УДК 004.056.53

А.А. Сиротский
(Российский государственный социальный университет;
e-mail: hotwater2009@yandex.ru)

СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ АВТОРИЗАЦИИ В СИСТЕМАХ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Проведён анализ основных технологий обеспечения безопасности в системах дистанционного банковского обслуживания. Предложена усовершенствованная схема взаимодействия банка и клиента, предусматривающая расширенный ряд мер защиты системы от несанкционированного доступа.

Ключевые слова: система дистанционного банковского обслуживания, пароль, угрозы, защита.

A.A. Sirotskiy

IMPROVEMENT OF SECURITY METHODS AT AUTHORIZATION IN REMOTE BANK SERVICE SYSTEMS

The analysis of main technologies of safety in remote bank service systems. The advanced scheme of interaction of bank and the client, providing an expanded number of measures of protection of system from unauthorized access is offered.

Key words: system of remote bank service, password, threats, protection.

Статья поступила в редакцию Интернет-журнала 24 сентября 2013 г.

В настоящее время наблюдается стремительный рост интереса к системам дистанционного банковского обслуживания. Российские банки активно внедряют данные системы вслед за иностранными банками, которые в своём большинстве уже давно предлагают своим клиентам данный сервис.

Системы дистанционного банковского обслуживания (СДБО) – это средства и методы, реализующие предоставление клиентам банковских услуг без непосредственного посещения офиса банка, используя каналы телекоммуникационных систем для получения заявок клиентов и извещения клиентов об исполнении полученных заявок.

В качестве телекоммуникационного канала уже традиционно используется Интернет. На первых порах, до широкого внедрения Интернета в нашей стране, некоторые финансовые организации использовали для этой цели обычную телефонную связь. При этом клиент звонил оператору по определённому телефонному номеру и передавал свою заявку. В настоящее время телефонный банкинг практически не встречается, ибо он не обладает всеми возможностями полноценного сервиса, хотя в плане безопасности он довольно эффективен, ведь клиент непосредственно общался с банковским работником и вмешаться в этот процесс со стороны было практически невозможно.

Пришедший на смену устаревшим технологиям Интернет-банкинг предоставил клиентам банков практически весь спектр банковских услуг. Интернет-банкинг как СДБО, как правило, предоставляет следующие возможности:

- открытие и закрытие счетов;
- открытие и закрытие вкладов;
- осуществление перевода денежных средств между своими счетами;
- перевод денежных средств на сторонние счета различных организаций межбанковским переводом;
- оплата коммунальных и иных услуг;
- подача заявок на выпуск банковских карт;
- блокирование банковских карт;
- подача заявок на получение кредитов.

При этом Интернет-банкинг имеет ещё и ряд положительных свойств:

- отсутствует человеческий фактор;
- клиент подаёт заявки посредством заполнения электронных форм, "не стесняясь" подать за один сеанс работы большое количество заявок;
- заявки подаются и фиксируются немедленно;
- клиент может видеть и контролировать все свои заявки и их статус;
- клиент может видеть все свои счета и их заполняемость денежными средствами;
- клиент может видеть статистику своих приходов и расходов, а также где и в какое время он производил оплату со своего счёта.

Перечисленные свойства и возможности сегодня присущи сервисам СДБО практически любого российского банка, внедрившего таковую систему и предоставляющего данную услугу.

СДБО в общем случае могут быть построены по двум принципам:

- с использованием специализированного клиентского программного обеспечения, устанавливаемого на рабочих компьютерах клиентов;
- с использованием обычного Интернет-браузера.

Несмотря на то, что применение специализированной клиентской программы представляется менее опасным, с точки зрения ***несанкционированного доступа (НСД)***, большинство банков предпочитают использовать доступ через Интернет-браузер.

Более высокая защищённость от НСД технологии доступа с применением специализированного клиентского программного обеспечения возможна за счёт:

- использования точек входа на сервер, недоступных (нетипичных) для обычных браузеров;
- применения уникальных алгоритмов сжатия и шифрования данных.

