телепорт банк

ПРАВИЛА
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ «UBS-HOME»

Настоящие Правила разработаны в целях:

- Предотвращения хищения денежных средств, находящихся на банковских счетах при осуществлении расчетов с использованием Системы ДБО «UBS-HOME».
- Минимизации рисков проведения злоумышленниками несанкционированных платежей с использованием Системы ДБО «UBS-HOME».

Пользователю Системы ДБО «UBS-HOME» необходимо:

1. При использовании Веб-приложения обеспечить безопасность своего АРМ:

- Применять на своем АРМ, лицензионное системное, прикладное и антивирусное программное обеспечение (далее по тексту – ПО).
- Своевременно устанавливать на АРМ необходимые обновления системы безопасности, обновления системного, прикладного и антивирусного ПО, обновления модулей и баз антивирусного ПО.
- Еженедельно производить полную проверку АРМ на наличие/отсутствие вредоносного кода.
- Применять на АРМ специализированные программные средства безопасности – персональные межсетевые экраны, а также средние или высокие параметры безопасности и конфиденциальности установленного на АРМ Интернет – браузера.
- При работе в сети Интернет никогда не соглашаться на установку каких-либо дополнительных программ или компонентов от неизвестных источников. Исключить посещение сайтов сомнительного содержания.
- При работе с электронной почтой не открывать письма и вложенные в них файлы, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
- Исключить возможность удаленно подключиться к АРМ:
- На АРМ, используемом для работы в Системе ДБО «UBS-HOME», не должно быть установлено программ удаленного администрирования и доступа к данному АРМ из вне.
- В повседневной работе на АРМ входить в систему под учетной записью с правами ограниченного доступа (как обычный пользователь), не имеющего неограниченные права администратора системы. Учетная запись "Гость" в системе АРМ должна быть выключена.
- Учетные записи пользователей АРМ (в том числе, но не исключая, учетные записи администратора операционной системы) не должны содержать простые пароли. Пароли учетных записей, при возможности, должны содержать не менее 8 символов, включающие в себя строчные и прописные буквы латинского алфавита, цифры и символы верхнего регистра клавиатуры. Смена пароля пользователя должна производиться не реже одного раза в месяц.
- Использовать для подтверждения расчетных (платежных) документов услугу SMS-код.
- Установить пароль на SIM-карту телефона сотовой связи, используемую, для получения SMS-кода – это не позволит злоумышленникам, в случае хищения телефона сотовой связи получить доступ к SMS-кодам путем перестановки SIM-карты в другое устройство.
- Обеспечить сохранность носителя ключа ЭП и обеспечить невозможность попадания носителя ключа ЭП в посторонние руки.
- Никогда не оставлять носитель ключа ЭП, вставленный в АРМ, без внимания. При окончании работы незамедлительно вынимать носитель и помещать его в безопасное место.
- Сохранять пароль для доступа в Систему ДБО «UBS-HOME» в секрете:
- Запомнить Пароль доступа в Систему ДБО «UBS-HOME». Никогда не разглашать и не записывать его в местах, доступных посторонним лицам. Периодически (не реже одного раза в месяц) менять Пароль доступа в Систему ДБО «UBS-HOME».
- Никому и никогда не сообщать сведения о Пароле в Систему ДБО «UBS-HOME», включая сотрудников Банка. Банк никогда не запрашивает данную информацию.
- Прежде чем ввести Логин и Пароль в Системе ДБО «UBS-HOME», необходимо убедиться, что адресная строка при входе в Систему начинается с https:// и отображается именно адрес https://dbo.teleportbank.ru:7887.
- Если в адресной строке не указано "https", вводить данные нельзя. В таком случае или случае появления предупреждений Интернет-браузера о перенаправлении на другой сайт при подключении к Системе ДБО «UBS-HOME», следует немедленно прекратить работу с Системой ДБО «UBS-HOME» и обратиться в рабочее время по телефонам, указанным на официальном сайте Банка.
- В случае появления предупреждений Интернет-браузера о перенаправлении на другой сайт, при подключении к Системе ДБО «UBS-HOME», немедленно обратиться в рабочее время по телефонам, указанным на официальном сайте Банка, отложив при этом совершение всех финансовых операций.
- В случае сбоев в работе АРМ, его поломки во время работы с Системой ДБО «UBS-HOME», или сразу после сеанса работы (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.),

немедленно обратиться в Банк в рабочее время по телефонам, указанным на официальном сайте Банка, и убедиться, что не производились несанкционированные переводы денежных средств.

