ТРЕБОВАНИЯ
по обеспечению безопасности при использовании Системы «Клиент - Банк»

Список оборудования и программного обеспечения, которым Клиент должен быть обеспечен для работы в Системе «Клиент - Банк»:

1. Персональный компьютер с операционной системой из семейства MS Windows версии 7 и выше, Linux, Mac OS.
2. Плагин «BIFIT Signer», предназначенный для подписи контента с использованием аппаратных криптопровайдеров. Рекомендуется установить последнею версию. Для этого выберите ссылку для скачивания на странице входа в сервис в зависимости от операционной системы.
3. Драйвер USB-токена.
4. Один из следующих браузеров:
    - Internet Explorer версия 9 и выше;
    - Firefox версия 23 и выше;
    - Opera версия 15 и выше;
    - Safari версия 5 и выше;
    - Chrome версия 23 и выше.
5. Соединение с сетью «Интернет» на скорости не менее 128КБ/с, с возможностью доступа к сайту Банка по адресу https://ibank2.pshb.ru/index.html по следующим портам: 443 (https), 9091 (IBTP).
6. На этапе регистрации требуется наличие принтера для печати Сертификата ключа проверки ЭП.

Клиент Системы «Клиент - Банк» обязан:

- Выделить отдельный компьютер, который будет использоваться только для работы с Системой «Клиент - Банк» и не выполнять на этом компьютере никакие другие задачи.
- Содержать компьютер, на котором установлена Система «Клиент - Банк» в исправном состоянии, в охраняемом служебном помещении, обеспечивающем невозможность несанкционированного доступа к нему.
- Использовать только лицензионное базовое программное обеспечение (операционную систему, офисный пакет, межсетевой экран, антивирус, антишпионское ПО и т.п.).
- Исключить возможность установки программного обеспечения, полученного из ненадежных источников.
- Регулярно устанавливать пакеты обновления безопасности операционной системы.
- Не допускать появления в компьютере, на котором установлена Система «Клиент - Банк» ВК (компьютерных вирусов, программ-шпионов и т.п.).
- На компьютерах, используемых для работы с Системой «Клиент - Банк», исключить посещение Интернет-сайтов, загрузку и установку различного программного обеспечения и т.п. По возможности, полностью запретить все соединения (входящие и исходящие) с сетью Интернет, разрешив только доступ к Системе «Клиент - Банк».
- В качестве Аппаратных средств усиленной ЭП использовать **специализированные устройства - USB-токены** или смарт-карты.
- В случае работы с Системой «Клиент - Банк» без Аппаратных средств усиленной ЭП в качестве файлового хранилища ключей ЭП использовать **съемные носители информации**, например, **USB-флеш-накопитель.** Запрещается хранить ключи ЭП на несъемном жестком диске.
- Для предотвращения несанкционированного доступа к защищаемой информации вне рабочего времени необходимо хранить носители ключевой информации в сейфе.
- Не допускать работу под учетной записью, имеющей права администратора. Необходимо использовать учетную запись с ограниченными правами в операционной системе, установленной на компьютере.
- Отключить учетные записи, позволяющие анонимный (гостевой) вход в операционную систему, установленную на компьютер.
- Исключить возможность автоматической регистрации пользователя в операционной системе без ввода им паролей или парольных фраз, предъявления аппаратных устройств (электронных ключей или смарт-карт), средств достоверного опознавания биометрических характеристик пользователя, или

использования иных аутентификационных механизмов.

- Отключить режимы отображения окна всех зарегистрированных в операционной системе пользователей и быстрого переключения пользователей (ОС из семейства MS Windows).
- Для всех учетных записей в операционной системе и для Ключа ЭП использовать пароли, удовлетворяющие следующим требованиям:
  - Пароль должен содержать не менее 8 различных символов;
  - Пароль обязательно меняется, если он стал известен постороннему лицу;
  - В качестве пароля не используются:
    - последовательности, состоящие из одних цифр;
    - последовательности повторяющихся букв или цифр;
    - идущие подряд в раскладке клавиатуры или в алфавите символы;
    - имена и фамилии, дни рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
    - ИНН или другие реквизиты Клиента.
- Для защиты от несанкционированного доступа из внешней или локальной сети использовать специализированное ПО для защиты информации — антивирусное ПО с регулярно обновляемыми базами, персональные межсетевые экраны, средства защиты от несанкционированного доступа.
- Не оставлять без контроля компьютер, на котором установлена Система «Клиент - Банк», после ввода ключевой информации либо иной конфиденциальной информации;
- Не передавать носители ключевой информации лицам, не допущенным к работе с Системой «Клиент - Банк»;
- Не оставлять носители ключевой информации в компьютере после завершения работы с Системой «Клиент - Банк»;
- Запрещать использование любых средств удаленного (дистанционного) доступа, которые обычно используется IT-специалистами для удаленной поддержки. Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного) и отключением такой функциональности.
- Не вносить никаких изменений в программные средства Системы «Клиент - Банк», не передавать их третьим лицам.
- По требованию Банка передавать ему письменное изложение обстоятельств, связанных с приемом и отправкой документов, ЭП под которыми не была подтверждена как подлинная.
- Немедленно сообщать Банку обо всех случаях, свидетельствующих о попытках посторонних лиц получить доступ к Системе «Клиент - Банк», а также о любой, даже кратковременной потере контроля над носителями ЭП. При подтверждении этих случаев Клиент обязан немедленно поменять все пароли и ЭП лиц, уполномоченных распоряжаться счетом, и зарегистрировать их в Банке.
- Хранить в тайне от посторонних лиц пароли для получения доступа к программным средствам Системы «Клиент - Банк». Эти пароли должны меняться не реже одного раза в месяц и каждый раз при смене состава лиц, уполномоченных распоряжаться счетом Клиента.
- В случае подозрения на компрометацию, а также при утрате (потере, хищении) носителя ключевой информации необходимо немедленно заблокировать ключи. Для этого нужно позвонить в Банк и сообщить «блокировочное слово».
- Периодически просматривать раздел «Банк-клиент», расположенный в сети Интернет по адресу http://pshb.ru/client-bank/bk. В этом разделе содержится регулярно обновляемая информация о мерах по защите от вредоносных программ и действий злоумышленников, угрожающих безопасной работе с Системой «Клиент - Банк».
- При появлении подозрений на заражение компьютера ВК или возникновении странностей в поведении компьютера, а также в случае обнаружения неизвестных программ или нарушения целостности операционной системы, если Клиент заметил проявление необычного поведения программного обеспечения Системы «Клиент - Банк» или какие-то изменения в интерфейсе программы, следует позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии программного обеспечения. Если нет - заблокировать ключи ЭП.

