УРОВЕНЬ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА КАК КЛЮЧЕВОЙ ПОКАЗАТЕЛЬ КАЧЕСТВА СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

А.Н. Визгунов,
доцент кафедры информационных систем и технологий факультета бизнес-информатики и прикладной математики нижегородского филиала Государственного университета — Высшей школы экономики, e-mail: Arseniy.Vizgunov@gmail.com.
Ар.Н. Визгунов,
научный сотрудник научно-учебной лаборатории теории и практики систем поддержки принятия решений факультета бизнес-информатики и прикладной математики нижегородского филиала Государственного университета – Высшей школы экономики, e-mail: Arseniy.Vizgunov@gmail.com
Адрес: 603155, г. Нижний Новгород, ул. Б. Печерская, 25/12.

Статья посвящена анализу направлений повышения уровня информационной безопасности в рамках систем дистанционного банковского обслуживания. Рассматриваются достоинства и недостатки различных технологических решений, призванных обеспечить высокий уровень безопасности при работе в системе. Авторами предлагается комплексный подоход к обеспечению информационной безопасности, противодействия широкому спектру угроз различного рода.

Ключевые слова: система безопасности банка, системы удаленного доступа, информационная безопасность, криптозащита, пароль, токен, троян, компьютерный вирус.

В настоящее время ключевой проблемой в сфере дистанционного банковского обслуживания является обеспечение безопасности работы в системе. В 2008-2009 годах существенно возросло количество преступлений, связанных с хищением денежных средств через системы дистанционного банковского обслуживания (ДБО). Например, в сентябре 2008 года было организовано хищение средств со счетов клиентов системы Интернет-Банк faktura.ru. В этот период «было зафиксировано 27 попыток проведения мошеннических операций в системе. Удалось предотвратить 17 из них 10 операций предотвратить не удалось. Пострадали клиенты 5 банков. Общая сумма ущерба составила 2 180 000 рублей» [1]. Число подобных преступлений постоянно растет. В частности, в Свердловской области, по оценкам экспертов, количество преступлений, связанных с хищением денежных средств через Интернет в мае-июне 2008 года «выросло по сравнению с аналогичным периодом предыдущего года примерно на 60 процентов» [2].

Злоумышленники получают доступ к счетам путем хищения у клиентов ключей электронной цифровой подписи (ЭЦП) и паролей доступа к системе. Иным способом получить доступ к секретному ключу не представляется возможным. В большинстве систем ДБО используется механизм ЭЦП на базе криптографического алгоритма, соответствующего стандарту ГОСТ Р 34.10-2001. В соответствие с ним длина закрытого (секретного) ключа составляет 256 бит, что обеспечивает практическую невозможность подбора ключа. Важно отметить, что секретный ключ ЭЦП не передается клиентом в банк. Банк получает от клиента только открытый ключ, который используется для проверки корректности ЭЦП. При этом на основе открытого ключа технически невозможно определить секретный ключ.

Хищение ключей ЭЦП выполняется одним из следующих способов [3]. В первом случае ключ копируется сотрудником организации, работавшим с системой криптозащиты. Обычно хищение выполняется злоумышленниками, которые принадлежат к одной из следующих групп:

- ✦ владельцы электронных ключей, уволенные из организации (менеджеры, бухгалтера),
- ✦ работавшие в организации IT-специалисты, задействованные в процессе обслуживания системы дистанционного обслуживания,
- ✦ нештатные, приходящие по вызову IT-специалисты, задействованные в процессе обслуживания системы ДБО.

Второй распространенный способ хищения – заражение компьютеров клиентов троянскими программами, обеспечивающими пересылку ключевой информации злоумышленнику. Важно отметить, что троянские программы позволяют злоумышленнику получить как данные секретного ключа, так и пароли доступа, вводимые с клавиатуры.

В договоре, заключаемом клиентом с банком, обычно предусматривается, что в том случае, если несанкционированный доступ к системе произошел не по вине банка, вся ответственность за убытки, связанные с хищением средств со счета через систему ДБО, возлагается на клиента. Для того, чтобы минимизировать риски возможных потерь, клиент должен выполнять требования безопасности, предусмотренные в договоре. Однако выполнение этих требований в полном объеме может быть для клиента трудновыполнимой задачей. Например, в том случае, если антивирусное ПО, используемое клиентом, не определяет троянскую программу, с помощью которой может быть выполнено хищение ключевой информации.

По мнению ряда российских и зарубежных экспертов, ситуация, при которой ответственность за убытки, связанные с хищением средств через систему ДБО, возлагается на клиента, не способствует защите интересов клиента. В частности, в 2008 году Комитет по Науке и Технике Палаты лордов Великобритании опубликовал отчет по интернет-безопасности, в котором отмечается, что банки не предлагают клиентам достаточной защиты от потерь. По мнению авторов отчета, улучшить безопасность интернет-банка можно только вынудив банки принимать на себя ответственность [4].

