КРУГЛЫЙ СТОЛ

Дистанционное банковское обслуживание в свете информационной безопасности

В практику деятельности российских банков стремительно входят системы дистанционного банковского обслуживания (ДБО) клиентов. Как обеспечить безопасность ДБО? Как повысить доверие пользователей к таким системам? Эти и другие вопросы обсуждались на «круглом столе» во время конференции «Информационная безопасность. Региональные аспекты». Организатор конференции «Академия Информационных Систем». В рамках «круглого стола» удалось собрать представителей служб защиты информации ведущих банков, поставщиков решений, представителей ассоциаций, в чью деятельность входят вопросы ИБ. Ведущий «круглого стола» – коммерческий директор компании Aladdin Алексей Сабанов.

В круглом столе принимают участие

Александр ВЕЛИГУРА,
председатель Комитета по информационной безопасности Ассоциации российских банков, заместитель генерального директора ООО «Андэк Технолоджиз», кандидат физ.-мат. наук, CISA

Вячеслав ГОРБАТЕНКОВ,
начальник отдела развития и обеспечения электронного документооборота Национального депозитарного центра

Андрей ГРИЦИЕНКО,
начальник службы информационной безопасности Банка «Возрождение», к. т. н.

Игорь КАЛАЙДА,
вице-президент Ассоциации «ЕВРААС»

Владимир МАМЫКИН,
директор по информационной безопасности компании Microsoft

Юрий МАСЛОВ,
коммерческий директор компании «КРИПТО-ПРО»

Владимир СКИБА,
начальник отдела информационной безопасности Федеральной таможенной службы, к. т. н.

Дмитрий СУШКОВ,
главный специалист по информационной безопасности Информационно-аналитического управления ОАО КБ «Агроимпульс»

Алексей САБАНОВ,
к. т. н., коммерческий директор ЗАО «Аладдин Р.Д.»

АЛЕКСЕЙ САБАНОВ

«Пока гром не грянет, мужик не перекрестится» – так издавна работает принцип защиты информации в российских условиях. В последнее время участились атаки на системы ДБО, и лишь после того, как убытки начинают быть ощутимыми, банки начинают задумываться о способах защиты этого вида бизнеса. Защита всегда ограничивает функционал. Где должна лежать грань разумного использования средств защиты? Какие рекомендации дает недавно принятый Стандарт Банка России? Как их выполнять? Надо ли следовать только этим рекомендациям или применять другие подходы? Итак, первый вопрос.

В области информационной безопасности организаций банковской системы в начале 2006 г. Банком России был принят специальный стандарт. Насколько требования этого стандарта практически реализуемы? Какие шаги нужны для их выполнения?

АНДРЕЙ ГРИЦИЕНКО

Требования ЦБ РФ постоянно возрастают, и в дополнение к разработанным и рекомендованным стандартам до конца года готовятся еще два: по оценке операционных рисков и переработанная версия стандарта СТО БР ИББС-1.0. В частности, если банк использует в своей деятельности криптографические средства, он обязан иметь лицензию ФСБ. Выдавая эту лицензию, ФСБ обращает внимание именно на системы ДБО, включающие подсистемы классического «толстого» банк-клиента и «тонкого» интернет банк-клиента.

Особенно активно используется классический банк-клиент: один только наш удостоверяющий центр выпустил 35 000 тыс. сертификатов – это примерно

20 тыс. активных пользователей ДБО. Вопросов два – какие криптографические средства и какие ключевые носители оптимально использовать? Как показала наша практика, целесообразно использовать только сертифицированные средства криптографической защиты и ключевые носители.

АЛЕКСАНДР ВЕЛИГУРА

Рекомендации стандарта направлены в первую очередь на организацию процессов управления – создание системы менеджмента информационной безопасности. Как показывает опыт оценки соответствия состояния ИБ требованиям стандарта, ничего невыполнимого в этих рекомендациях нет. Хочется обратить внимание на критерии выполнения. Если в качестве таковых использовать другой стандарт Банка России – СТО БР ИББС-1.2-2007 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2006», то уровень соответствия может быть разным. Этим стандарты Банка России отличаются от некоторых других стандартов, где предусмотрено только два варианта – «соответствует» или «не соответствует».

ДМИТРИЙ СУШКОВ

В стандарте Банка России СТО БР ИББС-1.0-2006 учтены основные положения международных стандартов по управлению информационной безопасностью и уникальный зарубежный опыт работы в этой области. С выходом в свет в мае 2007 г. дополнительных стандартов и методических рекомендаций по обеспечению информационной безопасности организаций банковской системы процесс внедрения основного стандарта СТО БР ИББС-1.0-2006 в банковском секторе стал прозрачным и более понятным. Наличие стандарта Банка России позволяет сформировать единые подходы, требования и принципы деятельности в сфере информационной безопасности, выработать унифицированный алгоритм деятельности лиц, ответственных за ее обеспечение.

