План семинара
«Обеспечение безопасности в сфере дистанционного банковского обслуживания в системе «Банк-Клиент»

1. О хищениях и причинах их возникновения
2. Меры противодействия новым угрозам в сфере ДБО
3. Средства обеспечения безопасности
4. Порядок действий при несанкционированном доступе к системе ДБО
5. Заключение

О хищениях

В настоящее время в российских банках начался лавинообразный рост хищений денежных средств со счетов клиентов с использованием систем дистанционного банковского обслуживания (далее ДБО). Используя уязвимости в операционных системах, Web-браузерах и почтовых программах, злоумышленники заражают компьютеры клиентов вредоносными программами (троянами) и дистанционно используют секретные ключи ЭЦП клиентов и пароли, вводимые с клавиатуры.

Далее злоумышленники по системе дистанционного банковского обслуживания «Банк-Клиент» от имени клиента подключаются к банку, отслеживают поступления средств и в нужный момент направляют в банк платежные поручения с корректными ЭЦП клиента.

Кроме того, мошенническое платежное поручение создается, подписывается ЭЦП клиента (в том числе с использованием подключенного USB-токена или Смарт-карты) и отправляется в банк непосредственно на инфицированном компьютере клиента. При этом все мошеннические действия выполнялись невидимо для пользователя.

После отправки мошеннического платежа в банк вредоносная программа предпринимала действия по сокрытию попытки хищения:

При работе на инфицированном компьютере мошеннический платеж не отображался в списке платежных поручений. При работе с обычного компьютера мошеннический платеж отображался.

При работе на инфицированном компьютере операция списания средств не отображалась в выписке. При работе с обычного компьютера проводка отображалась.

При работе на инфицированном компьютере остаток на счете модифицировался – не уменьшался на сумму мошеннического платежа. При работе с обычного компьютера отображался реальный остаток.

В результате действия вредоносной программы корпоративный клиент не мог с инфицированного компьютера обнаружить факт несанкционированного списания и оперативно помешать злоумышленнику осуществить вывод похищенных средств.

Кроме того, злоумышленниками в банк по системе ДБО направляются письма от имени клиента с просьбой провести тот или иной документ.

Успешно прошедшие проверку ЭЦП, но при этом подозрительные, абсолютно не свойственные данному клиенту платежные поручения пресекаются банковскими операционистами на этапе принятия решения об исполнении документов.

Большая же часть платежей, направляемых злоумышленниками, не вызывает подозрений у банка. Такие документы имеют корректную ЭЦП, обычные реквизиты получателей и типовое назначение платежа для данного клиента. Исполнение банком таких платежей приводит к хищению денежных средств с расчетного счета корпоративного клиента.

Судебная практика показывает, что в случае корректности ЭЦП под правильно оформленным платежным документом Банк не несет ответственности за причиненные убытки.

Для обеспечения аутентичности (целостности и авторства) электронных финансовых документов во всех системах ДБО используется механизм ЭЦП сертифицированный в соответствии с действующим законодательством. Для ЭЦП используется секретный ключ, на основе которого формируется подпись под документом. Подобрать или угадать секретный ключ ЭЦП не представляется возможным.

Секретный ключ ЭЦП находится у только клиента. В банке есть открытый ключ ЭЦП клиента, с помощью которого банковский сервер проверяет подпись клиента под электронными документами. Восстановить из открытого ключа ЭЦП секретный ключ ЭЦП технически невозможно.

Именно поэтому все действия злоумышленников направлены на хищение (использование) секретного ключа ЭЦП у его единственного владельца - клиента.

Анализ выявленных вредоносных программ показывает, что злоумышленники эксплуатируют фундаментальную проблему - неспособность массового пользователя обеспечивать доверенную среду на своем компьютере.

Угрозе хищений секретных ключей ЭЦП клиентов подвержены все системы ДБО, в которых используются секретные ключи вне зависимости от типа носителя - дискета, жесткий диск, флешка, USB-токен или смарт-карта

Причины их возникновения

Сегодня уже нельзя считать компьютер клиента доверенной средой. Особенно компьютер, подключенный к Интернету.

Антивирусы, персональные межсетевые экраны и средства защиты от несанкционированного доступа, безусловно, должны использоваться и своевременно обновляться на компьютере клиента. Но все эти механизмы не гарантируют защиту персонального компьютера клиента от постоянно модифицируемых вредоносных программ.

