УДК 681.3

# СОВРЕМЕННЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ОБЛАСТИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

**А. Н. Визгунов, А. Н. Визгунов**

*Национальный исследовательский университет – Высшая школа экономики в Нижнем Новгороде*

**Поступила в редакцию 6.09.2011 г.**

**Аннотация.** В статье рассматриваются актуальные угрозы в сфере дистанционного банковского обслуживания (ДБО) и способы противодействия этим угрозам. Анализируются методы хищения средств со счетов клиентов ДБО, достоинства и недостатки различных инструментов безопасности. Авторами рассматриваются основные положения формализованного подхода к построению модели противодействия угрозам, возникающим при эксплуатации систем ДБО.
**Ключевые слова:** система безопасности банка; системы удаленного доступа; информационная безопасность; криптозащита; пароль.
**Annotation:** The article deals with the safety of the modern bank remote access system. The different kinds of attacks and tools to resist attacks are considered. The approach to build reliable safety system is proposed.
**Keywords:** bank safety system, remote access system, information safety, criptoprotection, password.

Повышение уровня безопасности становится в настоящее время одной из наиболее актуальных проблем в сфере дистанционного банковского обслуживания (ДБО). Причиной этого является наблюдаемый в последние годы существенный рост количества преступлений, связанных с хищением денежных средств через системы ДБО (речь идет, прежде всего, о системах класса Интернет-Банк и Клиент-Банк). 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]. Другой пример – хищение группой мошенников ключей доступа к системам ДБО 457 компаний, обслуживающихся в 96 российских банках [2].

Приведенные данные показывают, что используемый большинством банков стандартный подход к обеспечению безопасности в сфере ДБО не обеспечивает высокую эффективность в современных условиях. Стандартный подход предполагает применение типовых средств криптографической защиты информации (СКЗИ) для шифрования обмена данными, формирования и проверки подписи (таких, например, как продукт «Крипто-КОМ» компании «Сигнал-КОМ»), при этом пароль клиента, используемый для его аутентификации обычно является постоянным, секретные ключи клиента хранятся на незащищенном носителе.

Для обеспечения высокого уровня безопасности должны использоваться дополнительные технологические и административные инструменты.

Необходимость принятия дополнительных мер, связанных с повышением уровня безопасности в рамках систем ДБО, отмечается и в документах Банка России. Так, в Письме Банка России 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» [3]. 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.

На наш взгляд, создание оптимальной технологии защиты информации должно выполняться на основе комплексной модели противодействия угрозам, возникающим при эксплуатации систем ДБО. Целью настоящей статьи является анализ ключевых элементов данной модели (угроз, возникающих на различных этапах работы с системой ДБО, инструментов противодействия угрозам, рассматриваемых применительно к различным группам клиентов). Отдельные аспекты формирования комплексной модели рассматривались авторами в работах [4] и [5].

Важно отметить, что в разработанном Банком России Стандарте «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» [6] существенное внимание уделяется вопросам безопасности ДБО, однако рекомендации, представленные в данном документе, во многих случаях носят общий характер (например, в пункте 7.6.6 указано, что «для доступа пользователей к системам дистанционного банковского обслуживания рекомендуется использовать специализированное клиентское программное обеспечение»). С другой стороны, ряд положений, приведенных в данном стандарте, фиксируют требования, реализуемые по умолчанию во всех современных системах ДБО (например, изложенное в п. 7.4.6 требование, определяющее, что системы ДБО должны обеспечивать возможность регистрации «проводимых транзакций, имеющих финансовые последствия»). Таким образом, данный стандарт может выступать в качестве ориентира при построении комплексной модели противодействия угрозам, возникающим при эксплуатации систем дистанционного обслуживания, однако модель должна базироваться, прежде всего, на анализе угроз, наиболее актуальных в современных условиях.

На наш взгляд, разработка комплексной модели противодействия угрозам, возникающим при эксплуатации систем дистанционного обслуживания, предполагает выполнение следующих этапов.