В этих условиях уровень защищенности системы ДБО становится для клиентов одним из ключевых показателей качества системы. На наш взгляд, совершенствование системы безопасности ДБО является одной из приоритетных задач и для банка, поскольку в случае хищения средств может пострадать репутация кредитной организации.

Необходимость принятия дополнительных мер, связанных с повышением уровня безопасности в рамках систем ДБО, отмечается и в документах Банка России. В частности, в Письме ЦБР от 7 декабря 2007 г. N 197-Т «О рисках при дистанционном банковском обслуживании» Банк России «обращает внимание кредитных организаций на необходимость распространения предупреждающей информации для своих клиентов, в том числе с использованием представительств в сети Интернет (web-сайтов), о возможных случаях неправомерного получения персональной информации пользователей систем ДБО» [5]. Проблема повышения уровня безопасности в рамках систем ДБО рассматривается также в следующих документах Банка России: Письме ЦБР № 11-Т от 30.01.2009 «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга», Письме ЦБР от 31 марта 2008 г. N 36-Т «О Рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга» и др. Существенное внимание данной проблеме уделено в Стандарте Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [6]

Рассмотрим возможные направления развития системы информационной безопасности ДБО. На наш взгляд, можно выделить два направления раз-

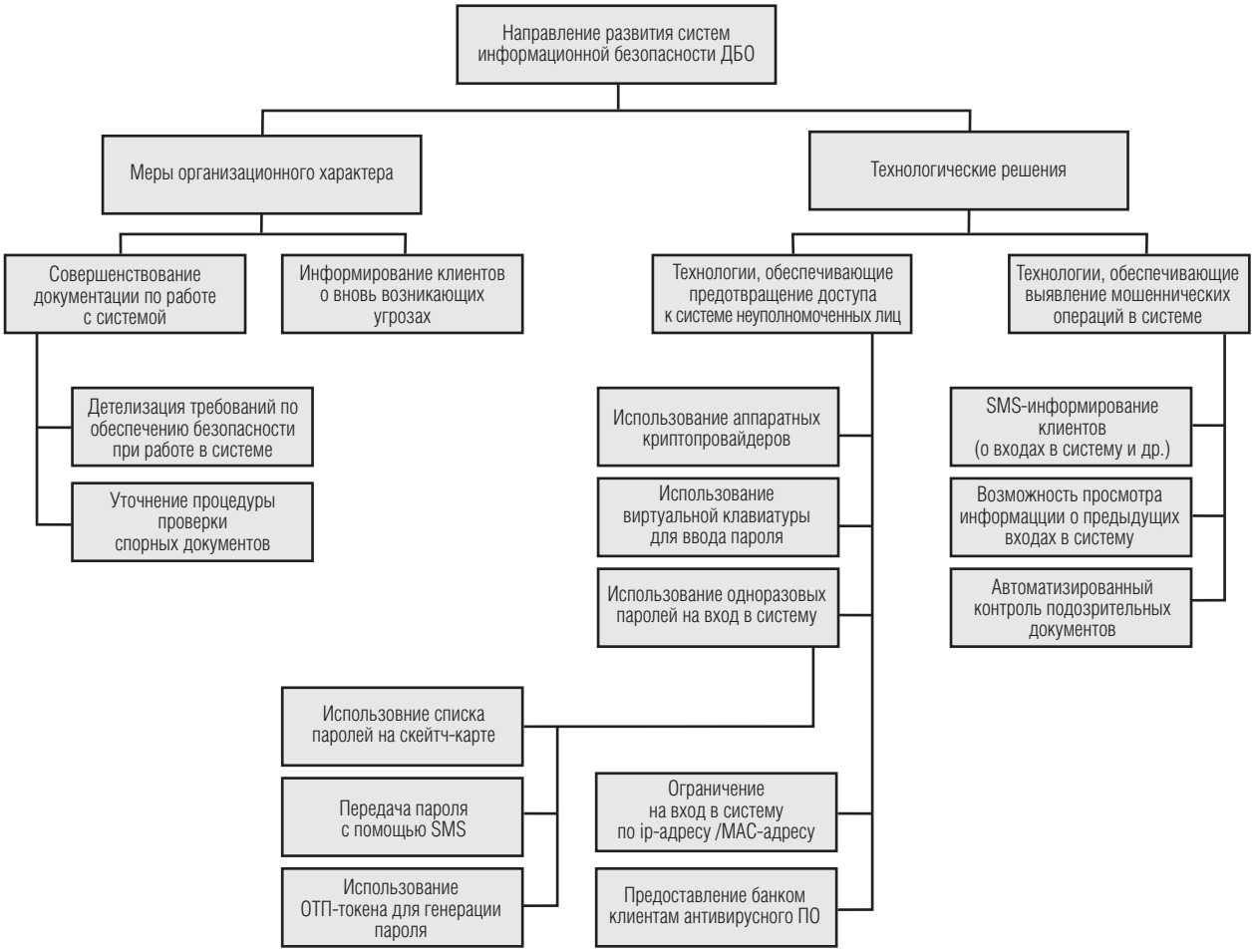

Рис.1. Направления развития системы информационной безопасности ДБО

вития системы информационной безопасности ДБО *(рис. 1)*:

✦ меры организационного характера, включающие совершенствование нормативной документации, организацию оперативного информирования клиентов об угрозах, связанных с обслуживанием в системе, и т.д.

✦ внедрение новых технологических решений, обеспечивающих более высокий уровень безопасности.

Рассмотрим подробнее возможные пути реализации указанных мер.

1. Мероприятия организационного характера.

Мероприятия организационного характера связаны, в первую очередь, с информированием клиентов о возможных рисках, возникающих при работе с системой ДБО: какие факторы обуславливают возникновение риска, каким образом клиент может минимизировать уровень риска, какие действия должны выполняться клиентом при реализации риска и т.п. На наш взгляд, наиболее важные мероприятия организационного характера можно разделить на две группы:

✦ Совершенствование документации по работе с системой (договора на обслуживание в системе, пользовательских инструкций и т.п.)

✦ Оперативное информирование клиента о вновь возникающих угрозах.

1.1. Совершенствование документации по работе с системой.

Важнейшим направлением совершенствования документации является детализация требований по обеспечению безопасной работы в системе, и, прежде всего, требований, связанных с использованием клиентом средств криптографической защиты информации (СКЗИ). В документах, передаваемых банком клиенту, должно быть уделено внимание следующим ключевым вопросам:

■ Порядок формирования клиентом секретного

ключа и получения сертификата, а также порядок смены ключей. В документации целесообразно указать, что сотрудники банка в процессе формирования сертификата, а также при оказании услуг, связанных с настройкой клиентского ПО, не должны получать доступа к секретному ключу клиента (секретный ключ не должен передаваться в банк).

■ Требования, связанные с ограничением доступа к автоматизированным рабочим местам, на которых эксплуатируется СКЗИ. Эти требования, на наш взгляд, должны определять:

✧ ограничения, связанные с физическим доступом к АРМ (примеры требований – требование размещения АРМ с СКЗИ только в помещениях, обеспечивающих невозможность несанкционированного доступа к СКЗИ, требование использования аппаратных средств защиты информации от НСД – так называемых «электронных замков» и т.п.),

✧ ограничения, связанные с доступом по сети (например, требование использования межсетевых экранов).

■ Требования, связанные с ограничением доступа к носителям ключевой информации (примеры требований – запрет хранения секретных ключей на жестком диске компьютера, требование, определяющее, что носитель ключевой информации должен храниться в сейфе и т.п.)

■ Порядок использования антивирусного ПО (требования использования только лицензионного ПО, своевременного обновления ПО; также могут быть представлены рекомендации по критериям выбора программного продукта).

■ Описание ситуаций, при которых возникает компрометация ключа, а также действий, которые должны выполняться клиентом в случае компрометации ключа. Под компрометацией ключа понимается утрата доверия к тому, что используемый секретный ключ недоступен посторонним лицам К событиям, связанным с компрометацией ключей, могут быть отнесены следующие:

✧ утрата носителей ключевой информации;

✧ увольнение сотрудников, имевших доступ к ключевой информации;

✧ временный доступ посторонних лиц к ключевой информации и др.

Также к событиям, связанным с компрометацией ключей, может быть отнесено и обнаружение вирусов на компьютере клиента.

■ Порядок исполнения банком документов, поступающих по системе ДБО, а также порядок отзыва документа клиентом (должны быть указаны сроки исполнения межбанковских и внутрибанковских документов, статусы документов, для которых возможна операция отзыва, сроки отзыва документов и т.п.). Знание этой информации может позволить клиенту своевременно отозвать ошибочный документ или документ, отправленный злоумышленником.

Кроме того, в документации должно быть также уделено особое внимание процедуре проверки спорного документа. В том случае, если произошло хищение средств со счета, необходимо выяснить, корректна ли ЭЦП документа. От этого во многом зависит, несет ли банк ответственность за убытки клиента. Описание процедуры проверки документа должно быть детальным и не допускать разночтений. Федеральный закон «Об электронной цифровой подписи» определяет, что «электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий: сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания; подтверждена подлинность электронной цифровой подписи в электронном документе; электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи» [7].