Причинами возникновения угроз хищений являются:

- Несоблюдение требований информационной безопасности при работе с системами ДБО
- Не соблюдение регламента ограниченного доступа к данному компьютеру
- Использовать и оперативно обновлять системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений
- Отсутствие или несвоевременное обновление антивирусного программного обеспечения
- Отсутствие средств защиты от несанкционированного доступа из Интернет (межсетевые экраны, политики безопасности)
- Соблюдать правила безопасной работы в Интернете
- USB-токены или смарт-карты подключены к компьютеру не только во время синхронизации и подписи документа при работе с системой «iBank 2»
-

Меры противодействия новым угрозам в сфере ДБО

Только комплексная защита и соблюдение требований информационной безопасности может снизить риск несанкционированного доступа к системе ДБО

1. Полное и корректное информирование клиентов о новых угрозах
2. Соблюдение правил информационной безопасности, регламента доступа к компьютерам для работы в системе дистанционного банковского обслуживания, и работы с секретными ключами ЭЦП клиента;
3. Недопустимость постоянного подключения к компьютеру USB-токенов и смарт-карт «iBank 2 Key». USB-токены и смарт-карты должны быть подключены к компьютеру только во время синхронизации и подписи документа при работе с системой «iBank 2».
4. При использовании клиентом двух секретных ключей ЭЦП (ключ ЭЦП директора с правом первой подписи, и ключ ЭЦП главного бухгалтера с правом второй подписи) осуществлять работу с системой «iBank 2» на двух отдельных компьютерах с хранением секретных ключей ЭЦП на двух отдельных USB-токенах или смарт-картах.
5. Использование встроенного в систему «iBank 2» механизма дополнительного подтверждения платежных поручений с помощью одноразовых паролей, отправляемых по SMS

При включенном механизме дополнительного подтверждения после подписи платежного поручения необходимым количеством ЭЦП документ получает статус «Требует подтверждения». Для перевода документа в статус «Доставлен» клиенту необходимо ввести одноразовый пароль, полученный в SMS-сообщении.

SMS-сообщение с одноразовым паролем содержит также критичные реквизиты подтверждаемого платежа: сумму, наименование получателя, счет получателя, БИК банка получателя. Это обеспечивает защиту от подмены отображаемых клиенту реквизитов документа вредоносной программой.

Подтверждение одноразовым паролем в Internet-Банкинге может быть выполнено как сразу после подписания документа, так и позднее. В РС-Банкинге подтверждение документов выполняется в ходе синхронизации.

К недостаткам SMS относится возможность задержки доставки сообщения по вине сотового оператора. Это может помешать клиенту оперативно войти в систему и совершить важные платежи

6. Дополнительные способы защиты в Internet-Банкинге

- **Справочник доверенных получателей;**

Принцип работы механизма доверенных получателей прост: клиент единоразово подтверждает реквизиты (БИК и счет) получателей, которым он доверяет. В дальнейшем при совершении платежей на счет доверенного получателя код подтверждения запрашиваться не будет, даже если сумма платежного поручения превышает установленный банком лимит.

Клиент может опционально задавать персональные лимиты на каждого доверенного получателя. В этом случае код подтверждения будет запрашиваться при совершении платежа на счет такого получателя, если сумма платежного поручения превышает заданный для него лимит.

Источниками кодов подтверждения, как и в случае с платежными поручениями, служат SMS-сообщения и MAC-токены.

- **Белые и черные списки получателей**
- **Дополнительное подтверждение платежей (при превышении лимитов) кодами подтверждений, полученными по SMS, с использованием MAC-токенов и AGSES-карт**

MAC-токены могут генерировать как одноразовые пароли (могут использоваться для входа в систему) так и коды подтверждения платежных документов. Для генерации кода подтверждения пользователь должен ввести с клавиатуры токена основные реквизиты документа. Код подтверждения, генерируемый MAC-токеном, зависит от введенных реквизитов; для документа с другими реквизитами использовать такой код подтверждения нельзя, что также служит защитой от подмены отображаемых клиенту реквизитов.

Недостатками MAC-токенов являются необходимость ввода большого количества информации со встроенной клавиатуры для генерации кода подтверждения платежного документа, а также невозможность группового подтверждения документов.

- **механизм контроля рабочей среды клиента – Device FingerPrint.**

Device FingerPrint основан на сборе информации о рабочем окружении клиента (аппаратной платформе, системном и прикладном ПО, сетевых настройках). Информация сохраняется в системе «iBank 2» в виде набора хэш-функций.