1. Анализ технологий хищения средств со счетов клиентов.

2. Определение административных и технологических инструментов противодействия угрозам, оценка их достоинств и недостатков.

3. Выбор оптимальных инструментов повышения уровня информационной безопасности.

Рассмотрим подробнее выполнение указанных этапов.

## 1. АНАЛИЗ ТЕХНОЛОГИЙ ХИЩЕНИЯ СРЕДСТВ СО СЧЕТОВ КЛИЕНТОВ

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.

Способы хищения и последующего использования ключевой информации можно условно разделить на следующие группы (данная классификация является расширением классификации, приведенной в работе [7]):

a. Хищение ключей сотрудником клиента, 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.

b. Заражение компьютеров клиентов троянскими программами, обеспечивающими пересылку ключевой информации злоумышленнику.

Данный вид атак подразумевает копирование ключей из незащищенного хранилища (с дискеты, жесткого диска и т.д.) или из оперативной памяти компьютера. Важно отметить, что троянские программы позволяют злоумышленнику получить как данные секретного ключа, так и пароли доступа, вводимые с клавиатуры.

c. Заражение компьютеров клиентов вирусными программами, обеспечивающими возможность удаленного управления компьютером. В отличие от технологии, описанной в предыдущем пункте, данная технология позволяет мошеннику работать, в том числе, и с ключами, хранящимися в защищенном хранилище.

d. Подмена документа в момент его подписания ЭЦП. Это сравнительно новый, дорогой и пока еще очень редкий вид атак. Низкая актуальность данной угрозы позволяет, в большинстве случаев, не принимать ее в рассмотрение при построении модели противодействия угрозам ДБО.

e. Атаки с использованием методов социальной инженерии. К данной группе относятся такие способы получения конфиденциальной информации, как фишинг (рассылка почтовых сообщений якобы от имени банка с требованием подтвердить свои идентификационные данные на специально созданном мошенниками сайте, имитирующем дизайн сайта банка), вишинг (разновидность фишинга – в сообщении содержится просьба позвонить на определенный телефонный номер и сообщить свои логин и пароль) и т.п. Отметим, что данный вид атак обычно направлен на получение пароля клиента, а не данных его секретного ключа.

## 2. ОПРЕДЕЛЕНИЕ АДМИНИСТРАТИВНЫХ И ТЕХНОЛОГИЧЕСКИХ ИНСТРУМЕНТОВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ, ОЦЕНКА ИХ ДОСТОИНСТВ И НЕДОСТАТКОВ

На наш взгляд, можно выделить два направления развития системы информационной безопасности ДБО (рис. 1):

– использование административных инструментов – совершенствование нормативной документации, организация оперативного информирования клиентов об угрозах, связанных с обслуживанием в системе, и т.д.

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

Рассмотрим подробнее сферы применения, достоинства и недостатки отдельных инструментов.

### 2.1. АДМИНИСТРАТИВНЫЕ ИНСТРУМЕНТЫ

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.

Важнейшим направлением совершенствования нормативно-правового обеспечения услуг ДБО является детализация требований по обеспечению безопасной работы в системе, и, прежде всего, требований, связанных с использованием клиентом средств криптографической защиты информации. В документации, передаваемой банком клиенту, должно быть уделено внимание следующим ключевым вопросам:

a. 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).

b. 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).

c. 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.)