Проверка ЭЦП документа обычно производится экспертной комиссией, в которую должны входить представители клиента и банка. Также к работе экспертной комиссии могут привлекаться эксперты – представители фирмы-разработчика СКЗИ.

Одна из возможных схем реализации процедуры проверки ЭЦП представлена *на рис. 2.* Представленный на данной схеме процесс проверки ЭЦП состоит из следующих этапов.

✦ Подтверждение подлинности ПО проверки ЭЦП документа. Если фирма-разработчик СКЗИ предоставляет в составе СКЗИ отдельную программу для проверки корректности ЭЦП документа, то на первом этапе проверки подписи необходимо определить подлинность этой программы. Для этого может использоваться, например, утилита контроля целостности, обеспечивающая вычисление криптостойкой хэш-функции для произвольного файла (если такая утилита поставляется разработчиком в составе СКЗИ и используется клиентом

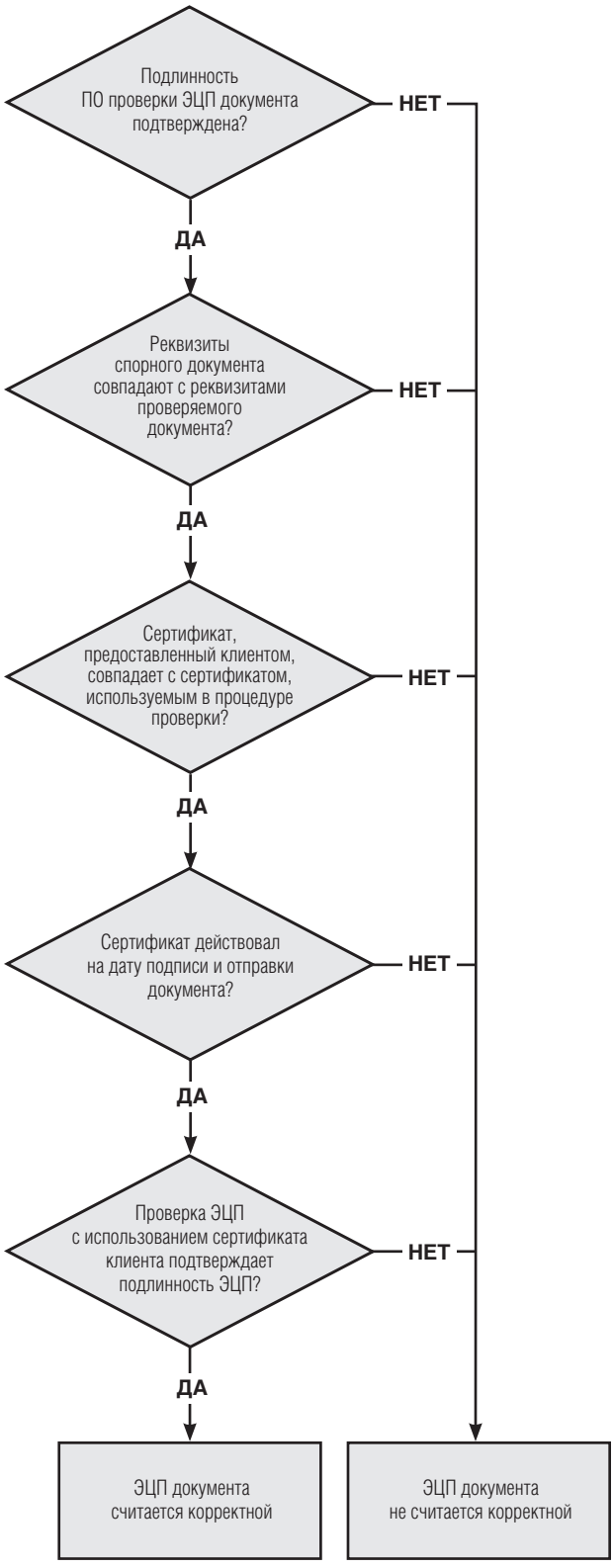

Рис.2 Возможная схема реализации процедуры проверки ЭЦП спорного документа

для контроля целостности ПО СКЗИ). Фирма-разработчик СКЗИ должна передать банку документ с указанием значения хэш-функции, рассчитанной для программы проверки ЭЦП. В процессе работы экспертной комиссии для программы проверки ЭЦП рассчитывается значение хэш-функции и сверяется со значением хэш-функции, представленной фирмой-разработчиком СКЗИ. Если значения совпадают, программа проверки ЭЦП может считаться подлинной.

✦ Контроль реквизитов проверяемого документа. На данном этапе документ выгружается из БД системы ДБО; контролируется соответствие реквизитов выгруженного документа реквизитам спорного документа, представленного клиентом.