1. При использовании Мобильного приложения обеспечить безопасность своего Мобильного устройства:

- Установить пароль на доступ к Мобильному устройству. Использовать сложный пароль или пин-код.
- Не использовать Мобильные устройства с расширенными правами (Jailbreak, Root или иные операции, не поддерживаемые официально производителями).
- Установите на Мобильном устройстве и регулярно обновлять мобильный антивирус.
- Своевременно устанавливать обновления для Вашего мобильного устройства и установленных на нем приложений. Установку производить только из доверенных источников.
- Не допускать установку или обновление приложений по ссылке в e-mail / SMS-сообщении от имени Банка (Банк никогда не высылает писем и SMS-сообщений с прямыми ссылками на установку или обновление приложений.
- При установке на Мобильное устройство дополнительного программного обеспечения обращать внимание на полномочия, которые необходимы программе. Не допускать установки программ, которым требуются излишние полномочия, особенно в части чтения и отправки SMS-сообщений, доступа к сети Интернет, клавиатуре и т.п.
- Если на Мобильное устройство перестали приходить SMS- сообщения, в том числе перестали приходить SMS-пароли от Банка, необходимо прекратить использование Мобильного устройства. В данном случае возможно мошенничество с заражением Мобильного устройства вирусом, перехватывающим SMS-сообщения.
- Для проверки рекомендуется установить SIM-карту в другое Мобильное устройство, провести операцию в Системе и дождаться прихода SMS-пароля.
- В случае выявления подозрительной работы устройства (самопроизвольные звонки и рассылки SMS-сообщений, несанкционированная загрузка и установка программного обеспечения) необходимо незамедлительно сообщить об этом в Банк с целью приостановления доступа в Систему.
- Осуществлять установку и обновление Мобильного приложения на Мобильном устройстве только в Интернет-магазинах RuStore, GooglePlay, Huawei AppGallery и AppStore, не устанавливать и не обновлять Мобильное приложение с использованием других Интернет-сайтов, переходов по ссылкам с других Интернет-сайтов и т.п.
- В случае утери/кражи/изъятия телефона и/или SIM-карты с номером телефона сотовой связи Клиента, указанного в Заявлении, Мобильного устройства с установленным Мобильным приложением, либо при возникновении риска несанкционированного использования указанного телефона / номера телефона, незамедлительно сообщить об этом в Банк с целью приостановления доступа в Систему.
- В случае Компрометации Кода мобильного приложения, Клиент обязан незамедлительно перерегистрироваться в Мобильном приложении, используя новый Код мобильного приложения.

2. При работе в Системе ДБО «UBS-HOME»:

- Не работать с Системой ДБО «UBS-HOME» через публичные сети Wi-Fi и т.п. (интернет-кафе, компьютерные салоны, иные общественные места), а равно используя чужие электронные устройства.
- Обращать внимание на любые изменения в привычных процессах установления соединения с Системой ДБО «UBS-HOME». При возникновении любых сомнений в правильности функционирования Системы ДБО «UBS-HOME», необходимо немедленно обратиться в рабочее время по телефонам, указанным на официальном сайте Банка.
- Никому не сообщать содержание полученных от Банка SMS- сообщений. При поступлении подозрительных звонков от имени Банка, Центрального Банка (Банка России), правоохранительных органов с просьбой предоставить какие-либо данные, касающиеся, персональных данных, счетов, пластиковых карт и содержания поступивших SMS- сообщений, немедленно прекратить разговор и самостоятельно обратиться в Банк по указанным на официальном сайте Банка телефонам в рабочее время.
- Регулярно контролировать состояние своих счетов в Системе ДБО «UBS-HOME» и незамедлительно сообщать работникам Банка в рабочее время по телефонам, указанным на официальном сайте Банка, обо всех подозрительных или несанкционированных финансовых операциях.
- При возникновении любых подозрений на компрометацию учетной записи в Системе ДБО «UBS-HOME» или компрометацию среды исполнения (наличие в электронном устройстве вредоносных программ) – незамедлительно позвонить в рабочее время по телефонам, указанным на официальном сайте Банка, временно заблокировать учетную запись в Системе ДБО «UBS-HOME» и следовать инструкциям работников Банка.
- В случае утраты телефона сотовой связи и /или носителя Ключа ЭП (потеря, хищение, поломка), при смене номера телефона сотовой связи, немедленно обратиться в Банк в рабочее время по телефонам, указанным на официальном сайте Банка, и убедиться, что не производились несанкционированные переводы денежных средств.