

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

### 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» вредоносного кода (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».
- Для предотвращения несанкционированного доступа к защищаемой информации вне рабочего времени необходимо хранить носители ключевой информации (USB-токены) 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 (USB-токены) 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 меж сетевого 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 «кодовое слово».

- При появлении подозрений на заражение компьютера вредоносным кодом 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.

**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 вредоносным кодом;
- 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 вредоносного кода;
- Если Клиент использует более одного ключа ЭП, то ключи рекомендуется хранить на разных носителях ключевой информации и использовать на разных компьютерах. Это позволит существенно снизить риск негативных последствий в случае заражения вредоносным кодом одного из компьютеров Клиента;
- Ни один антивирус не гарантирует полную защиту от вредоносных кодов, которые постоянно совершенствуются их авторами. Необходимо максимально серьезно относиться к поступающим из Банка предупреждениям о новых разновидностях вредоносного кода, о способах защиты от их воздействия, устранения последствий такого воздействия, о возможном заражении компьютера Клиента вредоносным кодом и следовать рекомендациям уполномоченных работников Банка.