✦ Контроль сертификата клиента. На данном этапе осуществляется сверка данных сертификата клиента, хранящегося в банке и используемого для проверки ЭЦП, и сертификата клиента, хранящегося у клиента. После сверки данных необходимо уточнить, не истек ли срок действия сертификатов на дату создания и отправки документа в банк. Другой вопрос – не был ли сертификат на эту дату включен в список отмененных сертификатов.

✦ Проверка ЭЦП документа. На данном этапе с помощью программы проверки ЭЦП выполняется проверка ЭЦП документа (входными данными для программы являются данные документа, ЭЦП документа, сертификат клиента). Если ЭЦП некорректна, значит, банк допустил ошибку, приняв к обработке документ, и, следовательно, несет ответственность за убытки клиента.

1.2. Оперативное информирование клиента о вновь возникающих угрозах.

Эффективным способом повышение уровня безопасности работы в рамках системы ДБО является оперативное информирование клиентов банка о вновь возникающих угрозах и способах борьбы с ними. Информация может выкладываться на сайте системы, либо сообщаться клиентам путем личных контактов. В качестве примера эффективного информирования клиентов можно привести информационное сообщение, выложенное на сайте одного из банков [8]. В нем рассматривается вопросы, связанные с компрометацией конфиденциальных данных пользователей систем он-лайн банкинга в результате атаки компьютеров пользователей вирусами-троянами «Sinowal», «Banker». Важно отметить, что в сообщении не только представлена информация о способах заражения вирусами и последствиях за-

ражения, но и указан ряд антивирусных программ, определяющих данные вирусы *(табл. 1)*.

Таблица 1.

Антивирусные средства, определяющие вирусы «Sinowal» и «Banker»

Антивирус	Номер версии	Сигнатура вируса
«Sinowal»		
AhnLab-V3	2008.2.27.0	Win-Trojan/MBRtool
AntiVir	7.6.0.67	TR/PSW.Sinowal.GJ.20
Avast	4.7.1098.0	Win32:Sinowal
AVG	7.5.0.516	PSW.Sinowal.C
CAT-QuickHeal	9.50	TrojanPSW.Sinowal.gj
DrWeb	4.44.0.09170	Trojan.PWS.Snap.310
eSafe	7.0.15.0	Win32.Sinowal.gj
Fortinet	3.14.0.0	W32/Sinowa.A!tr.pws
F-Secure	6.70.13260.0	W32/Sinowal.ALH
Ikarus	T3.1.1.20	Trojan-PWS.Win32.Sinowal.gc
Kaspersky	7.0.0.125	Trojan-PSW.Win32.Sinowal.gj
McAfee	5237	Generic.dx
Microsoft	1.3204	PWS:Win32/Sinowal.gen!D
NOD32v2	2903	probably a variant of Win32/PSW. Sinowal.Gen
Norman	5.80.02	W32/Sinowal.ALH
Panda	9.0.0.4	Adware/Lop
Sophos	4.27.0	Mal/Sinowa-A
Symantec	10	Trojan.Mebroot
TheHacker	6.2.9.229	Trojan/PSW.Sinowal.gj
VBA32	3.12.6.2	Trojan-PSW.Win32.Sinowal.gj
Webwasher-Gateway	6.6.2	Trojan.PSW.Sinowal.GJ.20
«Banker»		
Kaspersky	от 20 апр 2007 03:45 MSK	Trojan-PSW.Win32.Banker
McAfee	5018 (04/26/2007)	PWS-Banker

До клиентов также должна оперативно доводиться информация о новых технологических решениях, внедряемых банком с целью повышения уровня безопасности работы в системе. Анализ эффективности отдельных решений представлен в следующем разделе.

2. Технологические решения, обеспечивающие повышение уровня безопасности системы ДБО

Технологии, обеспечивающие повышение уровня защищенности систем ДБО, можно условно разделить на две группы:

- технологии, обеспечивающие предотвращение несанкционированного доступа к системе,
- технологии, обеспечивающие выявление мошеннических операций в системе.

2.1. Технологии, обеспечивающие предотвращение несанкционированного доступа к системе

Цель внедрения технологий данной группы – затруднить получение злоумышленником информации о ключах и паролях клиента. В этом аспекте наиболее надежной технологией считается использование клиентами для хранения ключей персональных аппаратных криптопровайдеров, обеспечивающих неизвлекаемость секретного ключа ЭЦП клиента (такие устройства реализуются в виде USB-токена или смарт-карты). Неизвлекаемость ключа означает, что все криптографические операции, в которых используется секретный ключ, должны выполняться непосредственно в микропроцессоре устройства. Таким образом, на входе устройству передается вся информация, которая должна быть подписана, а выходной информацией является ЭЦП, сформированная с использованием неизвлекаемого ключа.

