Электронный банкинг. М.: Издательский дом «Регламент», 2009.