ВЛАДИМИР МАМЫКИН

Вопросы безопасности, поднимаемые в связи с ДБО, существенны не только для банков, но и для крупных и средних компаний, для государственных структур и т. д. Но не стоит забывать и о частных пользователях, которые пользуются электронным банкингом. По ряду объективных и субъективных причин у них нет полного доверия к интернет-банкингу. Клиент-банк воспринимается как более надежный инструмент, и его пользователями часто становятся владельцы мелких компаний. Однако проблема в том, что поскольку в этих системах применяется криптография, пользователи обязаны предоставить проверяющим органам доступ к своему рабочему месту. С другой стороны, не должны проверяющие органы нести ответственность за то, что у частного пользователя возникли проблемы из-за отсутствия доверенной среды. На мой взгляд, по данному вопросу необходимо договориться регулирующим и проверяющим органам. И позволить частному пользователю самостоятельно определять свои риски и нести за них ответственность.

Система удаленного банковского обслуживания могла бы принести банкам существенную выгоду. Однако сегодня пропаганда такой формы обслуживания либо недостаточна, либо вовсе отсутствует. Кроме того, большинство пользователей просто не понимает половины терминов, используемых в договоре. Необходимо предоставлять информацию в доступной форме.

ВЯЧЕСЛАВ ГОРБАТЕНКОВ

Различные системы ДБО примерно одинаковы по структуре. Такие системы используются и в Национальном депозитарном центре (НДЦ), только связаны они с депозитарными операциями (транзакциями) ценных бумаг. К сожалению, у клиентов возникает немало претензий в связи с тем, что им приходится работать с разными ДБО – банка, НДЦ и т. д. Сложность в том, что применяются разные криптографические средства и ключи, поскольку владельцы этих систем ориентируются на продукты определенных производителей. А разные средства криптозащиты не стыкуются друг с другом, потому что отсутствует кросс-сертификация между удостоверяющими центрами.

На мой взгляд, создание единых требований для всех компаний – производителей средств защиты – дело соответствующих регулирующих органов. Но при этом важно не «зарегулировать» вопрос до мелочей, а именно выработать общие требования. Это позволило бы ликвидировать существующий на рынке хаос.

Кроме того, сегодня регулятором системы ДБО фактически является тот, кто ее организует. Вопросы же, касающиеся входа в систему, использования тех или иных средств криптозащиты, прописываются в соответствующих договорах. Но при этом не существует определений, общих для многих систем. У каждого регулятора системы ДБО свое понятие об ЭЦП, о форматах используемых документов и т. д. Сейчас основными задачами являются: превращение электронной сегментированной в данное время инфраструктуры финансового рынка в единую гибкую систему информационного взаимодействия со своим правилами, форматами, взаимно-интегрированными программными средствами обработки и защиты информации; осуществление на первом этапе кросс-сертификации ключей ЭЦП, сертифицированных различными удостоверяющими центрами; создание и использование на втором этапе единого для всех участников финансового рынка удостоверяющего центра.

ИГОРЬ КАЛАЙДА

Есть пример эффективного подхода к аналогичной проблеме при реализации Закона «О Бюро кредитных историй», инициатором которого стала Ассоциация российских банков. Поэтому имеет смысл договариваться с производителями средств защиты через АРБ, используя тот же механизм. У Ассоциации достаточно возможностей для этого, как и для организации диалога с регулирующими и контролирующими органами.

АЛЕКСЕЙ САБАНОВ

Конструктивной представляется идея проведения семинаров на базе ФСТЭК. Такой опыт уже есть.

Должны ли применяемые финансово-кредитными организациями средства защиты быть промышленными и основанными на открытых стандартах? Следует ли публиковать информацию о них, чтобы повысить доверие пользователей?

АНДРЕЙ ГРИЦИЕНКО

Несомненно, необходимо использовать только надежные промышленные

средства и публиковать информацию о них. Клиент должен знать, какие криптографические средства и ключевые носители использует банк.

АЛЕКСАНДР ВЕЛИГУРА

Да, должны, к этому нужно стремиться. Стремление должно, на мой взгляд, выражаться и в разработке некоторых стандартов. По поводу публикации – на усмотрение кредитной организации, но я считаю, что следует.