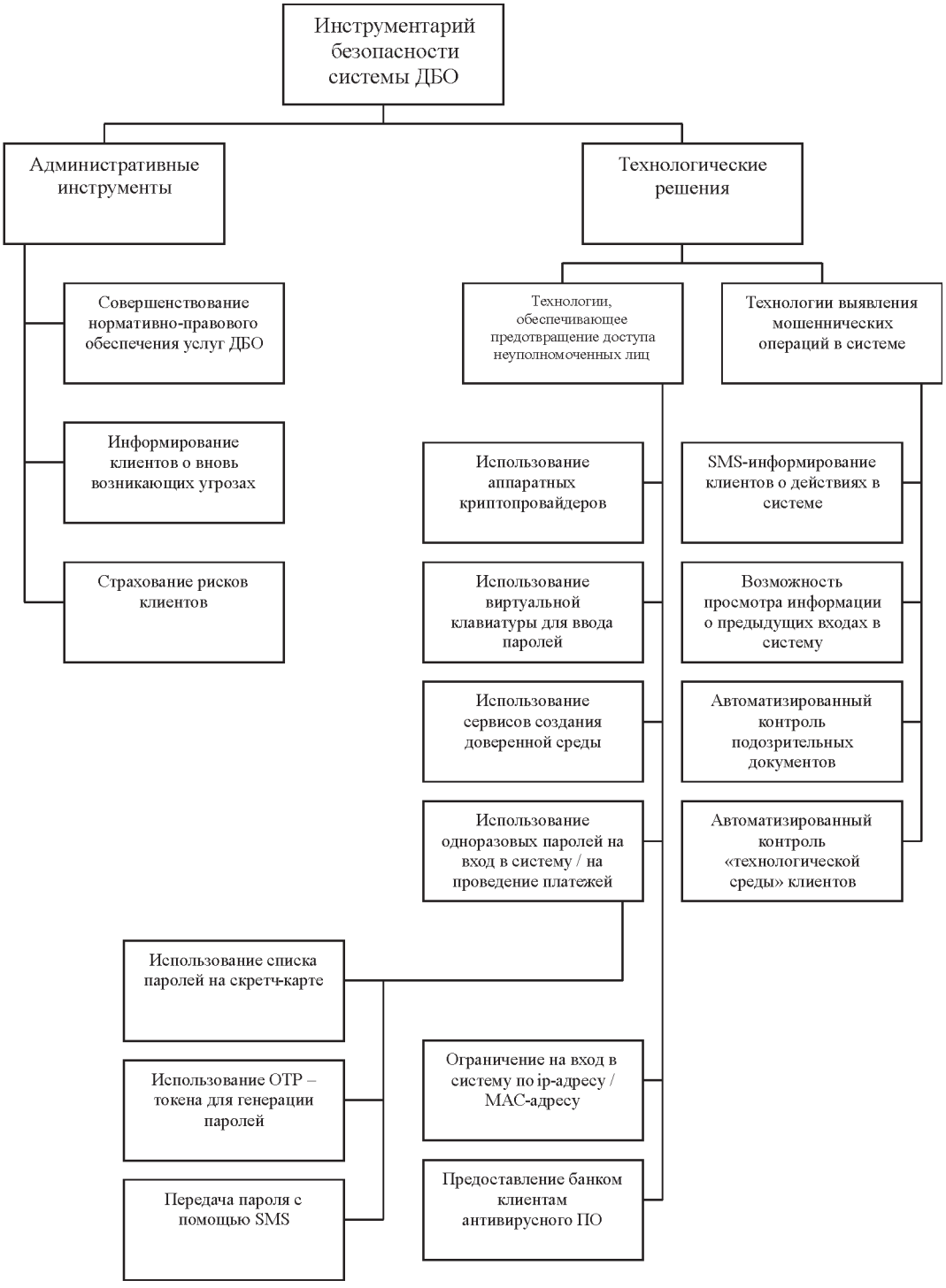


Рис. 1. Дополнительный инструментарий безопасности систем ДБО

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

e. Описание ситуаций, при которых возникает компрометация ключа, а также действий, которые должны выполняться клиентом в случае компрометации ключа.

f. 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.