Кроме того, злоумышленнику для целей НСД может потребоваться использование дополнительного программного обеспечения либо получение такой же клиентской программы, либо вскрытие её программного кода.

Разработка клиентского ***программного обеспечения (ПО)***, отвечающего требованиям безопасности, а также использование уникальных алгоритмов и технологий доступа вместе с последующей отладкой и тестированием разработанного ПО, – дело долгое, хлопотное и затратное. Поэтому в настоящее время практически все банки предоставляют доступ посредством обычного Интернет-браузера. Система Интернет-Клиент размещается на веб-сервере банка. Вся клиентская информация (автоматически формирующиеся платёжные документы и выписки, история операций) доступны на сайте банка. При этом доступ осуществляется по протоколу HTTPS, представляющему собой совместное использование протоколов HTTP и SSL.

В Интернете, на профильных сайтах, посвящённых банковской тематике, постоянно появляются сообщения о мошенничествах, связанных с хищением денежных средств со счетов клиентов различных банков посредством получения НСД к СДБО.

Рассмотрим, какие технологии безопасности и контроля доступа к СДБО в настоящее время применяются банками. Прежде всего технологии безопасности и контроля доступа следует разделить на две категории: технологии безопасности для входа в СДБО и технологии безопасности для совершения операций (подачи заявок на операции) после успешного входа в СДБО.

Технологии безопасности и контроля доступа для входа в СДБО обычно применяются следующие:

- вход в систему посредством ввода символьных логина и пароля;
- вход в систему посредством ввода уникального одноразового кода, получаемого клиентом от банка на мобильный телефон при запросе на вход.

И если несанкционированный вход в систему чреват только утечкой конфиденциальной информации о состоянии счёта клиента и проводимых им операциях, то возможность несанкционированного совершения операций от имени клиента в СДБО приводит к необратимым финансовым потерям.

Технологии безопасности для совершения операций (подачи заявок на операции) после успешного входа в СДБО обычно применяются следующие:

- принятие заявки посредством ввода уникального одноразового кода, получаемого клиентом от банка на мобильный телефон при запросе на совершение банковской операции;
- принятие заявки на совершение банковской операции только после ввода уникального одноразового кода, имеющегося у клиента, и получаемого клиентом от банка на твёрдом носителе только в офисе банка;
- принятие заявки на совершение банковской операции только при наличии электронного ключа, вставляемого в USB-порт компьютера.

Из перечисленных технологий большинство банков активно используют только первую. И только немногие банки предлагают своим клиентам вторую и третью технологии обеспечения безопасности.

В некоторых случаях банки практикуют некоторые вторичные (сопутствующие) меры пассивной безопасности, которые сами по себе не предотвращают несанкционированный доступ, но способны выявить его факт на ранних стадиях, а именно:

- SMS-информирование о входе в систему и совершаемых операциях;
- телефонный звонок клиенту при совершении по счёту множества операций или операций на крупные суммы (автор данной статьи при подаче ряда заявок получал такие звонки для подтверждения своих действий, причём от служб безопасности разных банков);
- отказ в выполнении заявки (временное приостановление) в случае, если была заменена SIM-карта в мобильном телефоне клиента.

На первый взгляд, такая мера обеспечения безопасности, как принятие заявки посредством ввода уникального одноразового кода, получаемого клиентом от банка на мобильный телефон при запросе на совершение банковской операции, может показаться достаточной. В большинстве случаев этим ограничиваются. Однако, следует иметь в виду, что существуют технологии, позволяющие изготовить действующий дубликат (клон) SIM-карты. Да, для этого необходимы соответствующие знания и оборудование. Но профессиональные мошенники способны решить эту задачу. Поэтому такая мера, особенно если она единственная, на сегодняшний день представляется уже недостаточной.