ДМИТРИЙ СУШКОВ

Я сторонник применения сертифицированных средств защиты информации в столь важном секторе экономики, как банковский. Ответственность, которую несут банки за сохранность персональных данных о клиентах, их счетах и т. д., требует применения сертифицированных средств защиты информации, разработанных и созданных в промышленных условиях. Использование не сертифицированных средств защиты информации, тем более не стандартизированных, влечет за собой риск утечки (утраты, искажения) информации, как за счет не декларированных возможностей, так и за счет иных свойств и особенностей применяемых средств защиты. Одним словом, средства защиты информации должны быть сертифицированы по требованиям информационной безопасности и обеспечивать гарантированную отказоустойчивость и минимизацию риска утечки (утраты, искажения) защищаемой информации. Что касается публикаций в открытых источниках информации сведений о применяемых средствах защиты, то они не могут служить инструментом повышения доверия со стороны клиентов и партнеров, которым, по сути, безразлично, с помощью каких средств и технологий осуществляется защита их информации в кредитной организации, которой они доверили свои сбережения и персональные данные. Мощным стимулом для сотрудничества с кредитной организацией, привлечения дополнительных инвестиций может служить только наличие у нее сертификата соответствия системы управления информационной безопасностью стандарту Банка России СТО БР ИББС-1.0-2006 или международному стандарту ISO/IEC 27001.

Сегодня практически в каждом гипермаркете открыты точки кредитования покупателей, которые находятся в «недоверенной среде». Как обеспечить необходимый уровень ИБ для таких точек? За счет чего можно повысить доверие потребителей к данной услуге?

ВЛАДИМИР МАМЫКИН

Если покупатель получил в супермаркете деньги в кредит, и это документально зафиксировано, то ему безразлично, какие у банка могут возникнуть проблемы с передачей информации. А для банка проблема ничем не отличается от проблемы обеспечения удаленного доступа сотрудников к корпоративным ресурсам с помощью, например, ноутбука и сети Wi-Fi.

АЛЕКСЕЙ САБАНОВ

Однако при этом передаваемые с точки кредитования персональные данные могут попасть «не в те руки».

АНДРЕЙ ГРИЦИЕНКО

В такой ситуации клиенту нужно четко понимать, на каких условиях он эти деньги получил. А проблема банка – обеспечить как защиту информации внутри банка, так и при передаче по каналам связи.

Это проблема обеспечения защищенного доступа. Мы решаем эту задачу с помощью «Крипто-Про» и eToken. В результате с любого рабочего места организуется доступ к централизованному ресурсу через VPN-соединение. При этом все важные данные и программы хранятся в центре.

Но точки кредитования – не очень большая проблема. Намного серьезнее проблемы применения клиент-банка, использования шифровальных средств и разбора конфликтных ситуаций. Последний вопрос наиболее сложный. Ведь по договору о клиент-банкинге ФСБ имеет право прийти с проверкой к любому клиенту.

ВЛАДИМИР СКИБА

Использование средств криптографической защиты предполагает выполнение клиентом ряда требований ФСБ России, предусматривающих, в том числе, проведение тематических исследований в специализированных организациях, имеющих соответствующие лицензии ФСБ России. Кроме того, выполнение всех требований, связанных с обеспечением безопасности информации, предполагает аттестацию рабочих мест клиента по требованиям ФСТЭК России. Либо клиент должен брать на себя ответственность за риски. Целесообразно организовать более удобную схему аттестации участников процесса, пока эта процедура очень сложная.

А клиенту следует очень внимательно читать договор, чтобы действия сторон в случае конфликтных ситуаций были для него прогнозируемы.

С аналогичными проблемами мы (таможенные органы) столкнулись при внедрении декларирования товаров в электронной форме.

АНДРЕЙ ГРИЦИЕНКО

Договор клиент-банкинга вместе с регламентом – один из самых сложных документов, его объем – около 40 страниц. Потому-то интернет-банкинг для физических лиц не скоро наберет популярность.

Каким требованиям должны отвечать средства информационной безопасности, используемые при ДБО?

АЛЕКСАНДР ВЕЛИГУРА

Аргументированный ответ на этот вопрос требует определения угроз, которые предполагается парировать, и зависит, в частности, от технологии ДБО. Поэтому хорошей практикой было бы, чтобы те, кто предлагает средства ДБО (производители) и услуги ДБО (кредитные организации), указывали, в каких предположениях вводились те или иные меры и средства безопасности.

АНДРЕЙ ГРИЦИЕНКО

Есть три принципиальных условия: сертифицированный ключевой носитель, сертифицированное криптографическое средство, изготовление ключей на стороне клиента. Невыполнение хотя бы одного из них чревато серьезными рисками.

По опыту банка «Возрождение», ключевой носитель должен быть сертифицирован и должна существовать гарантия того, что ключи из него извлечь невозможно. Соблюдение этих требований уже помогало нам в решении конфликтных ситуаций.

ЮРИЙ МАСЛОВ

На основании нашего опыта разбора конфликтных ситуаций можно утверждать, что если в результате использования ЭЦП необходимо иметь юридическую значимость с правовыми последствиями совершенной операции, то следует использовать ключевые носители типа eToken или смарт-карт. Применение ключевого носителя типа eToken или смарт-карты исключает возможность доступа к хранящимся в них ключам и сертификатам. Они ориентированы лишь на три попытки подбора PIN-кода, после чего он будет заблокирован. И если ключи инициировать, постороннее лицо сможет получить доступ, только вступив в сговор с владельцем.

