

ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для минимизации рисков несанкционированного доступа к Счетам Клиента со стороны злоумышленников и компрометации ключевой информации, Банк настоятельно просит Клиентов соблюдать следующие меры информационной безопасности:

- Выделить компьютер, который не будет использоваться в иных целях, кроме как для работы в Системе; не осуществлять, а при наличии технической возможности, запретить выход в Интернет с этого компьютера на иные адреса, за исключением адресов серверов Банка.
- Ограничить или полностью запретить удаленный доступ к выделенному компьютеру с других компьютеров локальной сети. Не использовать средства удаленного администрирования на выделенном компьютере. При наличии технических средств, поместить выделенный компьютер в отдельную сеть, контролируемую межсетевым экраном и системами обнаружения атак.
- Заменить все стандартные пароли, заданные при установке Системы, на уникальные собственные, производить периодическую смену паролей (не реже одного раза в три месяца).
- Использовать на постоянной основе антивирусное программное обеспечение с последней актуальной версией баз.
- Регулярно (не реже одного раза в неделю) выполнять антивирусную проверку для своевременного обнаружения вредоносных программ.
- Использовать на компьютере исключительно лицензионное программное обеспечение.
- Регулярно (не реже одного раза в месяц или по факту публикации) устанавливать обновления операционной системы.
- Проверить группу «Администраторы» на выделенном компьютере, исключить всех рядовых пользователей из этой группы, не работающих с Системой.
- При наличии технической возможности, для пользователей, работающих с Системой – создать отдельную групповую политику, разрешающую запуск только определенных приложений.
- Для доступа к серверам Банка использовать только заведомо известные Вам адреса интернет серверов Банка.
- В случае отсутствия возможности подключения к серверу Банка незамедлительно сообщать об этом Банку.
- Хранить в безопасном месте (в сейфе) и никому не передавать носители с ключевой информацией, обеспечив к ним доступ только уполномоченных лиц.
- Никогда не осуществлять копирование закрытых (секретных) ключей электронной подписи на локальный жесткий диск компьютера, даже с последующим его удалением.
- Регулярно (не реже одного раза в месяц) проверять целостность ключевых носителей, проводя проверку наличия на них файлов электронной подписи.
- Своевременно (в соответствии с условиями Соглашения) проводить Плановую смену рабочих ключей*.
- Не оставлять носители с ключевой информацией без присмотра, подключать их к компьютеру только на время использования и незамедлительно их отключать после

проведения банковских операций. При оставлении рабочего места Системы без присмотра всегда блокировать экран с последующим вводом пароля для его разблокировки.

- Производить незамедлительную замену ключей электронной подписи в случае их компрометации или подозрении на компрометацию.
- Своевременно устанавливать все обновления Системы.
- Не устанавливать обновления, а также не открывать ссылки в почтовых сообщениях, полученных от имени Банка по электронной почте, не открывать ссылки в таких почтовых сообщениях, получив такое сообщение, незамедлительно сообщать об этом Банку.
- Ежедневно, в течение операционного дня Банка и по окончании рабочего дня, осуществлять дополнительный вход в Систему для контроля перечня исходящих документов за текущий день. При обнаружении подозрительных документов, незамедлительно обращаться в Банк.
- В случае подозрений на замедление работы компьютера отключить компьютер физически от локальной сети и интернет и обратиться к системному администратору с просьбой о необходимости проведения полной антивирусной проверки сканированием всех файлов и памяти компьютера.
- В случае, если инцидент информационной безопасности все же произошел, ни в коем случае не выключать компьютер, а отключить его физически только от локальной сети и интернет, незамедлительно обратиться к системному администратору и сообщить об инциденте в Банк для проведения оперативного расследования и принятия необходимых мер для сбора доказательств.
- В случае выявления Клиентом подозрительных операций в Системе незамедлительно сообщать об этом в Банк.

* – для СКЗИ «КриптоПро»