Рекомендации по информационной безопасности

Системы «Клиент-Банк» предназначены для подготовки, передачи по каналам связи и хранения финансовых документов, представленных в электронном виде (электронный документ).

Безопасность обмена электронными документами обеспечивается посредством их шифрования и наложением электронно-цифровой подписи, которая является аналогом собственноручной подписи. Именно электронный документ с ЭП является основанием для совершения финансовых операций и доказательной базой при разрешении конфликтной ситуации.

Шифрование и подпись электронных документов осуществляется с помощью секретного ключа электронно-цифровой подписи. Секретный ключ ЭП клиента хранится в хранилище в файле в зашифрованном виде. Доступ к секретному ключу защищен паролем, известным только его владельцу.

Выполнение нижеследующих рекомендаций является необходимым условием обеспечения безопасности расчетов в системе «Клиент-Банк».

При выборе пароля доступа к секретному ключу электронно-цифровой подписи рекомендуем выполнять следующие правила выбора пароля:

- пароль выбирается самостоятельно;
- если пароль записан на бумаге, то хранится в месте, недоступном для посторонних лиц;
- пароль содержит не менее 6 различных символов;
- пароль обязательно меняется, если он стал известен постороннему лицу;
- в качестве пароля не используются:
    - последовательности, состоящие из одних цифр (в том числе даты, номера телефонов, номер автомобиля и т.п.);
    - последовательности повторяющихся букв или цифр;
    - подряд идущие в раскладке клавиатуры или в алфавите символы;
    - имена и фамилии;
    - ИНН или другие реквизиты клиента.

Следует исключить доступ посторонних лиц к ключевому носителю USB токену.

- Ключевой носитель и пароли доступа к нему хранятся в недоступном для окружающих месте отдельно друг от друга.
- По завершении работы в Системе «Клиент-Банк» или перерыве в работе ключевой носитель извлекается из устройства.
- Ключевой носитель используется только для подписания электронных документов, после чего извлекается из устройства.
- Ключ ЭП не копируется и не передается никому даже на короткое время.
- В случае смены лица, осуществляющего подпись электронных документов, утере ключевого носителя, а также о любом подозрении на компрометацию ключа ЭП незамедлительно сообщается в Отдел клиентского обслуживания для блокировки ключа ЭП, а также по телефону +7 (495) 744-55-55.

Следует ограничить доступ к рабочим местам, с которых осуществляется работа с ПО системы «Клиент-Банк»

- Право доступа предоставляется только лицам, непосредственно осуществляющим работу в системе «Клиент-Банк».
- Рабочие места системы «Клиент-Банк» не оставляются без контроля: при кратковременном отсутствии сохраняются все открытые на редактирование документы, средствами операционной системы блокируется рабочее место.

Следует соблюдать правила настройки «доверенной среды» и исключения несанкционированного изменения программного обеспечения на рабочих местах системы «Клиент-Банк»

- Используется только лицензионное программное обеспечение.
- Устанавливаются все обновления системы безопасности, рекомендуемые производителем операционной системы, установленной на компьютере.
- Отключается учетная запись для гостевого входа (Guest).
- Отключаются режимы отображения окна всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей (ОС семейства Windows).
- Для всех учетных записей в операционной системе используются пароли, удовлетворяющие требованиям настоящих рекомендаций.
- Для защиты от несанкционированного доступа из внешней или локальной сети используется и оперативно обновляется специализированное ПО для защиты информации:
    - антивирусное ПО с регулярно обновляемыми базами;
    - персональные межсетевые экраны;
    - средства защиты от несанкционированного доступа и пр.
- Работа в системе «Клиент-Банк» немедленно прекращается при подозрении, что компьютер заражен, а также в случае обнаружения незарегистрированных программ или нарушения целостности операционной системы.

Следует соблюдать правила безопасной работы в сети Интернет на рабочих местах системы «Клиент-Банк».

- Не допускается открывать сайт системы «Клиент-Банк» по ссылкам (особенно баннерным или полученным через почту);
- Не допускается отвечать на подозрительные письма с просьбой выслать секретный ключ ЭП , пароль и другие конфиденциальные данные.
- Не устанавливаются и не сохраняются подозрительные файлы, полученные из ненадежных источников, скачанные с известных web-сайтов, присланные по электронной почте, полученные в телеконференциях;
- На компьютере не запускаются программы, полученные не из доверенных источников.

Внимание!

Секретным ключам ЭП и паролям могут завладеть не только вредоносные программы, но и третьи лица, тем или иным образом получившие доступ к Вашему компьютеру. Злоумышленниками могут являться:

1. Ответственные сотрудники клиентов, имевшие доступ к секретным ключам ЭП организации. Как правило, это уволенные директора, бухгалтеры и их заместители, а также совладельцы организации.

2. Штатные ИТ-сотрудники клиентов, имевшие технический доступ к носителю (USB - токену) с секретными ключами ЭП клиентов, а также доступ к компьютерам клиентов, с которых осуществлялась работа по системе «Клиент-Банк».

3. Нештатные, приходящими по вызову, ИТ-специалисты, обслуживающие компьютеры корпоративного клиента, с которых осуществлялась работа по системе «Клиент-Банк». Как правило, это приходящие ИТ-специалисты, осуществляющие профилактику и подключение к Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого ПО.

Будьте предельно внимательны и осторожны!

- При каждом входе в систему (если Вы работаете on-line) и при каждой синхронизации с банковским сервером (если Вы используете клиентское приложение РС-Банкинг) обращайте внимание на информацию о последних сеансах работы с системой: в какое время и с каких IP адресов был произведен вход в интернет-банк.
- Используйте для хранения секретных ключей ЭП USB-токен.
- Не допускайте постоянного подключения к компьютеру USB-токена.
- Используйте USB-токен исключительно для входа в систему «Клиент-Банк» (при работе on-line), а также только в момент подписания документов, после чего обязательно извлекайте носитель с ключами из устройства
- Используйте в дополнение к USB-токенам расширенную многофакторную аутентификацию (одноразовые пароли), зарегистрировав в банке устройство защиты информации OTP-токен. При использовании расширенной многофакторной аутентификации злоумышленник не сможет подключиться к банковскому Серверу Приложения «Клиент-Банк» от имени клиента, поскольку не имеет возможности получения одноразового пароля.

ПРОСИМ ВАС НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАТЬСЯ В БАНК ПРИ ВОЗНИКНОВЕНИИ СЛЕДУЮЩИХ СИТУАЦИЙ:

- На компьютере, используемом для работы в системе «Клиент-Банк», обнаружено вредоносное ПО (вирусы, «трояны»).
- Обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
- В выписке обнаружены несанкционированные Вами расходные операции.
- Не работает по неизвестным причинам система удаленного обслуживания или компьютер, с которого осуществлялась работа с ПО системы «Клиент-Банк».