Довольно слабо выдерживает критику и метод входа в систему посредством ввода символьных логина и пароля. И хоть их длина может быть достаточно большой, они могут быть утрачены или похищены. К сожалению, операционная система Windows способна запоминать эти данные в специальном служебном файле, а это означает, что этот файл может быть скопирован, если к компьютеру будет получен удалённый доступ путём атаки или внедрения компьютерного вируса – "червя". Соответствующее вредоносное программное обеспечение уже давно стоит на вооружении у злоумышленников. Существуют также и методы его внедрения, основанные на уязвимостях операционных систем и интернет-браузеров.

Даже если на компьютере клиента не сохраняются логины и пароли, то злоумышленники всё равно могут их получить, внедрив на компьютер клиента другой вид вредоносного ПО – так называемый "кейлоггер", который отслеживает и запоминает нажатия клавиш на клавиатуре, а затем передаёт эту информацию злоумышленнику.

Типичная схема информационного взаимодействия банка и клиента показана на рис. 1. Данная схема имеет два канала информационного взаимодействия: дуплексный канал посредством сети "Интернет" и симплексный канал посредством сети сотовой связи. После введения клиентом правильных логина и пароля на сотовый номер клиента банк отправляет SMS-сообщение с одноразовым кодом доступа, который клиент вводит на странице авторизации, то есть направляет в СДБО через Интернет.

Рис. 1. Типичная схема информационного взаимодействия банка и клиента

Определённый уровень стойкости процесса информационного взаимодействия обеспечивается расчётом на относительно низкую вероятность одновременного НСД со стороны злоумышленника к обоим этим каналам одновременно.

Повышение уровня защищённости СДБО будем рассматривать по следующим направлениям:

- средства и методы авторизации, устойчивые к вредоносным программам типа "кейлоггер", червям и троянам, похищающим файлы с авторизационными данными;
- средства и методы усложнения схемы информационного взаимодействия банка с клиентом, снижающие вероятность получения контроля со стороны злоумышленника ко всем необходимым информационным каналам.

В настоящее время наиболее распространённым является ***способ авторизации путём ввода с клавиатуры символьных логина и пароля***. Как уже отмечалось, у этого способа имеется значительная уязвимость, поскольку перехват кодов нажимаемых клавиш позволит злоумышленнику завладеть авторизационными данными. В качестве противодействия данной угрозе многие банки внедрили в своих системах виртуальную клавиатуру (рис. 2), которая отображается на клиентском компьютере, и ввод логина и пароля происходит не нажатием реальных клавиш, а кликанием мышью на виртуальные кнопки на экране компьютера.

