Waybank

Правила безопасности Клиента при использовании Системы «Банк-Клиент»

При работе в Системе «Банк-Клиент» (далее – Система) возникает риск получения несанкционированного доступа злоумышленников к секретным ключам электронной подписи (далее – ЭП) и паролям с целью хищения денежных средств. Как правило, хищение денежных средств с расчетных счетов осуществляется:

- бывшими сотрудниками организации, имеющими доступ к секретным ключам ЭП;
- IT – сотрудниками, имеющими доступ к носителям с секретными ключами ЭП, а также к компьютерам, с которых осуществляется работа в Системе;
- злоумышленниками, путем заражения компьютеров, с которых осуществляется работа в Системе, вредоносным кодом (далее – ВК) с последующим дистанционным похищением секретных ключей ЭП и паролей;

С целью снижения рисков, при работе в Системе, рекомендуется соблюдать следующее:

- Для работы с Системой необходимо иметь отдельный компьютер;
- Доступ к компьютеру должны иметь только доверенные лица;
- Обязательно защищать учетные записи пользователей операционной системы паролями;
- При первом входе в систему, а также регулярно, каждый месяц менять пароли на Систему;
- Не работать от имени (под учетной записью) «Администратор»;
- Контролировать действия сотрудников IT- подразделений при обслуживании компьютера, на котором установлена Система;
- Своевременно устанавливать все обновления безопасности, рекомендуемые производителем операционной системы, установленной на компьютере;
- Обязательно установить и настроить на компьютере персональный Firewall;
- Операционная система и необходимое программное обеспечение (далее- ПО) данного компьютера должны быть только лицензионными;
- Используемый компьютер должен быть оснащен антивирусным программным обеспечением с ежедневно обновляемыми базами.
- Не реже одного раза в год производить перегенерацию секретных ключей ЭП;
- Не выполнять никаких рекомендаций, особенно связанных с вводом каких-либо данных на любых страницах, открытых браузером в интернете. Следует иметь в виду, что работники «Вэйбанк» АО (далее – Банк) никогда не обращаются к клиентам по телефону с предложениями попытаться войти в Систему еще раз или ввести еще один код подтверждения, не пытаются узнать у клиентов средства доступа к Системе;
- Включить систему фильтрации ложных web-узлов (антифишинг) в браузере, если браузер ее не имеет, обновить браузер;
- При временном неиспользовании (например, при перерыве, при кратковременном покидании рабочего места), после завершения работы с Системой, рекомендуется выполнить выход из Системы путем выбора соответствующего пункта меню Системы.
- Доступ к данному компьютеру и его использование внутри организации Клиента должен быть регламентирован

Очень опасно хранить секретные ключи ЭП на жестком диске и в реестре. Необходимо хранить секретные ключи и их копии на съемном носителе и держать их в надежном, недоступном для третьих лиц месте (например, сейф).

Использование секретного ключа ЭП должно производиться в момент работы с Системой и контролироваться Вами как Владельцем ключа. Используя нелицензионное ПО и оставляя секретные ключи ЭП без присмотра, Вы рискуете их скомпрометировать и сделать доступными для третьих лиц, т.к. такое ПО может заведомо содержать вредоносный код.

Никогда и никому не сообщайте логины \ пароли Системы и тем более не доверяйте секретные ключи. Даже если этого попросит работник Банка.

В случае, если Вы, как Владелец ключа, доверяете управление своим банковским счетом посредством Системы другому лицу, такая передача управления должна быть зафиксирована юридически, с обязательным письменным уведомлением Банка и предоставлением заверенной нотариально копии доверенности.

В случае, если у Вас:

- Неожиданно сломался компьютер, на котором у Вас установлена Система;
- Заблокировался логин;
- Невозможно зайти в Систему;
- Потерян контроль над носителем с секретными ключами ЭП;
- Потерян контроль над программой «Банк-Клиент»;
- Возникли подозрения в несанкционированном доступе к Системе:
  - появляются \ *исчезают* \ документы, контрагенты;
  - остатки на расчетном счете Клиента в Системе не соответствуют Вашим расчетам;
  - любое другое подозрение,

Вы должны немедленно обратиться в Банк с тем, чтобы решить все возникшие вопросы.

Соблюдая эти простые правила и требования, Вы существенно снизите риски несанкционированного доступа к вашему расчетному счету посредством Системы.

Помните!

Все риски, связанные с утратой и компрометацией секретных ключей, несет Владелец ключа.

Банк не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с нарушением и (или) ненадлежащим исполнением ими Правил безопасности Клиента при использовании Системы «Банк-Клиент».