Правила безопасной работы при использовании сервиса Интернет-банк

Для обеспечения безопасной работы в Интернет-банке Клиент и Уполномоченные лица Клиента обязуются соблюдать следующие организационные меры.

1. Выполнение следующих правил выбора паролей доступа (PIN-кода пользователя и PIN-кода администратора) к Закрытым ключам проверки ЭП

- при первом использовании Ключевого носителя Клиент обязан изменить PIN-код, используемый по умолчанию (12345678 – PIN-код пользователя, 87654321 – PIN-код администратора); в случае последующего использования клиентом ключевого носителя с неизмененными PIN-кодом, используемым по умолчанию, и PIN-кодом администратора, Клиент принимает на себя риски по использованию Ключевого документа неуполномоченными лицами;
- PIN-код пользователя и PIN-код администратора выбираются самостоятельно;
- самостоятельно выбранные PIN-код пользователя и PIN-код администратора подлежат запоминанию и не подлежат разглашению другим лицам;
- если PIN-код пользователя и/или PIN-код администратора записаны на бумаге, то хранятся в месте, недоступном для других лиц;
- PIN-код пользователя содержит не менее 6 и не более 8 различных символов;
- PIN-код пользователя обязательно меняется, если он стал известен другому лицу;
- в качестве PIN-кода пользователя 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.

2. Правила эксплуатации Ключевых носителей

- Клиент признает, что полученный им Ключевой носитель исправен (не заблокирован) и может быть заблокирован (приведен в нерабочее состояние) только в результате действий самого Клиента (Уполномоченного лица), в т.ч. в результате неправильного указания (введения) Уполномоченным лицом PIN-кода пользователя и/или PIN-код администратора;
- Ключевой носитель может быть разблокирован с помощью программного обеспечения, размещенного на сайте производителя (http://www.rutoken.ru/support/download/get/?fid=2), применением функции форматирования. В результате форматирования вся информация (в том числе, ключевая информация) из памяти Ключевого носителя уничтожается и восстановлению не подлежит. После форматирования Ключевого носителя Клиент должен обратиться в Банк для получения нового СКП;
- Ключевые носители хранятся в недоступном для других лиц месте;
- по завершении работы в Интернет-банке или перерыве в работе Ключевой носитель запрещается оставлять подключенным к компьютеру;
- Ключевой носитель используется только для подписания Электронных документов;
- запрещается передача Ключевого носителя другим лицам;
- в случае смены Уполномоченного лица, осуществляющего подпись Электронных документов Электронной подписью, утере Ключевого носителя, а также о любом подозрении на Компрометацию ключа ЭП незамедлительно сообщается в Банк для блокировки работы в Системе.
- не допускаются повреждения Ключевого носителя от механических воздействий (ударов, падения, сотрясения, вибрации и т. п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения — все это может привести к его поломке. Не допускается попадания на Ключевой носитель (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема необходимо принять меры для его очистки. Для очистки корпуса и разъема устройства необходимо использовать сухую безворсовую ткань; использование растворителей и моющих средств недопустимо.
- не рекомендуется прилагать излишние усилия при подсоединении Ключевого носителя к порту компьютера.

— следует избегать ношения Ключевого носителя в кошельке, совместно с ключами, монетами и др. твердыми предметами, т.к. это может привести к его повреждению.

— Запрещается разбирать Ключевое устройство; при этом будет утрачена гарантия производителя на Ключевое устройство. Кроме того, такие действия могут привести к поломке корпуса Ключевого носителя, а также к порче или поломке элементов печатного монтажа и, как следствие, к ненадежной работе или выходу из строя Ключевого носителя.

— не рекомендуется использовать для подключения Ключевого носителя к компьютеру длинные переходники или USB-хабы без дополнительного питания, поскольку из-за этого на вход, предназначенный для Ключевого носителя, может подаваться несоответствующее напряжение.

— запрещается извлекать Ключевой носитель из порта компьютера, если на нем мигает индикатор, это обозначает работу с данными, и прерывание работы может негативно сказаться как на данных, так и на работоспособности Ключевого носителя.

— не рекомендуется оставлять Ключевой носитель подключенным к компьютеру во время включения, выключения перезагрузки, ухода в режимы sleep или hibernate, поскольку в это время возможны перепады напряжения на USB-порте и, как следствие, выход Ключевого носителя из строя.

— при несоблюдении правил эксплуатации Ключевого носителя (в том числе, неправильном указании (введении) и/или невозможности восстановления PIN-кода пользователя и/или PIN-кода администратора к Закрытым ключам ЭП, механическом повреждении Ключевого носителя и пр.), повлекшим за собой неработоспособность Ключевого носителя, указанный Ключевой носитель подлежит замене в Банке на новый в соответствии с действующими Тарифами Банка.

3. Ограничение доступа к рабочим местам, с которых осуществляется работа с Интернет-банком (далее «Рабочие места ИБ»)

— право доступа предоставляется только Уполномоченным лицам, непосредственно осуществляющим работу в сервисе;

— рабочие места ИБ не оставляются без контроля: при кратковременном отсутствии сохраняются все открытые на редактирование документы, средствами операционной системы блокируется рабочее место.

4. Настройка «доверенной среды» и исключение несанкционированного изменения программного обеспечения на рабочих местах ИБ

— используется только лицензионное программное обеспечение;

— устанавливаются все обновления системы безопасности, рекомендуемые производителем операционной системы, установленной на компьютере;

— на компьютере запрещается установка и запуск программ, полученных не из доверенных источников;

— отключается учетная запись для гостевого входа (Guest);

— отключаются режимы отображения окна всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей;

— для всех учетных записей в операционной системе используются пароли (PIN-код пользователя и PIN-код администратора), удовлетворяющие требованиям п.1 настоящего Приложения;

— 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.

5. Соблюдение правил безопасной работы в сети Интернет на рабочих местах Системы

— не допускается открывать сайт системы по ссылкам (особенно баннерным или полученным через почту);

— не допускается отвечать на любые письма с просьбой выслать Закрытый ключ ЭП, пароль (PIN-код пользователя и PIN-код администратора) и другие конфиденциальные данные;

— не допускается устанавливать и сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных Web-сайтов, присланные по электронной почте, полученные в телеконференциях.

6. Правила эксплуатации Логина/Пароля, в том числе при использовании Мобильного приложения

— производить установку Приложения необходимо только из авторизованного магазина приложений (Google Play, App Store);

— необходимо установить код доступа на мобильное устройство Клиента;

— установить и своевременно обновлять лицензионные антивирусные программы на мобильном устройстве Клиента;

— всегда совершать выход из Приложения с помощью пункта меню «Выйти» после окончания работы;

— не хранить Логин и Пароль для доступа, а также код доступа в Мобильное приложение на своем мобильном устройстве или в общедоступном месте, не записывать его на бумагу;

— ни при каких обстоятельствах не сообщать никому (в том числе работникам банка, родственникам и друзьям) Логин, Пароль и Код доступа в Мобильное приложение;

— никогда не отвечать на электронные письма, входящие звонки, SMS-сообщения, письменные/устные обращения, в которых запрашиваются коды доступа, разовые пароли, персональная конфиденциальная информация;

— в случае утери мобильного устройства или в случае обнаружения подозрительных действий, совершенных от вашего имени в Сервисе, незамедлительно обратиться в Банк для смены Логина и Пароля.