Эффективным способом повышения уровня безопасности работы в рамках системы ДБО является оперативное информирование клиентов банка о вновь возникающих угрозах и способах борьбы с ними; прежде всего – об актуальных угрозах, связанных с появлением новых троянских программ, реализующих различные технологии хищения идентификационных и аутентификационных данных пользователей. Информация, передаваемая клиентам в этом случае, должна включать не только описание вирусов, но и рекомендации по выбору антивирусного ПО, которое может использоваться для их обнаружения. Информация может выкладываться на сайте системы, либо сообщаться клиентам путем личных контактов. Отметим, что данная технология эффективна и в плане противодействия атакам, основанным на использовании различных методов социальной инженерии.

Третий вид административных мероприятий, представленный на схеме, – страхование рисков клиентов, – в настоящее время только еще проходит апробацию на российском рынке. Суть его состоит в следующем – клиент, обеспечив определенные банком требования безопасности, может застраховать свои риски, связанные с возможным хищением средств через систему ДБО. Отметим, что реализация данного сервиса требует совместной работы банков, поставщиков технологий ДБО и страховых компаний.

## 2.2. ТЕХНОЛОГИЧЕСКИЕ РЕШЕНИЯ

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.

### *2.2.1. 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 [8].

В то же время данная технология не лишена определенных недостатков. Во-первых, стоимость подобных устройств достаточно высока. Во-вторых, данная технология не гарантирует защиту от некоторых видов атак, связанных, например, с подменой данных документа, передаваемых на вход устройству. Снизить эти риски позволяет использование токенов, дополнительно обеспечивающих возможность доверенной загрузки операционной системы, однако подобные устройства характеризуются значительно более высокой стоимостью.

Помимо технологий, обеспечивающих противодействие хищению секретных 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. В то же время данную технологию нельзя считать достаточно надежной, поскольку существуют возможности полу-

чения данных, вводимых на экранной клавиатуре: получение изображений с экрана, чтение набранного пароля из окна ввода и т.д.

Более эффективную защиту данных, вводимых пользователем, обеспечивает использование сервисов создания доверенной среды. Такой сервис, предлагаемый одной из российских компаний [9], предполагает как локальную защиту компьютера от внутренних угроз (троянов, кейлоггеров и т.п.), так и сетевую защиту информационного взаимодействия пользователя с ДБО, обеспечивая, в том числе, блокировку сетевых атак различных видов. Использование подобных сервисов представляется достаточно эффективным, однако их встраивание в общую инфраструктуру безопасности системы ДБО может стать серьезной проблемой.

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:

a. Передача клиенту скретч-карты со списком паролей.

b. Передача паролей с помощью SMS.

c. 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 [10]. 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 [11].

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 доступ 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 [12]. 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.

### *2.2.2 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 [13]:

a. перевод на счет физического лица (408..., 423... и т.д.), являющегося клиентом в другом российском банке

b. перевод на “котловой” счет карточного процессинга (30232..., 30233...) в другом банке с указанием в назначении платежа номера специального карточного счета

c. перевод на расчетный счет организации или частного предпринимателя с указанием в назначении платежа номера электронного кошелька Web-money, 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.

Другая технология, позволяющая банку выявить действия неуполномоченных лиц в

системе, – контроль «технологической среды» клиента. Контроль «технологической среды» клиента подразумевает мониторинг параметров аппаратной (например, носители, используемые для хранения ключей: жесткий диск, дискета или токен), программной (операционная система, браузеры и т.п.) и сетевой (провайдер, диапазон ip-адресов и т.п.) среды, в которой работают клиенты. Изменение параметров работы клиента может свидетельствовать о том, что с системой работает неуполномоченное лицо. Основные недостатки данной технологии очевидны. Во-первых, это необходимость сбора и поддержки в актуальном состоянии данных о параметрах технологической среды. Во-вторых, данная технология непригодна для контроля клиентов, характеризующихся высоким уровнем мобильности.

Таким образом, каждая из представленных на рынке технологий характеризуется определенными достоинствами и недостатками. Только совместное использование различных технологий позволит обеспечить достижение оптимального уровня безопасности.