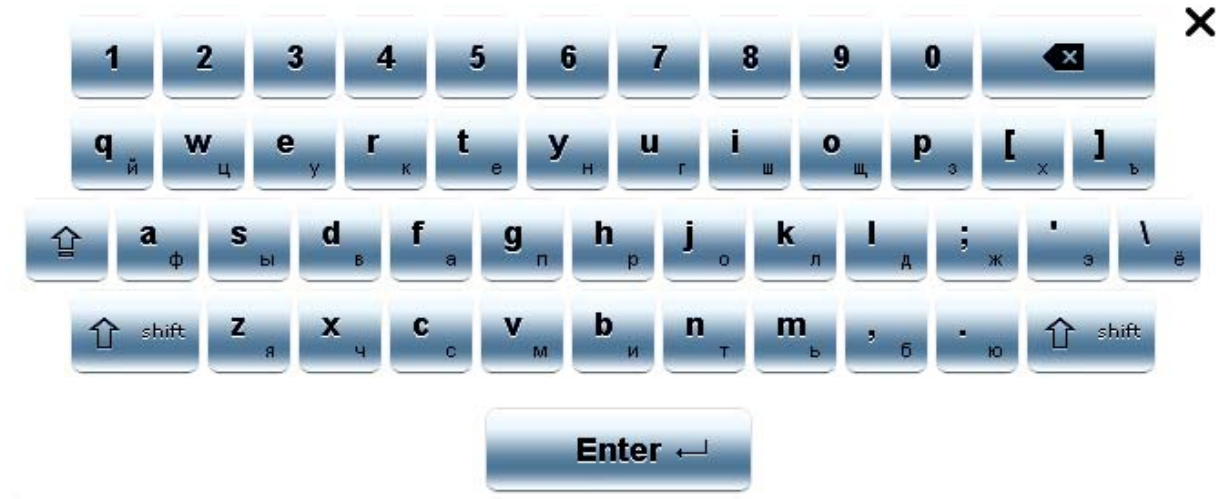

Рис. 2. Пример отображения виртуальной клавиатуры на сайте банка

Этот способ действительно позволяет повысить уровень защищённости, но только в том случае, если злоумышленник использует программу типа "кейлоггер". Однако, используя другой подход, а именно – перехватывание информации о движениях мыши и нажатии её кнопок (которых обычно только две или три) с помощью программы "мауслоггер", узнать вводимый логин и пароль становится возможным. Хотя программа типа "мауслоггер" и не выдает на выходе злоумышленнику готовые логин и пароль, тем не менее, получив данные о траектории движения мыши и моментах нажатия её кнопок, и сопоставив их с графическим отображением виртуальной клавиатуры, пароль можно вычислить если не однозначно, то по крайней мере, можно получить всего несколько вариантов, один из которых должен оказаться верным.

Положим, для примера, что вводимым паролем является комбинация "vstn9", тогда определяются места кликов мыши, как это показано на рис. 3. Далее, получив необходимые знания о координатах мыши, нетрудно составить алгоритм сопоставления этих координат с виртуальным изображением клавиатуры. Так, на рис. 4 показано, что анализ полученной информации позволит предположить, что наиболее вероятными паролями будут являться "carb8", "vstn9", "bdym0". Это упрощённый пример. Но в любом случае у злоумышленника есть большая вероятность этот пароль подобрать.

Тем не менее, можно предложить эффективный способ противодействия описанной технологии вычисления пароля. Достаточно каждый раз случайным образом генерировать новую раскладку клавиатуры с нетрадиционным расположением клавиш (рис. 5). Тогда описанная технология подбора пароля потеряет смысл. К сожалению, при этом пользователю каждый раз придётся "отыскивать" на виртуальной клавиатуре нужные клавиши, что будет для пользователя очень неудобно и неприятно. Но это нельзя назвать большой платой за безопасность.

