

Инструкция Клиента по обеспечению информационной безопасности при работе по Системе Клиент-Банк «iBank 2» (далее – «Система»)

1. Риски клиентов при работе с системами дистанционного банковского обслуживания

За последние несколько месяцев в ряде российских банков участились случаи хищения денежных средств с расчетных счетов корпоративных клиентов путем совершения платежей с использованием систем дистанционного банковского обслуживания типа «Клиент-Банк».

Анализ выявленных ситуаций показал, что хищения денежных средств с расчетных счетов осуществляются:

- как работающими, так и уволенными ответственными сотрудниками предприятия, имевшими доступ к секретным ключам электронно-цифровой подписи (далее – «ЭЦП») для системы дистанционного банковского обслуживания;
- штатными ИТ-сотрудниками организаций, имевшими доступ к носителям с секретными ключами ЭЦП (дискеты, флеш-диски, жесткие диски и пр.), а также доступ к компьютерам, с которых осуществлялась работа по системе дистанционного банковского обслуживания;
- нештатными, приходящими по вызову, ИТ-специалистами, выполняющими профилактику и подключение к Интернет, установку и обновление бухгалтерских и справочных программ, установку и настройку другого программного обеспечения на компьютерах, с которых осуществляется работа по системе дистанционного банковского обслуживания;
- злоумышленниками путем заражения вредоносными программами компьютеров клиентов в связи с уязвимостью системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.) с последующим дистанционным похищением секретных ключей ЭЦП и паролей.

Как правило, действия злоумышленников направлены:

- на похищение файла с секретным ключом ЭЦП;
- на похищение пароля доступа к ключу;
- на передачу в банк электронных платежных документов, заверенных похищенным ключом ЭЦП.

Документы, направляемые злоумышленниками с использованием действующих секретных ключей ЭЦП клиентов, могут не вызывать подозрений у сотрудников банков, поскольку такие документы имеют корректную ЭЦП, вполне обычные реквизиты получателей и типовое назначение платежа. Благодаря этому, полученные платежные документы признаются банками поступившими от клиента – владельца расчетного счета, и банки обязаны их исполнять. Таким образом происходит хищение злоумышленниками денежных средств с расчетных счетов клиентов. При этом вся ответственность за убытки безусловно и полностью возлагается на клиентов как единственных владельцев секретных ключей ЭЦП.

В целях:

- повышения безопасности при работе с системами дистанционного банковского обслуживания,

- выполнения рекомендаций ЦБ РФ, изложенных в Письме ЦБ РФ №197-Т от 07 декабря 2007 года «О рисках при дистанционном банковском обслуживании»,

ОАО АКБ «Перминвестбанк» разработал Инструкцию Клиента по обеспечению информационной безопасности при работе по Системе Клиент-Банк «iBank 2», предусматривающую комплекс требований и рекомендаций, выполнение которых позволит снизить указанные выше риски.

2. Требования по обеспечению информационной безопасности при работе по Системе

В целях обеспечения информационной безопасности при работе по Системе **Клиент наделяется следующими обязанностями:**

1. Осуществлять вход в Систему только через корпоративный сайт ОАО АКБ «Перминвестбанк» www.pibank.ru либо через сайт ibank2.pibank.ru.
2. Ни в коем случае не отвечать на письма, якобы от имени Системы, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену www.pibank.ru, прислать секретный ключ или пароль доступа к нему, а немедленно сообщить о подобном факте Администратору Системы в рабочие часы Банка по телефону: (342) 245-53-81.

Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать секретный ключ ЭЦП или пароль. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.

3. Хранить ключи ЭЦП на съемном носителе (USB-токены, дискеты, флеш-диски, CD-диски), а не на жестком диске компьютера.
4. Не отлучаться от компьютера, пока в нем находится съемный носитель, содержащий секретный ключ.
5. Извлекать из компьютера съемный носитель, содержащий секретный ключ, сразу после завершения работы по Системе.
6. Не записывать на носитель, содержащий секретный ключ, какую либо другую информацию.
7. Не создавать дубликат секретного ключа.
8. Обеспечить использование секретного ключа только ответственным сотрудником, уполномоченным на то соответствующим распорядительным документом.
9. Никогда не передавать ключи ЭЦП ИТ-сотрудникам для проверки работы Системы «iBank 2», проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично владелец ключа ЭЦП должен подключить съемный носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа «iBank 2», и лично ввести пароль, исключая его подсматривание.
10. Хранить съемный носитель, содержащий секретный ключ, в надежном месте, исключающем доступ к нему неуполномоченных лиц и повреждение материального носителя.

Банк информирует Вас, что вся ответственность за конфиденциальность Ваших секретных ключей ЭЦП полностью лежит на Вас, как единственных владельцев секретных ключей ЭЦП.

11. В случае выявления явных или косвенных признаков компрометации ключей ЭЦП или вредоносных программ в компьютере, используемом для работы по Системе, незамедлительно уведомить Банк по

телефону: (342) 245-53-81 либо лично явившись в Банк с целью блокирования скомпрометированных секретных ключей ЭЦП с последующей их заменой.

К событиям, связанным с компрометацией ключей ЭЦП относятся, включая, но не ограничиваясь, следующие:

- утеря материального носителя, содержащего секретный ключ, в том числе с последующим обнаружением;
 - выход из строя материального носителя, содержащего секретный ключ, когда невозможно достоверно определить причину этого события (доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
 - обнаружение факта или угрозы использования (копирования) секретного ключа и/или доступа к Системе с использованием секретного ключа неуполномоченными лицами (несанкционированная отправка электронных документов);
 - обнаружение ошибок в работе Системы, в том числе возникающих в связи с попытками нарушения информационной безопасности;
 - увольнение ответственного сотрудника Клиента, имевшего доступ к секретному ключу.
12. Обеспечивать конфиденциальность использования пароля Клиента для доступа к секретному ключу; пароль не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы в работоспособном состоянии.
13. Применять на рабочем месте средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение и т.п.
14. Производить смену ключей ЭЦП как в случае компрометации, так и по требованию Банка.

Помимо указанных выше требований **Банк рекомендует** также:

1. Исключить доступ к компьютерам, используемым для работы по Системе, посторонним лицам и персоналу предприятия, не уполномоченному на работу по Системе и/или обслуживание компьютеров.
2. На компьютерах, используемых для работы по Системе, исключить посещение всех Интернет-сайтов, кроме используемых для входа в Систему, а также исключить установку развлекательных и игровых программ.
3. Использовать только лицензионное ПО (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного ПО.
4. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.
5. Использовать в качестве съемных носителей для хранения секретных ключей USB-токены, гарантирующие защиту секретных ключей Клиента от хищения злоумышленниками путем копирования или с помощью вредоносных программ.
6. В качестве дополнительной меры по обеспечению информационной безопасности воспользоваться предоставляемой Банком возможностью IP-фильтрации (разрешение доступа к Системе только с указанных Клиентом IP-адресов/сетей). Несмотря на то, что использование IP-фильтрации ограничивает возможности Клиента работать по Системе, используя подключение к Интернет в произвольном месте, данная мера исключает использование злоумышленником похищенного секретного ключа ЭЦП Клиента.