Использование носителей с неизвлекаемыми секретными ключами ЭЦП в криптографических системах делает их неуязвимыми в отношении хакерских атак, нацеленных на похищение секретных ключей пользователей из памяти компьютера, куда они считываются с традиционно используемых съемных носителей ключевой информации (например, дискет) перед выполнением криптографических операций [9].

В то же время данная технология не лишена определенных недостатков. Во-первых, это достаточно высокая стоимость устройства. По оценкам представителей банковской сферы, она не должна превышать суммы, эквивалентной 10 долларам США [10]. В настоящее время на рынке нет предложений в данном ценовом диапазоне (стоимость устройств, представленных на рынке, может составлять около 1000 рублей). Во-вторых, для того, чтобы использовать данную технологию, необходимо устройство доступа в интернет с портом USB, на котором должны быть установлены соответствующие драйверы. Поэтому с мобильных телефонов, смартфонов, КПК USB-токеном воспользоваться не удастся.

Кроме того, учитывая постоянное развитие технологий хищения средств через системы ДБО, нельзя исключить возможность появления программных средств, которые позволяли бы обойти

защиту, связанную с использованием неизвлекаемых ключей, – например, путем подмены данных документа, передаваемых на вход устройству.

Помимо технологий, обеспечивающих противодействие хищению ключей, важную роль в обеспечении безопасности играют технологии, обеспечивающих противодействие хищению паролей, вводимых клиентом на сайте системы. Пример такой технологии – использование виртуальной клавиатуры для ввода пароля. Использование виртуальной клавиатуры обеспечивает защиту от программ «кейлоггеров», осуществляющих перехват нажатий клавиш. Кнопки на виртуальной клавиатуре могут располагаться в случайном порядке, а их расположение может меняться при каждой новой загрузке страницы. При работе с виртуальной клавиатурой данные вводятся либо нажатием указателем мыши на кнопку, либо фиксацией указателя мыши на кнопке в течение определенного времени (более безопасный метод, обеспечивающий защиту от шпионских программ, перехватывающих нажатия кнопок мыши с одновременным копированием изображения с экрана). В то же время данную технологию нельзя считать достаточно надежной, поскольку существуют возможности получения данных, вводимых на экранной клавиатуре: получение изображений с экрана, чтение набранного пароля из окна ввода и т.д.

Достаточно надежную защиту пароля можно реализовать путем использования одноразовых паролей. Сложность состоит в том, каким образом обеспечить передачу пароля клиенту. В настоящее время используются различные технологии передачи информации о паролях, среди которых нужно отметить следующие:

- ✦ Передача клиенту скретч-карты со списком паролей.
- ✦ Передача паролей с помощью SMS.
- ✦ Использование OTP-токена для генерации паролей.

Скретч-карты представляют собой карты с нанесенной непрозрачной скретч-полосой, под которой находится конфиденциальная информация – пароль, PIN-код и т.п. (для прочтения информации необходимо стереть полосу). Достоинством скретч-карт является их надежность и достаточно низкая стоимость, а основным недостатком является то, что клиент должен каждый раз после использования последнего пароля, записанного на карте, обращаться в банк за новой картой. Необходимость постоянного обращения в банк в значительной степени нивелирует преимущества дистанционного обслуживания.

Технология передачи одноразовых паролей с помощью SMS не требует обращения клиента в банк за новыми паролями. Однако она также не лишена определенных недостатков. Во-первых, СМС-сообщение, содержащее пароль, может поступить клиенту с существенной задержкой или вообще не дойти. Во-вторых, стоимость данной технологии является достаточно высокой (высокая стоимость обусловлена необходимостью оплаты большого количества СМС-сообщений). В-третьих, СМС-сообщения передаются по незащищенному каналу и, следовательно, могут быть перехвачены злоумышленником.

Наиболее надежным и удобным способом получения одноразовых паролей можно считать использование технологии OTP (One-Time Password). Данная технология подразумевает использование одноразовых паролей, которые генерируются с помощью специального устройства (OTP-токена). Для этого служит секретный ключ пользователя, размещенный как внутри OTP-токена, так и на сервере аутентификации. Для того, чтобы получить доступ к системе, клиент должен ввести пароль, созданный с помощью OTP-токена. Этот пароль сравнивается со значением, сгенерированным на сервере аутентификации, после чего выносится решение о предоставлении доступа. Преимуществом такого подхода является то, что пользователю не требуется соединять токен с компьютером (в отличие от USB-токенов), соответственно, не требуется и установка специального ПО для работы с токеном [11]. Недостатком OTP-токенов является их высокая стоимость, а также ограниченное время жизни этих устройств (три-четыре года), обусловленное тем, что автономность работы предполагает использование батарейки.