Банк может отслеживать изменение Device FingerPrint с помощью внешней системы Fraud-мониторинга электронных платежей. По его изменению можно делать выводы о характере изменений рабочей среды клиента. Это позволяет выявлять хищения, проходящие по типовым сценариям, например, копирование файла с секретными ключами электронной подписи, удаленный доступ вредоносной программы к рабочему месту клиента по RDP и т.д.

7. Желательно формирование безопасной среды выполнения системы ДБО на компьютере клиента.

Средства обеспечения безопасности

Средствами обеспечения безопасности при работе с системой дистанционного банковского обслуживания является создание безопасной среды выполнения действий в системе Банк-Клиент. Для этого необходим комплексный подход безопасности при использовании системы Банк-Клиент.

Средства электронной подписи и формирование ЭЦП должно производиться в USB-токене или смарт-карте. При использовании клиентом двух электронный подписей ЭЦП (например ключ директора с правом первой подписи, и ключ главного бухгалтера с правом второй подписи) осуществлять работу с системой «iBank 2» на двух отдельных компьютерах с хранением секретных ключей ЭЦП на двух отдельных USB-токенах или смарт-картах.

USB-токены и смарт-карты должны быть подключены к компьютеру только во время синхронизации и подписи документа при работе с системой «iBank 2».

Использовать встроенный в систему «iBank 2» механизм дополнительного подтверждения платежных поручений с помощью одноразовых паролей, отправляемых по SMS. При этом существует возможность настраивать для корпоративного пользователя параметры платежного документа, при которых документ требует подтверждения. Такими параметрами являются превышение суммы документа порогового значения, исключение требования подтверждения для платежей в бюджет. Отправка СМС–сообщений нескольким сотрудникам Клиента.

В системе Интернет-банкинга доступны дополнительные способы защиты:

Механизм доверенных получателей с использованием справочника доверенных получателей. Клиент единоразово заносит в справочник доверенных получателей и подтверждает реквизиты (БИК и счет) получателей, которым он доверяет. В дальнейшем при совершении платежей на счет доверенного получателя код подтверждения запрашиваться не будет, даже если сумма платежного поручения превышает установленный банком лимит.

В системе дистанционного банковского обслуживания «IBank 2» доступно ведение белых и черных списков получателей.

Порядок действий при несанкционированном доступе к системе ДБО

Действия клиента

1. В случае выявления хищения денежных средств в системе ДБО немедленно прекратить любые действия с компьютером, подключенным к системе ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.). При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

2. Немедленно обратиться в банк по телефону с заявлением о блокировке системы ДБО, приостановке исполнения платежа и возврате средств. Подготовить письменное заявление об отзыве платежа, возврате средств и блокировании доступа к системе ДБО, а также о компрометации ключей и необходимости смены закрытого ключа. Копия заявления должна быть направлена в банк незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в банк плательщика течение одного дня.

3. При наличии необходимой информации обратиться в банк получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении платежа и возврате денежных средств

4. Предпринять меры для обеспечения сохранности и неизменности журналов операционных систем, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) и системы дистанционного банковского обслуживания за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

5. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его локальной вычислительной сети как минимум за три месяца, предшествовавшие факту хищения денежных средств

6. Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к системе Банк-Клиент, действия с электронными ключами, подключенным к системе ДБО, предшествовавшие факту хищения денежных средств, подготовить объяснения работников клиента об использовании электронных устройств в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, о странностях при работе системы Клиент-Банк, перебоях или отказах, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших на рабочем месте с системой Клиент-Банк и т.д.

7. Оперативно обратиться с заявлением в правоохранительные органы по факту хищения денежных средств.

8. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить все необходимые документы.

9. Копии вышеуказанных документов по перечню, установленному банком, направить в банк с приложением Справки по факту инцидента информационной безопасности в системе ДБО, а также подтверждающих документов.

Действия Банка

1. При получении телефонного обращения плательщика о приостановке исполнения платежа немедленно предпринять разумно возможные и достаточные действия для идентификации плательщика, в том числе, посредством использования контактной информации, указанной в договоре банковского счета. При наличии возможности использовать дополнительные каналы для подтверждения обращения (SMS-уведомление, сообщение по электронной почте)

2. При подтверждении обращения незамедлительно принять меры к приостановке дальнейшей обработки платежа. Провести блокировку всех ключей ЭЦП клиента и доступа к системе Банк-Клиент.