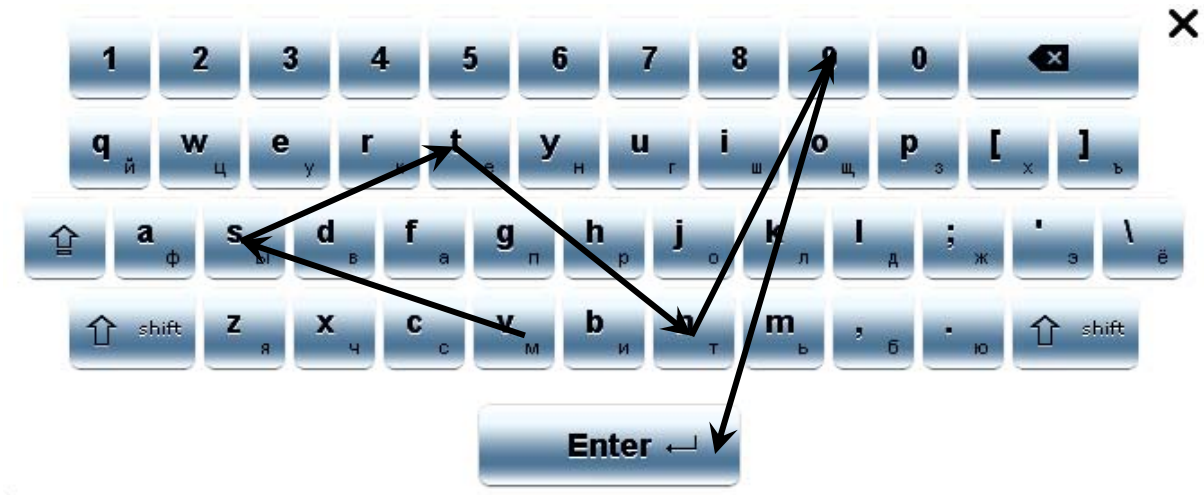

Рис. 3. Ввод пароля нажатиями мыши

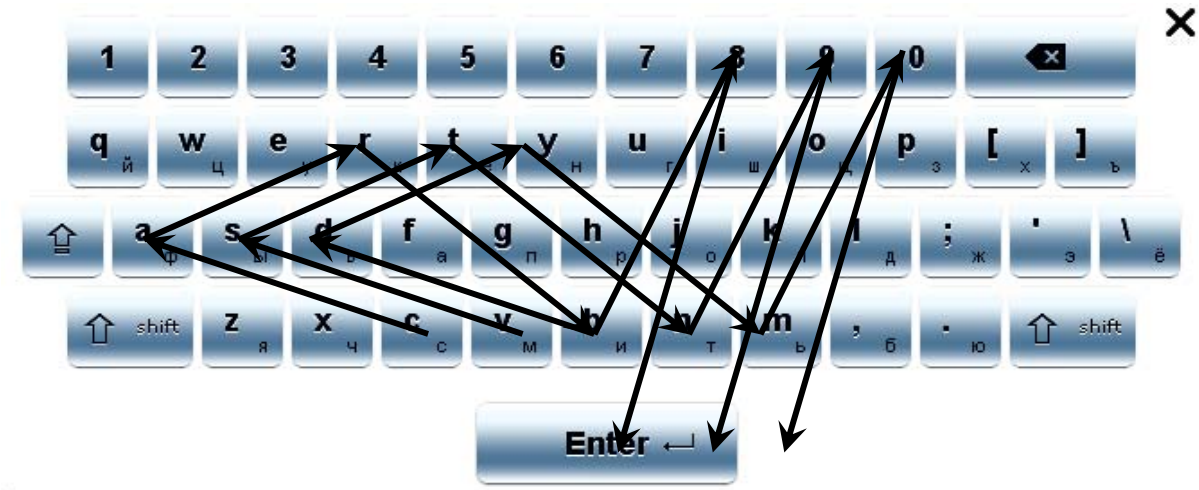

Рис. 4. Анализ возможных вариантов паролей

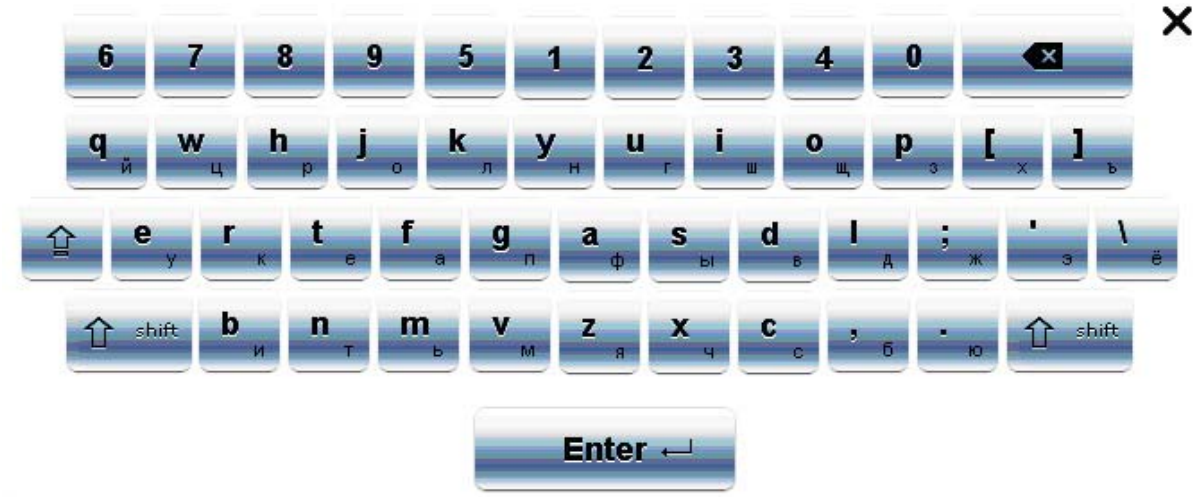

Рис. 5. Виртуальная клавиатура с измененной раскладкой

Другим способом аутентификации является ***использование графических паролей***. Данная технология основана на выборе пользователем определённых мест в графическом объекте или выборе определённой последовательности графических объектов. Несмотря на известность данной технологии, она ещё пока мало распространена. Достоинством данной технологии является то, что она является устойчивой к кейлоггерам и мауслоггерам и эффективность их применения близка к нулю.

Можно назвать две основные системы графических паролей. В первом случае пользователь должен последовательно кликнуть мышью в нескольких местах в пределах примерно десятка пикселей на большом графическом изображении. Подобрать такой пароль крайне сложно. Например, при размере одной области изображения 60×60 пикселей и общем количестве областей 128 изображение с запасом размещается на экране VGA. Количество возможных комбинаций из трёх неповторяющихся объектов из 128 составит

$A_{128}^{3} = \frac{128!}{(128-3)!} = 2048256$ комбинаций. А количество возможных комбинаций из четырёх неповторяющихся объектов из 128 составит $A_{128}^{4} = \frac{128!}{(128-4)!} = 25603200$ комбинаций.

Во втором случае пользователь в качестве ключевой информации знает несколько иконок из нескольких сотен возможных. Запросом на ввод пароля является экран с большим числом случайно расположенных иконок, и среди них обязательно есть несколько ключевых (рис. 6).

Рис. 6. Пример запроса на ввод графического пароля

Ключевые иконки нужно мысленно соединить линиями, получив некую фигуру, и кликнуть мышью в любой точке внутри этой фигуры. Эта процедура повторяется несколько раз. После нескольких успешных итераций система авторизует пользователя. Достоинство данного способа в том, что он устойчив к подглядыванию, поскольку основная идея – это позволить пользователю доказать знание им ключа, не показывая сам ключ в процессе авторизации.

Переходя к вопросу оптимизации и совершенствования схемы информационного взаимодействия банка с клиентом, следует отметить, что в целях повышения уровня защищённости от постороннего вмешательства целесообразно удлинить процедуру авторизации и ввести дополнительные каналы взаимодействия.

В частности, заслуживают внимания следующие меры:

- введение второго канала информационного обмена по сети сотовой связи;

- введение дуплексного режима обмена информацией по сети сотовой связи.

При этом схему информационного взаимодействия банка и клиента можно представить в виде, приведённом на рис. 7.

