АКЦИОНЕРНОЕ ОБЩЕСТВО
БАНКПЕРМЬ

УТВЕРЖДЕНО:
решением Правления Банка Пермь (АО)
(Протокол заседания от 10 декабря 2019 г.)

Председатель Правления

_____ Л.В. Саранская
10 декабря 2019 г.

Рекомендации по безопасному использованию системы Интернет-Банк

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», Положению Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», Положению Банка России от 17 апреля 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

2. В целях защиты информации, передаваемой через систему Интернет-Банк и обеспечения сохранности денежных средств необходимо соблюдать следующие правила:

2.1. Обеспечить сохранность ключевого носителя

При регистрации в системе Интернет-Банк создаются ключи электронной подписи (ЭП). Клиенту необходимо **обеспечить их сохранность** от посторонних лиц.

Ключи электронной подписи (ЭП) необходимо хранить **на отдельном сменном носителе** (флеш-карта, USB-токен и т.д.), не хранить на нем другие данные. Использовать носитель с ключами ЭП только для работы с системой Интернет-Банк, **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 выйдет из строя.

2.2. Ограничить доступ к оборудованию с системой Интернет-Банк

Доступ к оборудованию, на котором установлена система Интернет-Банк, должны иметь только доверенные сотрудники.

Операционная система и все программы, устанавливаемые на оборудовании, 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 внешних носителей для исключения запуска вредоносных программ.

Необходимо предусмотреть невозможность установки посторонними лицами (гостями, посетителями, обслуживающим персоналом) на оборудование с системой Интернет-Банк специальных "шпионских" программ. Хорошей практикой является работа на оборудовании от имени пользователя, не имеющего полномочий администратора.

Нельзя устанавливать программу Интернет-Банк и работать в ней на чужом оборудовании.

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 оборудованию, на котором установлено ПО Интернет-Банк.

2.3. Контролировать состояние денежных средств в банке

Необходимо регулярно проверять состояние денежных средств и документов в банке, просматривая выписки и документы (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" оборудования в момент работы с системой Интернет-Банк, 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 Интернет-Банк. Необходимо подтвердить это бумажным письмом с печатью и подписью руководителя.

2.4. Заменять ключи ЭП в следующих случаях:

Срок действия ключа ЭП составляет 1 год, до окончания срока его действия Клиенту необходимо самостоятельно в системе Интернет-Банк создать новые ключи ЭП и зарегистрировать Сертификат ключа проверки ЭП 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 оборудовании, на котором установлено ПО Интернет-Банк.

При проведении ремонтных и любых других работ на оборудовании с ПО Интернет-Банк сторонними специалистами заранее звоните в банк и предупреждайте о запрете приема банком документов по системе Интернет-Банк. После окончания работ — обязательно **смените ключи ЭП** на новые. Просьбу о запрете приема документов необходимо подтвердить бумажным письмом с печатью и подписью руководителя.

2.5. Использовать все возможности системы Интернет-Банк

Необходимо ограничить суммы документов, передаваемых по системе Интернет-Банк (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 Банк будет принимать от Клиента сообщения по системе Интернет-Банк. Сообщения с других ip-адресов не будут приниматься Банком.

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

Начальник Управления ИТ Р.М. Бикмансуров