3. В случае завершения обработки платежа незамедлительно в любой доступной форме направить в банк получателя информацию о факте хищения денежных средств с просьбой о приостановке обработки платежа

4. Оперативно направить письмо в банк получателя или к оператору платежной системы по факту хищения денежных средств с просьбой о прекращении обработки платежа, блокировке ДБО и платежных карт клиента – получателя, применении к получателю платежа мер контроля в рамках системы ПОД/ФТ[1] и возврате средств.

5. Истребовать у плательщика подтверждение о подаче плательщиком заявления в правоохранительные органы и получить его копию в течение не более 2 рабочих дней со дня получения обращения плательщика в банк о факте хищения денежных средств

6. Осуществить силами уполномоченных сотрудников либо с привлечением организаций, предоставляющих квалифицированные услуги по расследованию инцидентов информационной безопасности, по меньшей мере, следующие действия:

- Провести мероприятия, определённые договорными отношениями с клиентом, в отношении проверки легитимности электронной подписи оспоренного платёжного документа. При необходимости – провести мероприятия по факту компрометации ключей электронной подписи.
- Получить от ответственных сотрудников банка, обслуживающих системы ДБО, администраторов сети, систем криптографической защиты и т.д. экспертные заключения в рамках их компетенции по корректности ЭЦП в составе платежного документа, ее целостности и авторства.
- Обеспечить хранение собранной информации в неизменном виде для передачи правоохранительным органам по запросу.

7. Документально зафиксировать полученные результаты, выполнив следующие проверочные мероприятия в целях формирования необходимой доказательной базы по факту хищения денежных средств:

- По журналам систем ДБО и АБС установить присутствовал ли платежный документ в системе ДБО ранее.
- В свойствах платежного документа установить его авторство, дату, время и способ его создания.
- Провести сбор записей журналов работы системы Банк-Клиент
- При наличии в банке электронного документа с подлинной электронной подписью и при оспаривании подлинности электронной подписи в составе электронного документа, подтверждающего поручение плательщика банку выполнить действия по созданию комиссии в соответствии с регламентом соглашения по предоставлению банковских услуг с использованием программно-технического комплекса «БАНК-КЛИЕНТ»

Банку получателя необходимо:

1. В рамках действующего законодательства Российской Федерации оказывать любое возможное содействие банку плательщика и плательщику в целях предотвращения хищения денежных средств, а при невозможности его предотвращения – в целях максимально оперативного расследования факта хищения денежных средств и возврата неосновательно полученных сумм, в том числе в части направления банку плательщика и плательщику имеющейся информации о получателе платежа на основании статьи 19 Конституции Российской Федерации, пункта 1.7 статьи 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», статей 6 и 131 ГПК РФ, а также статьи 7 Федерального конституционного закона от 31.12.1996 №1-ФКЗ «О судебной системе Российской Федерации» для предъявления иска к получателю о возврате неосновательного обогащения в соответствии с главой 60 ГК РФ.

2. При получении обращения банка плательщика о приостановке исполнения платежа подтвердить достоверность и правомочность данного обращения.

3. На основании полученной от банка плательщика информации зачислить указанную в сообщении сумму на счет 47416 «Суммы, поступившие на корреспондентские счета до выяснения» и осуществить мероприятия в порядке, предусмотренном Положением Банка России «О Правилах ведения бухгалтерского учета в кредитных организациях, расположенных на территории Российской Федерации».

4. В случае, если похищенные денежные средства были сняты со счетов, открытых в банке получателя, необходимо подготовить технический носитель

информации, содержащий записи видеокамер банкомата и других видеокамер, имеющих отношение к хищению денежных средств

5. Подготовить и по запросу банка плательщика, правоохранительного органа необходимые документы в отношении получателя похищенных денежных средств.

6. В случае, если похищенные денежные средства со счетов, открытых в банке получателя, были переведены на счет (счета) в ином банке (иных банках), банку получателя необходимо, в свою очередь, незамедлительно направить в этот банк (банки) информацию о факте хищения денежных средств и копии материалов, полученных от банка плательщика.

7. Одновременно с мероприятиями по возврату похищенных средств необходимо провести полный анализ движений по всем счетам подставного физического или юридического лица, используемого в мошеннических схемах обналичивания финансовых средств.

Заключение

Создание максимально защищенной среды для работы с системой Банк-Клиент, использование USB-токенов или Смарт-карт для хранения ключей ЭЦП и формирования подписи под платежным документом, а также использование дополнительных мер по защите от несанкционированного доступа (использование SMS-сообщений с одноразовыми паролями, справочников доверенных получателей и т.д.), дает возможность обеспечить сохранность денежных средств и безопасное использование систем дистанционного банковского обслуживания.