АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНКПЕРМЬ

УТВЕРЖДЕНО
решением Правления
ОАО АКБ «Пермь»
(Протокол заседания
от «20 » ноября 2013 года)
Председатель Правления
ОАО АКБ «Пермь»
_____ Л.В. Саранская

Рекомендации по безопасному использованию системы «Банк-Клиент» в ОАО АКБ «Пермь»

1. Настоящие рекомендации разработаны согласно Письму Банка России от 30 января 2009 г. № 11-т «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга».

2. В целях защиты информации, передаваемой через систему «Банк-Клиент» и обеспечения сохранности денежных средств необходимо соблюдать 5 правил:

2.1. Обеспечение сохранности ключевого носителя

После регистрации в системе «Банк-Клиент» выдается ключевой носитель, который содержит ключи ЭП, базу данных, инструкции. Клиенту необходимо **обеспечить его сохранность** от посторонних лиц.

Ключи электронной подписи (ЭП) необходимо хранить **на отдельном сменном носителе** (флеш-карта, USB-флешка, дискета), не хранить на нем другие данные. Использовать носитель с ключами ЭП только для работы с «Банк-Клиент», **убирать его** в запираемый ящик (сейф) в остальное время.

Нельзя хранить копии ключевого носителя на жестком диске, в сетевых каталогах с общим доступом и на других общедоступных ресурсах.

Нельзя передавать ключевой носитель или его копию посторонним, оставлять его без присмотра.

Необходимо сделать **резервную копию** ключевого носителя и хранить ее в сейфе, она может Вам потребоваться, если основной носитель повредится.

2.2. Ограничение доступа к компьютеру с системой «Банк-Клиент»

Доступ к компьютеру, на котором установлен «Банк-Клиент», должны иметь только доверенные сотрудники.

Операционная система и все программы, устанавливаемые на компьютер, должны быть лицензионными, поступать из заслуживающих доверия источников. Нельзя использовать взломанные программы.

Операционная система и установленные программы должны регулярно **обновляться**. В обновления системных и прикладных программ входят доработки, повышающие безопасность и надежность работы, предотвращающие распространение компьютерных вирусов.

Необходимо **установить антивирусную программу** и поддерживать её функционирование, регулярно обновлять, регулярно запускать. Незамедлительно удалять обнаруженное вредоносное программное обеспечение (вирусы, шпионские программы и т. д.).

Необходимо отключить "автоматическое выполнение" для подсоединяемых к компьютеру флеш-карт и компакт-дисков для исключения запуска вредоносных программ.

Необходимо предусмотреть невозможность установки посторонними лицами (гостями, посетителями, обслуживающим персоналом) на компьютер специальных "шпионских" программ. Хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.

Нельзя устанавливать программу «Банк-Клиент» и работать в ней с **чужих компьютеров**.

Необходимо **ограничить** свой обмен через интернет только надёжными информационными порталами и проверенными корреспондентами электронной почты.

Небезопасно открывать письма и вложения, полученные по электронной почте от неизвестного отправителя, переходить по подозрительным ссылкам. Часто в виде "интересной ссылки" в письме от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.

Необходимо запретить удаленный доступ к компьютеру, на котором установлен «Банк-Клиент».

2.3. Контроль за состоянием денежных средств в банке

Необходимо регулярно проверять состояние счетов и документов в банке, выполняя запросы выписки и документов (ежедневно, обязательно утром и вечером, желательно в течение дня). Если обнаружены документы, которые Вами не передавались — необходимо срочно позвонить в банк с просьбой остановить обработку и разобраться.

При неожиданном "зависании" компьютера в момент работы с системой "Банк-Клиент", с последующим полным отказом в работе, необходимо позвонить в операционный отдел банка и убедиться, что по счёту от имени Клиента не отправлен платёж.

Необходимо позвонить в службу технической поддержки банка и сообщить, что до момента устранения неисправности Клиент не будет передавать документы в банк по системе «Банк-Клиент». Необходимо подтвердить это письмом с печатью и подписью руководителя.

2.4. Замена ключей ЭП в следующих случаях:

Срок действия ключа ЭП составляет 1 год, до окончания срока его действия Клиенту необходимо самостоятельно в программе «Банк-Клиент» создать новые ключи ЭП и зарегистрировать Регистрационную карточку в банке.

Ключи ЭП необходимо **менять при смене специалиста** (руководителя, программиста, системного администратора, бухгалтера), непосредственно работающего с ключами ЭП, или при подозрении в **компрометации ключей**. В частности, компрометацией является вирусная активность на компьютере, на котором установлена программа «Банк-Клиент».

При проведении ремонтных и любых других работ на компьютере с программой «Банк-Клиент» сторонними специалистами заранее звоните в банк и

предупреждайте о запрете приема банком документов по «Банк-Клиент». После окончания работ — обязательно **смените ключи ЭП** на новые. Просьбу о запрете приема документов необходимо подтвердить письмом с печатью и подписью руководителя.

2.5. Использование всех возможностей системы «Банк-Клиент»

Необходимо ограничить суммы документов, передаваемых по системе «Банк-Клиент» (первоначально эта сумма определяется в Заявке, можно ее изменить по дополнительному соглашению).

Если Клиент работает в интернет с постоянного ip-адреса, можно установить его как единственный разрешенный, с которого можно принимать от Клиента сообщения по системе Банк-Клиент. Сообщения с других ip-адресов не будут приниматься Банком

Можно установить период обмена (например с 08:15 по 19:30), в который банк будет принимать от Клиента сообщения по системе Банк-Клиент в рабочие дни Банка. Сообщения, поступающие в другое время, не будут приниматься Банком.

Кроме стандартной ЭП сообщений (которой подписываются все сообщения системы «Банк-Клиент» при передаче через интернет), можно добавить **дополнительные ЭП документов** (ЭПдок). В этом случае Клиент указывает количество дополнительных ЭПдок, необходимых для передачи документа в банк и создает необходимое число **дополнительных ЭПдок**. Передать документ в банк в этом случае можно будет только после подписывания его нужным числом ЭПдок. Ключи **дополнительных ЭП документов** должны храниться на отдельных сменных носителях, отличных от ключевых носителей ЭП сообщений.

Включить данные механизмы можно по **Заявке** на дополнительные меры безопасности (ЭП Документов, ограничение ip-адреса или времени работы) в системе Банк-Клиент. Заявка распечатывается, заполняется, **подписывается руководителем, заверяется печатью** и передается в банк.

Рекомендуем подключить услугу SMS-информирования, в жтом случае Вы сможете получать SMS-сообщения на свой телефон при поступлении документов по системе Банк-Клиент, регистрации новых ключей ЭП.

Начальник УИТ Р.М. Бикмансуров