В целях снижения возможного ущерба от несанкционированного доступа к Системе «Клиент - Банк», Банк обязан:

- Немедленно блокировать операции по счету при получении сообщения (Блокировочного слова) Клиента по телефону о хищении или утрате носителей ЭП, совершении или попытке совершения несанкционированных переводов, и иных фактов, дающих основание полагать о возможных хищениях денежных средств Клиента. В течение 1 (Одного) рабочего дня сообщение должно быть подтверждено письменным Уведомлением о блокировке пары ЭП (Приложение № 4).
- При непредставлении Клиентом последующего письменного Уведомления, по истечении 1 (Одного) рабочего дня Банк возобновляет работу Клиента в Системе «Клиент - Банк» в полном объеме.

Банк напоминает Клиенту о том, что:

- Не имеет доступа к ЭП Клиента и не может от имени Клиента сформировать корректную ЭП под ЭД;
- Не осуществляет рассылку электронных писем с просьбой прислать ЭП Клиента, пароль или иную информацию о Системе «Клиент - Банк». Не допускается отвечать на подозрительные письма с просьбой выслать ключ ЭП, пароль и другие конфиденциальные данные;
- Банк не рассылает по электронной почте программы для установки на компьютеры Клиента. Если Клиент получил подобное письмо от имени Банка, содержащее программу для установки или запрос на предоставление паролей, ЭП, необходимо незамедлительно сообщить об этом по телефону технической поддержки Клиентов Банка. Не допускается запускать на исполнение или сохранять в файловой системе компьютера подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных WEB-сайтов, присланные по электронной почте, полученные в телеконференциях;
- Не допускается открывать сайт Системы «Клиент - Банк» по ссылкам (особенно баннерным или полученным через почту);
- Не рекомендуется посещать непроверенные сайты в сети Интернет, особенно те, которые распространяют пиратское программное обеспечение, музыкальные и видеофайлы, так как при входе на такие сайты можно заразить компьютер ВК;
- Информация, обрабатываемая в Системе «Клиент - Банк», является конфиденциальной и требует защиты от несанкционированного доступа к ней в соответствии с действующим законодательством;
- В сети «Интернет» возможно появление ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемой Банком Системы «Клиент - Банк», и (или) использующих зарегистрированные товарные знаки и наименование Банка, поэтому Пользователю рекомендуется обращать внимание на любые отличия от привычного интерфейса и незамедлительно информировать об этом Банк, использовать антифишинговые возможности браузеров и средств обнаружения ВК;
- Если Клиент использует более одной группы ключей ЭП (для отправки документов требуется по одной ЭП из каждой группы), то ключи разных групп рекомендуется хранить на разных носителях ключевой информации и использовать на разных компьютерах. Это позволит существенно снизить риск негативных последствий в случае заражения ВК одного из компьютеров Клиента;
- Ни один антивирус не гарантирует полную защиту от ВК, которые постоянно совершенствуются их авторами. Необходимо максимально серьезно относится к поступающим из Банка предупреждениям, о новых разновидностях ВК, о способах защиты от их воздействия, устранения последствий такого воздействия, о возможном заражении компьютера Клиента ВК и следовать рекомендациям уполномоченных работников Банка;
- При использовании средств подтверждения платежей, важно обращать внимание на присылаемые в SMS вместе с одноразовым паролем и отображаемые на экране реквизиты подтверждаемого платежа. Это позволит избежать подмены платёжных реквизитов ВК.

После ознакомления с Приложением № 6 Клиент подтверждает, что ему известны последствия несоблюдения вышеуказанных требований безопасности, и он полностью берет на себя ответственность за такие последствия в случае нарушения требований безопасности. Банк освобождается от ответственности за несанкционированное списание денежных средств со счета Клиента вследствие воздействия ВК из-за несоблюдения Клиентом вышеуказанных требований безопасности.