## 3. ВЫБОР ОПТИМАЛЬНЫХ ИНСТРУМЕНТОВ ПОВЫШЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для построения модели противодействия угрозам ДБО необходимо, в первую очередь классифицировать клиентов, пользующихся данным видом услуг, – ведь предоставление всем группам клиентов одних и тех же универсальных инструментов безопасности обычно неоправданно дорого и неудобно для клиентов. В качестве критериев классификации может выступать вид клиентов (физические лица / юридические лица), объем платежей по счетам, важность клиента для банка (обычные клиенты / VIP-клиенты), уровень мобильности клиентов и др. Группы клиентов могут быть определены, например, следующим образом:

– физические лица, совершающие небольшие платежи с редкой периодичностью,

– физические лица, совершающие большой объем платежей (по количеству и / или по сумме),

– юридические лица – малый бизнес,

– юридические лица – средний и крупный бизнес,

– VIP-клиенты.

Для каждой группы клиентов определяется набор административных и технологических инструментов, обеспечивающих требуемый уровень безопасности (определение требуемого уровня безопасности для каждой группы клиентов может осуществляться на основе анализа практического опыта банка в сфере противодействия мошенничеству в сфере ДБО). При рассмотрении отдельных инструментов противодействия угрозам важно учитывать, на каком этапе процесса хищения денежных средств они могут применяться. На наш взгляд, можно выделить следующие основные этапы процесса хищения:

a. Заражение компьютера клиента вирусными программами (примеры инструментов, обеспечивающих эффективное противодействие угрозам данного этапа, – предоставление клиентам антивирусного ПО, оперативное информирование клиента о новых вирусах).

b. Кража ключевой информации (пример инструментов – использование носителей с неизвлекаемыми секретными ключами ЭЦП).

c. Кража пароля доступа к системе (примеры инструментов – использование виртуальной клавиатуры для ввода пароля, использование одноразовых паролей).

d. Несанкционированный доступ в систему (пример инструментов – контроль технологической среды, СМС-информирование клиента о входах в систему).

e. Хищение средств со счета через систему ДБО (примеры инструментов – СМС-информирование клиента о его операциях, автоматизированный контроль подозрительных документов в банке).

Четкое понимание этапов процесса хищения позволит избежать использования дублирующих инструментов противодействия и обеспечить комплексную, многоуровневую защиту от угроз, связанных с мошенничеством.

Кроме того, модель противодействия угрозам ДБО, разрабатываемая для каждой группы клиентов, должна включать разделение всех ранее рассмотренных административных и технологических инструментов на две группы: основные инструменты (в обязательном порядке используемые клиентом) и дополнительные инструменты (предоставляемые по желанию клиента). Так, например, для группы клиентов «юридические лица – средний и крупный бизнес» набор инструментов безопасности в рамках

модели противодействия угрозам может выглядеть следующим образом: (см. табл. 1).

На практике часто возникает задача выбора между различными наборами инструментов, подходящими для обслуживания той или иной группы клиентов. В этом случае выбор, на наш взгляд, должен осуществляться по следующим критериям:

– уровень безопасности, обеспечиваемый данным набором инструментов,

– стоимость внедрения и сопровождения набора инструментов,

– удобство работы с инфраструктурой безопасности.

Важно отметить, что рассмотренные критерии не могут быть сведены к одному. Опыт показывает, что попытки объединения различных критериев могут привести к неадекватной оценке банком эффективности внедрения набора инструментов безопасности ДБО. Исходя из этого, в том случае, если существуют различные пути повышения уровня безопасности, выбор оптимального варианта может осуществляться с использованием метода Парето. В этом случае различные варианты реализации программы повышения уровня информационной безопасности сравниваются исходя из следующих положений:

1. Если вариант $A_i$ превосходит вариант $A_j$ хотя бы по одному критерию оценки характеристик, а по всем другим критериям не уступает ему, то вариант $A_i$ является более предпочтительным по сравнению с вариантом $A_j$.