Важно отметить еще один существенный недостаток всех перечисленных технологий, обеспечивающих работу с одноразовыми паролями, – уязвимость в плане атак типа «человек посередине». При такой атаке злоумышленник вклинивается в информационный обмен между клиентом и сервером и получает возможность совершить нужные транзакции якобы от имени клиента [12].

Наряду с технологиями, обеспечивающими защиту секретных ключей и паролей, используются также технологии ограничения доступа в систему по ip-адресам или MAC-адресам. В случае необходимости ограничения по ip-адресам клиент должен представить в банк перечень ip-адресов, с которых он собирается работать в системе, после чего до-

ступ в систему с других адресов запрещается. Использование этого механизма снижает вероятность того, что злоумышленники, получившие секретные ключи и пароли клиентов, смогут войти в систему. Однако данная технология также не лишена определенных недостатков. Во-первых, существенно снижается мобильность клиентов – клиент не сможет выполнять платежи с любого компьютера, подключенного к сети Интернет. Это может быть неприемлемо для клиентов, привыкших работать с разных рабочих мест (в частности, для клиентов, которые часто ездят в командировки). Во-вторых, данная технология может эффективно применяться только в том случае, если клиент работает со статического ip-адреса. При этом клиенты, работающие с динамических ip-адресов, могут быть не заинтересованы в переходе на статический адрес, поскольку переход на статический адрес потребует дополнительных затрат. В-третьих, клиент должен обращаться в банк каждый раз при смене ip-адреса (например, в случае перехода на другого провайдера). И последний недостаток – данный механизм не обеспечивает защиту в том случае, если злоумышленники используют технологии подмены ip-адреса. Большинство из перечисленных недостатков присущи и технологии, предусматривающей ограничение по MAC-адресам. Использование этого механизма также ограничивает мобильность клиента и предусматривает необходимость обращения клиента в банк в случае изменения MAC-адреса.

Говоря о технологиях, обеспечивающих предотвращение несанкционированного доступа к системе, нельзя обойти вниманием тот факт, что одной из основ всей системы информационной безопасности является применение антивирусного ПО. В настоящее время некоторые зарубежные банки предлагают своим клиентам бесплатное антивирусное ПО – необходимый программный продукт пользователи могут загрузить с сайта банка [13]. Российские банки пока в меньшей степени уделяют внимание обеспечению своих клиентов эффективными антивирусными средствами. Возможно это происходит из-за того, что реализация данного механизма банком предполагает высокий уровень затрат, связанных с приобретением, настройкой и поддержкой антивирусного ПО.

2.2. Технологии, обеспечивающие выявление мошеннических операций в системе

Вторую группу технологических решений составляют технологии, обеспечивающие выявление мошеннических операций в системе. Выявление операций, совершаемых в системе неуполномоченными лицами, должно выполняться как со стороны клиента, так и со стороны банка. Основной технологией, предлагаемой банками клиентам для контроля работы в системе, является СМС-информирование о входах в систему и об операциях, совершаемых в системе. Основные недостатки данного решения были рассмотрены при анализе технологии отправки одноразовых паролей с помощью СМС-сообщений.

Другая технология, которая может предлагаться клиентам, – реализация возможности просмотра информации о предыдущих входах в систему (когда пользователь входил в систему, с какого ip-адреса происходил вход в систему, отличается ли ip-адрес, с которого происходил последний вход в систему, от ip-адресов, использовавшихся клиентом ранее и т.п.). Использование данной опции может позволить клиенту своевременно отследить несанкционированный доступ в систему. Однако эффективность ее использования во многом зависит от того, насколько внимательно клиент относится к вопросам безопасности, будет ли он заниматься мониторингом доступа к системе.

Базовой технологией контроля операций со стороны банка является автоматизированный контроль подозрительных документов. По мнению экспертов, к подозрительным документам могут быть отнесены следующие платежи [14]:

- ✦ перевод на счет физического лица (408..., 423... и т.д.), являющегося клиентом в другом российском банке
- ✦ перевод на «котловой» счет карточного процессинга (30232..., 30233...) в другом банке с указанием в назначении платежа номера специального карточного счета
- ✦ перевод на расчетный счет организации или частного предпринимателя с указанием в назначении платежа номера электронного кошелька Webmoney, PayPal и др.

Недостатком данной технологии является то, что настроить автоматическое отслеживание всех видов подозрительных платежей не представляется возможным. В частности, к подозрительным платежам можно отнести платежи, не соответствующие основной деятельности клиента. Такого рода платежи могут отслеживаться только вручную.

Проведенный анализ показывает, что ни одна из перечисленных технологий не лишена существенных недостатков. Построение системы безопасности ДБО должно ориентироваться на

противодействие широкому спектру угроз различного рода (угроза заражения компьютера клиента вирусными программами, кражи ключевой информации и т.п.). Перечень угроз и возможные мер противодействия этим угрозам представлены в *таблице 2.*

Таблица 2.