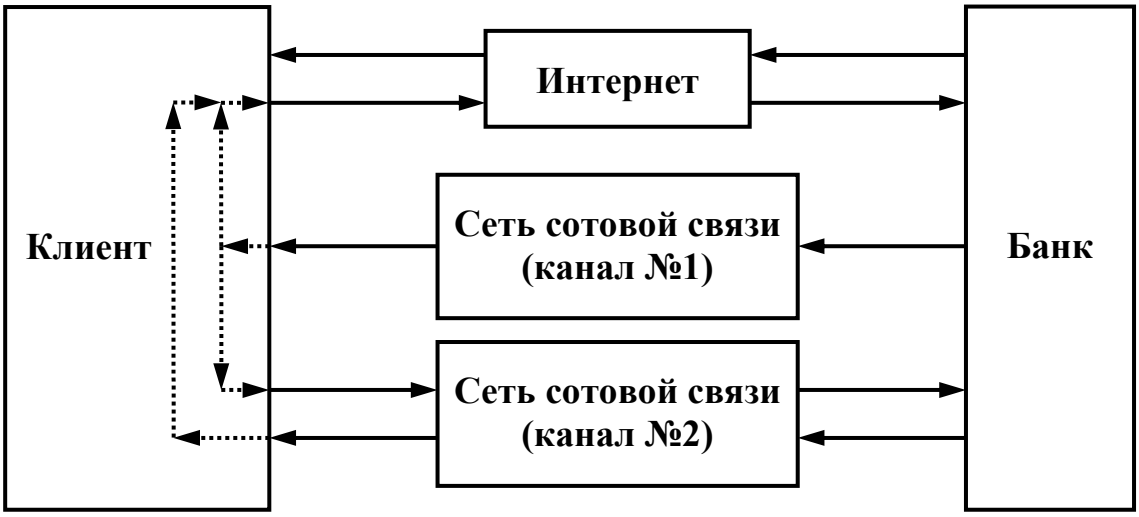

Рис. 7. Схема информационного взаимодействия банка и клиента с повышенным уровнем защищённости

Согласно данной схеме, предлагается задействовать в процессе авторизации сразу два принадлежащих клиенту сотовых телефонных номера, причём желательно, чтобы они были от разных операторов сотовой связи. При этом возникает несколько вариантов построения процедур авторизации, например возможны следующие случаи.

В первом случае клиент получает на один из своих телефонных номеров сразу два секретных одноразовых кода. Один из них, как и в традиционной процедуре, он отправляет в СДБО через Интернет, а второй – отправляет в виде ответного SMS-сообщения на специально выделенный телефонный номер банка, причём делает это со своего второго телефонного номера (задействуется второй канал сотовой связи). Достоинством данного способа будет являться тот факт, что информация от клиента поступает в банк по двум различным каналам. Однако, исходящие SMS-сообщения могут быть платными, что делает такую схему авторизации зависимой от баланса счёта.

Поэтому во втором случае можно построить процедуру так, чтобы клиент получал на оба своих телефонных номера по одному секретному коду и затем направлял их в СДБО через Интернет.

В любом из этих случаев, уровень защищённости повышается, так как злоумышленнику будет необходимо осуществить перехват SMS-сообщений уже сразу с двух различных мобильных номеров от разных операторов связи.

Подводя итог вышеизложенного, можно перечислить набор средств и методов, совместное применение которых в процедурах авторизации способно повысить уровень защищённости от НСД в СДБО:

- ввод символьных логина и пароля, набираемых пользователем на виртуальной клавиатуре со случайной раскладкой клавиш;
- ввод графического пароля;
- ввод уникального одноразового кода, получаемого клиентом от банка на мобильный телефон;
- ввод двух различных уникальных одноразовых кодов, получаемых клиентом от банка на два различных мобильных телефона, зарегистрированных у разных операторов сотовой связи;
- отправка в виде SMS-сообщения на специальный номер банка уникального одноразового кода со второго сотового телефона, принадлежащего клиенту;
- ввод уникального одноразового кода, имеющегося у клиента, и получаемого клиентом от банка на твёрдом носителе только в офисе банка;
- использование электронного ключа, вставляемого в USB-порт компьютера.

Введение дополнительных этапов в процедуру авторизации и расширение схемы информационного взаимодействия СДБО банка с клиентом позволит повысить общий уровень защищённости системы от НСД со стороны злоумышленников и криминальных посягательств.

Литература

1. ***Сиротский А.А.*** Информационная безопасность личности и защита персональных данных в современной коммуникативной среде // Технологии техносферной безопасности: интернет-журнал. Вып. 4 (50). 2013. 8 с. http://ipb.mos.ru/ttb.

2. ***Сиротский А.А.*** Информационная безопасность личности в современном деловом обороте // Современные проблемы информационной безопасности и программной инженерии. Сборник избранных статей научно-методологического семинара № 3 кафедры информационной безопасности и программной инженерии 7 декабря 2011 г. / Москва, Российский Государственный Социальный Университет. М.: Изд-во "Спутник +", 2011. С. 11-19.