АКЦИОНЕРНОЕ ОБЩЕСТВО
БАНКПЕРМЬ

«УТВЕРЖДАЮ»

Председатель Правления
Акционерного общества Банк «Пермь»

_____ Л.В. Саранская
11.03.2024 г.

Рекомендации по безопасному использованию

системы Интернет-Банк

1. Общие положения

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 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. Правила безопасности

В целях защиты информации, передаваемой через систему Интернет-Банк, и обеспечения сохранности денежных средств необходимо соблюдать 5 правил:

2.1. Обеспечение сохранности ключевого носителя

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

Ключи ЭП необходимо хранить **на отдельном сменном носителе**, 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. Ограничение доступа 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 оборудование, 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 и запускать. Незамедлительно удалять обнаруженное вредоносное программное обеспечение (вирусы, шпионские программы и т. д.).

Необходимо отключить "автоматическое выполнение" для подсоединяемых к оборудованию 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 в операционной системе от имени пользователя, не имеющего полномочий администратора.

Нельзя устанавливать программное обеспечение (ПО) Интернет-Банк и работать с ним на чужом оборудовании.

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

Остерегайтесь поддельных сайтов, имитирующих внешний вид сайта банка, использующих в оформлении логотип или название банка. Всегда проверяйте, что работа с системой Интернет-Банк происходит через защищённое соединение с официальным сайтом: https://dbo.bankperm.ru. В браузере рядом с адресом сайта должен быть значок «замок», означающий использование защищённого соединения.

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. Контроль за состоянием 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. Замена ключей 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. Использование всех возможностей 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.

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

Для дополнительной защиты можно установить использование одноразовых паролей при входе в систему и передаче документов. Одноразовый пароль будет приходить в SMS-сообщении на зарегистрированный номер телефона. Таким образом, только владелец номера сможет работать в системе Интернет-Банк.

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.

3. Дополнительная информация о рисках использования системы Интернет-Банк

Согласно статистической информации Банка России наблюдается значительное число переводов денежных средств без добровольного согласия клиента, а именно без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием, в том числе с использованием методов социальной инженерии.

Просим проявлять максимальную бдительность и соблюдать все меры предосторожности при распоряжении денежными средствами.

Также злоумышленники производят действия по вовлечению граждан, в частности молодежи, в дропперство - деятельность по выводу и обналичиванию денежных средств, полученных преступным путем, в том числе с использованием таких электронных средств платежа, как система Интернет-Банк.

Информируем о том, что дропперство интерпретируется как легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем, и участники могут быть привлечены к ответственности в соответствии с Уголовным кодексом РФ.