При использовании других носителей риск доступа к системе постороннего лица существует. И теперь, если клиенту требуется юридическая значимость ЭЦП, мы не рекомендуем использовать дискеты.

В случае конфликтной ситуации назначается экспертиза с целью доказательства принадлежности ЭЦП. По закону инструмент проведения экспертизы должен иметь сертификат, как и само средство защиты. У «Крипто-Про» такой инструмент есть.

Стандарт Банка России носит рекомендательный характер. Каковы могут быть мотивы для выполнения его требований?

ДМИТРИЙ СУШКОВ

На мой взгляд, основными мотивами для внедрения стандарта Банка России СТО БР ИББС-1.0-2006 в кредитных организациях служат:

- повышение эффективности и управляемости.

  Внедряя систему информационной безопасности, реализующую положения стандарта Банка России, банк создает предпосылки для обеспечения гарантированной непрерывности бизнес-процессов, минимизации возможного ущерба за счет снижения внутренних и внешних угроз информационной безопасности;
- оптимизация управления операционными рисками.

  Банк, внедривший эффективную систему информационной безопасности в соответствии с положениями стандарта Банка России, решает тем самым основную массу проблем, связанных с управлением операционными рисками;
- поддержание имиджа кредитной организации.

  Грамотно построенная и четко функционирующая система информационной безопасности во многом позволяет избежать инцидентов, способных ухудшить имидж банка, а сам факт совместимости со стандартом Банка России служит веским доводом в пользу сотрудничества с такой кредитной организацией.

АЛЕКСАНДР ВЕЛИГУРА

Управление рисками в деятельности банков, например, для достижения соответствия требованиям Базеля II, включает в себя управление информационной безопасностью. В решении многих вопросов большую помощь могут оказать стандарты Банка России как база для выстраивания всего процесса и применения рекомендаций других документов, в том числе международных, зарубежных и российских стандартов информационной безопасности.

В подтверждение этого приведу небольшую цитату из п. 5.15 стандарта СТО БР ИББС-1.0-2006:

«...Требования настоящего стандарта к СМИБ для организаций БС РФ имеют прикладную практическую направленность, определяющую условия, цели и задачи применения в организациях БС РФ высокоуровневых международных стандартов для СМИБ организаций». Организация этой работы – задача высшего руководства банков.

АЛЕКСЕЙ САБАНОВ

Стоит заметить, что мотив к использованию стандарта для руководителей вытекает из оценки рисков: каковы будут штрафные санкции и кому придется нести ответственность.

АНДРЕЙ ГРИЦИЕНКО

Хочу обратить внимание на то, что клиент-банк – та область деятельности, где очень легко попасть под уголовное или административное преследование, например, в случае отсутствия лицензий на работу с криптографическими средства.

В случае разбора конфликтных ситуаций в суде судебное разбирательство начинается с выяснения – сертифицировано ли средство ЭЦП. Если нет, суд не принимает это дело к рассмотрению. В противном случае вы попадаете под действие Федерального закона «О лицензировании отдельных видов деятельности».

ЮРИЙ МАСЛОВ

Применение ЭЦП регулируют 11 федеральных законов и постановлений Правительства, более 50 нормативных ведомственных актов, не считая писем Минфина и Федеральной налоговой службы. Причем большинство писем появилось примерно в 2005 г., после ряда судебных процессов.

АЛЕКСЕЙ САБАНОВ

Итак, подводя итоги, можно констатировать следующее. Выполнять требования Стандарта Банка России весьма непросто, хотя и нужно. И для этого необходимо договориться с различными производителями средств защиты об унифицированных стандартах.

Нужно применять открытые стандарты средств защиты, чтобы повысить доверие пользователей.

Ответственность за точки кредитования и вопросы, связанные с их работой, ложатся на банк.

И, наконец, нужно использовать только сертифицированные средства аутентификации и сертифицированные носители.

И, наконец, мотивы к использованию стандарта для руководства кредитно-финансовых учреждений следующие:

- Требования настоящего стандарта к СМИБ для организаций БС РФ имеют прикладную практическую направленность, определяющую условия, цели и задачи применения в организациях БС РФ высокоуровневых международных стандартов для СМИБ организаций.
- Использование стандарта Банка России повышает эффективность и управляемость бизнеса, оптимизирует управление операционными рисками, положительно влияет на имидж кредитной организации.
- Риски, которые берет на себя руководство кредитно-финансовых учреждений, не поддерживая инициативы ЦБ РФ, направленные на стабилизацию банковской системы в России. ■