2. Если оценка вариантов $A_i$ и $A_j$ по всем критериям совпадает, варианты считаются равнозначными.

3. Если вариант $A_i$ по некоторым критериям превосходит вариант $A_j$, а по другим критериям уступает варианту $A_j$, то из этих вариантов не может быть выбран предпочтительный.

На наш взгляд, предлагаемый подход к построению модели противодействия угрозам в сфере ДБО позволит упростить решение задачи обеспечения высокого уровня безопасности при работе в системе.

## СПИСОК ЛИТЕРАТУРЫ

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.

2. В Москве сорван план хакеров по краже денег из 96 банков. // Сайт РБК. 02.02.2011. URL: http://top.rbc.ru/society/01/02/2011/536317.shtml.

Таблица 1

*Пример набора инструментов, обеспечивающих противодействие угрозам, связанным с отдельными этапами мошенничества (для группы клиентов «юридические лица – средний и крупный бизнес»)*

| | Этапы хищения средств со счетов клиентов | | | | |
|---|---|---|---|---|---|
| | Заражение компьютера клиента вирусными программами | Кража ключевой информации | Кража пароля доступа к системе | Несанкционированный доступ в систему | Хищение средств со счета (отправка платежа) |
| Основные инструменты | 1. Оперативное информирование клиентов о новых вирусах через почтовую службу системы ДБО. | 1. Использование USB-токенов с неизвлекаемыми секретными ключами ЭЦП. | 1. Использование одноразовых паролей на вход в систему, передаваемых с помощью СМС | 1. Контроль технологической среды клиентов | 1. Контроль подозрительных документов |
| Дополнительные инструменты | 1. Предоставление клиентам антивирусного ПО. | | 1. Использование виртуальной клавиатуры для ввода пароля. | 1. СМС-информирование клиентов о входах в систему | 1. СМС-информирование клиентов об операциях, выполняемых через систему. 2. Страхование рисков клиентов |

3. Письмо ЦБ РФ от 07.12.2007 N 197-Т О рисках при дистанционном банковском обслуживании. // Вестник Банка России. – 12.12.2007. – № 68.

4. *Визгунов А.Н.* Технологии дистанционного банковского обслуживания: российские реалии и перспективы. // Бизнес-Информатика. – 2008. – № 3.

5. *Визгунов А.Н., Визгунов А.Н.* Уровень защищенности от несанкционированного доступа как ключевой показатель качества системы ДБО // Бизнес-Информатика. – 2010. – № 2.

6. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». // Вестник Банка России. – 16.01.2009. – № 2.

7. *Калемберг Д., Плотников О.* Подводные камни безопасности ДБО. Опыт реализованных проектов // Информационная безопасность. – 2010. – № 4.

8. 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/.

9. Сервис WebSafer – В // Сайт компании WebSafer.ru. URL: http://www.ws-b2b.ru/Index/9?childID=109.

10. *Доля А.* Обзор рынка средств многофакторной аутентификации» // КомпьютерПресс. – 2006. – № 5.

11. *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.

12. 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.

13. 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.

**Визгунов Александр Николаевич** – доцент кафедры информационных технологий НИУ ВШЭ в Нижнем Новгороде, НИУ ВШЭ в Нижнем Новгороде. E-mail: vizgunovhse@yandex.ru. Тел. (831) 416-95-49.

**Визгунов Арсений Николаевич** – доцент кафедры информационных технологий НИУ ВШЭ в Нижнем Новгороде, НИУ ВШЭ в Нижнем Новгороде. E-mail: anvizgunov@hse.ru. Тел. (831) 416-95-49.

**Vizgunov Aleksandr Nikolaevich** – National Research University Higher School of Economics in Nizhnii Novgorod). E-mail: vizgunovhse@yandex.ru.

**Vizgunov Arsenii Nikolaevich** – National Research University Higher School of Economics in Nizhnii Novgorod). E-mail: anvizgunov@hse.ru.