

МЕРЫ БЕЗОПАСНОЙ РАБОТЫ В СИСТЕМЕ ИНТЕРНЕТ-БАНК.

- При входе в систему Интернет-банк (далее по тексту – Система) проверять адрес страницы и наличие соответствующего SSL сертификата, правильный адрес - <https://ibank.slbank.ru/>.
- Не знакомить с программным обеспечением и технической документацией по Системе лиц, не имеющих права доступа к системе.
- Подключать носитель электронной подписи (токен) только для выполнения необходимых операций в Системе. После завершения работы, токен должен быть отключен от компьютера и убран на хранение. Запрещено оставлять токен постоянно подключенным к компьютеру.
- Использовать как пограничный межсетевой экран на оборудовании доступа к системе провайдера, так и персональный межсетевой экран на компьютере.
- На оборудовании доступа к сети Интернет исключить использование стандартных (заданных производителем) паролей.
- При работе с сетью Интернет использовать статический IP адрес (при наличии технической возможности) и привязать этот адрес к договору с банком для исключения случаев использования токена за пределами организации.
- Подключить услугу смс-уведомление о входе в систему и движениях по счету, чтобы своевременно узнавать о фактах возможного несанкционированного доступа в Систему.
- Один раз в два-три месяца изменять пароль доступа к Системе.
- При возникновении сбоев в работе Системы обращаться за технической помощью только к специалистам Банка.
- При возникновении подозрений на взлом Системы немедленно оповестить сотрудников Банка и заблокировать токен.

МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ (ЭП).

- Токен с ЭП необходимо хранить в надежно запирающемся сейфе или шкафу.
- Пароль на доступ к ключу ЭП должен быть известен только Вам как владельцу.
- Не допускайте постоянного и бесконтрольного подключения к компьютеру токена.
- Не передавайте токена с ключами ЭП никому.
- Не пользуйтесь Системой в Интернет-кафе, а также там, где Вы не уверены в безопасности компьютеров.
- При увольнении ответственного сотрудника, имевшего доступ к ключу ЭП, обязательно сообщите в Банк и заблокируйте ключ.
- При возникновении любых подозрений на компрометацию ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно сообщите в Банк и заблокируйте ключи ЭП.

МЕРЫ ПО ЗАЩИТЕ КОМПЬЮТЕРА, С КОТОРОГО ОСУЩЕСТВЛЯЕТСЯ РАБОТА В СИСТЕМЕ:

- Соблюдайте регламент ограниченного физического доступа к данному компьютеру. Должен быть утвержден список сотрудников организации, включая ответственных сотрудников и технический персонал, которым разрешен доступ к компьютерам, с которых осуществляется работа в Системе.
- Рекомендуется использовать отдельный компьютер исключительно для работы в Системе. Другие действия (работа с другими программами, работа с электронной почтой, посещение сайтов в Интернете) с этого компьютера осуществляться не должны.
- Используйте в работе только лицензионное ПО. Не загружайте и не устанавливайте ПО, полученное из непроверенных источников.
- Старайтесь использовать современные операционные системы (ОС). Данные системы

являются более защищенными, в отличие от предыдущих, зачастую устаревших версий. Своевременно устанавливайте исправления и обновления для ОС. Включите автоматическое обновление ОС, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости ОС.

- Используйте системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность данных на получаемых носителях или загружаемых из Интернета обновлениях.

- Используйте и оперативно обновляйте специализированное ПО для защиты информации — антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.

- В антивирусном программном обеспечении должны быть постоянно включены функции мониторинга системы в реальном времени, мониторинга WEB - и E-mail – трафика, мониторинга подключения съемных устройств и не менее одного раза в неделю полная проверка компьютера на наличие вредоносных программ.

- Не устанавливайте на компьютер, где установлено программное обеспечение Системы, программное обеспечение удаленного доступа, а также отключите штатные средства удаленного доступа (Удаленный помощник и Удаленный доступ к системе), примите меры для предотвращения установки подобного рода программ.

- Не подключайте к компьютеру непроверенные на наличие вирусов отчуждаемые носители (Flash-диски, CD, DVD).

- У учетных записей пользователей, работающих с Системой должны отсутствовать административные права на компьютере.

- У учетных записей пользователей, имеющих права входа в систему должны использоваться сложные пароли, с периодичностью раз в два-три месяца их необходимо менять.

- На компьютере где используется Система необходимо отключить учетные записи гостей и ограничить круг лиц, владеющих паролем администратора.

ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ.

- Не нажимайте на всплывающие окна, которые содержат рекламу. Желательно настроить Ваш браузер на автоматическую блокировку таких окон.

- Не посещайте непроверенные и небезопасные сайты. Вы можете непреднамеренно загрузить на свой компьютер вирусы и шпионские программы.

- Не читайте подозрительных электронных писем от незнакомых людей, они могут содержать вирусы. Читайте темы сообщений внимательно, если не уверены, что письмо пришло из надежного источника, не открывайте его. Не доверяйте дружественному тону сообщений или срочности содержащейся в них просьбы. В подозрительных письмах не нажимайте на содержащиеся в письме ссылки, а также не открывайте вложенные файлы, особенно если в письме указано, что проблема безотлагательная, и при этом просят срочно открыть приложенный файл.

- Максимально ограничьте использование Интернет-мессенджеров (Viber, ICQ, Telegram и пр.).

- Будьте внимательнее к странным или непонятным сообщениям об ошибках браузера. В случае возникновения подозрений просканируйте свой компьютер на наличие вирусов или шпионского ПО.

За дополнительной информацией обращайтесь только к сотрудникам Банка по телефонам (3452) 566-026 и 8-800-100-60-26