Угрозы безопасности системы ДБО и возможные меры противодействия

Угроза	Меры противодействия
Заражение компьютера клиента вирусными программами	● Совершенствование документации по работе с системой – уточнение требований по обеспечению безопасности. ● Оперативное информирование клиента о вновь возникающих угрозах в данной области. ● Предоставление клиентам антивирусного ПО.
Кража ключевой информации	● Использование носителей с неизвлекаемыми секретными ключами ЭЦП.
Кража пароля для доступа к системе	● Использование виртуальной клавиатуры для ввода пароля. ● Использование одноразовых паролей.
Несанкционированный доступ в систему	● Ограничение доступа в систему по ip-адресу / MAC-адресу. ● СМС-информирование клиента о входах в систему. ● Предоставление клиенту возможности просмотра информации о предыдущих входах в систему.
Хищение средств со счета через систему ДБО	● СМС-информирование клиента об операциях, совершаемых через систему. ● Автоматизированный контроль подозрительных документов в банке.
Предъявление клиентом необоснованных претензий банку в случае хищения средств со счета через систему ДБО	● Совершенствование документации по работе с системой – уточнение процедуры проверки спорного документа.

Таким образом, только комплексное использование различных технологических решений и организационных мер позволит обеспечить высокий уровень безопасности при работе в системе ДБО и, тем самым, повысить качество обслуживания клиентов. ■

Литература

1. О противостоянии хакерской атаке на систему Faktura.ru. // Сайт группы компаний ЦФТ. 19.09.2008. URL: http://www.cft.ru/scdp/page?serviceid=26144&prfx_obj=26144&sc=news&origin=content&event=link(viewdetails)&obj=2703348&service=26144&viewsubmode=archive (дата обращения 22.03.2010).
2. Свыше тысячи попыток хищения через Интернет-банк фиксируется ежедневно в Свердловской области. // Сайт Уральского регионального информационного центра «ИТАР-ТАСС» («ТАСС-Урал»). 13.08.2008. URL: http://www.tass-ural.ru/news/?id=39256 (дата обращения 22.03.2010).
3. О попытках хищения денежных средств со счетов корпоративных клиентов с использованием системы электронного банкинга «iBank 2». // Сайт ООО БИФИТ. 21.01.2008. URL: http://www.bifit.com/ru/company/press/vazhno1.html (дата обращения 22.03.2010).
4. Английские лорды настаивают на ответственности банков за онлайн-мошенничества // MoneyNews: ежедневное электронное издание. 11.07.2008. URL: http://moneynews.ru/9018/ (дата обращения 22.03.2010).
5. Письмо ЦБ РФ от 07.12.2007 N 197-Т О рисках при дистанционном банковском обслуживании. // Вестник Банка России. – 12.12.2007. – № 68.
6. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». // Вестник Банка России. – 16.01.2009. – № 2.
7. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи». // Российская газета. – 12.01.2002. – № 6.
8. Предупреждение для клиентов. // Сайт ЗАО Райффайзенбанк. URL: http://www.raiffeisen.ru/attention (дата обращения 22.03.2010).
9. Интеграция криптографических приложений «Сигнал-КОМ» с аппаратной криптографией на «борту» USB-ключа MS_Key. // Сайт ЗАО Сигнал-КОМ. 19.05.2009. URL: http://www.signal-com.ru/ru/news/news_523/ (дата обращения 22.03.2010).
10. Антон Крячков: В отношении к вопросам информационной безопасности мы выходим на фазу «возрождения». // Сайт ЗАО Аладдин Р.Д. 08.09.2006. URL: http://www.aladdin.ru/press-center/publications/detail.php?print=Y&ID=9065 (дата обращения 22.03.2010).
11. Доля А. Обзор рынка средств многофакторной аутентификации» // КомпьютерПресс. – 2006. – № 5.
12. Комаров А. Современные методы аутентификации: токен и это всё о нем. // Сайт ЗАО Аладдин Р.Д. 15.10.2008. URL: http://www.etoken.ru/press-center/publications/publication20823.php (дата обращения 22.03.2010).
13. Barclays защитил своих веб-пользователей бесплатно. // www.TRISTAR.com.ua: ежедневное информационное издание. 04.07.2008. URL: http://tristar.com.ua/2/news/barclays_zashitil_svoih_veb_polzovatelei_besplatno.html (дата обращения 22.03.2010).
14. «Обнаружен троян, похищающий файлы с секретными ключами ЭЦП клиентов системы «iBank 2» // Сайт ООО БИФИТ. 07.07.2008. URL: http://www.bifit.com/ru/company/press/vazhno2.html (дата обращения 22.03.2010).