телепорт банк

ПРАВИЛА ОРГАНИЗАЦИИ И ОСУЩЕСТВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ в системе ДБО «UBS-HOME» для физических лиц

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила организации и осуществления обмена электронными документами в системе ДБО «UBS-HOME» для физических лиц (далее Система), не являющимися индивидуальными предпринимателями или не занимающимися в установленном законодательством Российской Федерации порядке частной практикой (далее – Правила) разработаны в соответствии с законодательством Российской Федерации и иными нормативными актами.

1.2. Настоящие Правила являются публичным предложением (офертой) Банка заключить Договор об электронных расчетах с использованием Системы дистанционного банковского обслуживания на определенных Правилами условиях. Присоединение к Правилам производится в соответствии со ст. 428 Гражданского кодекса Российской Федерации для чего заинтересованное лицо, с учетом п. 1.4 настоящих Правил, должно представить в Банк надлежащим образом заполненное и подписанное Заявление на подключение к Системе ДБО, установленной Банком формы, а также иные необходимые документы и информацию. Присоединение к Правилам означает также присоединение к Регламенту Удостоверяющего центра АО «ТелеПорт Банк», размещенному на сайте Банка

1.3. Договор об электронных расчетах считается заключенным с момента проставления на Заявлении на подключение к Системе ДБО подписи уполномоченным сотрудником Банка.

1.4. Настоящие Правила не регулируют обмен Банка электронными документами с кредитными организациями, юридическими лицами и индивидуальными предпринимателями.

1.5. Если не указано иное, термины и определения, применяемые в тексте настоящих Правил, означают следующее:

АБС – автоматизированная банковская Система;

Автоматизированное рабочее место (АРМ) – комплекс программно-технических средств, используемых Клиентом для обмена ЭД;

Банк – Акционерное общество «ТелеПорт Банк», являющийся оператором Системы;

Биометрический метод идентификации – способ входа в Мобильное приложение и доступа к Ключу ЭП, посредством которого Пароль или Код мобильного приложения вводится с использованием технологии Face ID (только для устройств Apple) или отпечатка пальца Клиента, зарегистрированного в Мобильном устройстве, на котором установлено Мобильное приложение. Возможность использования Биометрического метода идентификации обеспечивается программно-аппаратными средствами Мобильного устройства Клиента и активируется Клиентом в Мобильном приложении после успешной Аутентификации посредством введения корректных Логина, Пароля и Кода подтверждения. Банк не получает, не анализирует и не хранит отпечаток пальца Клиента и снимки лица Клиента, используемые при Биометрическом методе идентификации;

Владелец ЭП – физическое лицо, указанное в Карточке с образцами подписей, владелец денежных средств, находящихся на Счете, Ключ проверки ЭП которого зарегистрирован в Системе;

Веб-приложение (web-приложение) – это программное обеспечение, установленное на стороне Банка и доступное через веб-браузер, которое обеспечивает работу Клиента в системе ДБО;

Договор – заключенный между Банком и Клиентом договор банковского счета, договор банковского вклада, договор о предоставлении и обслуживании банковской карты и открытии специального карточного счета, договор аренды ячейки банковского сейфа, иной договор, при исполнении которого возможно использование Системы ДБО «UBS-HOME»;

Договор об электронных расчетах с использованием Системы ДБО (Договор об электронных расчетах):

- при использовании **Веб-приложения** это совместно представленное Клиентом Заявление на подключение к Системе ДБО установленной Банком формы и настоящие Правила;
- при использовании **Мобильного приложения** это заполненная и подтвержденная Клиентом форма регистрации в Мобильном приложении и настоящие Правила.

Документация – документация по установке и эксплуатации Системы и средств ЭП;

Дополнительное подтверждение – подтверждение корректности поступившего в Банк ЭПД Клиента посредством введения кода подтверждения, полученного владельцем ЭП в виде SMS-сообщения;

Клиент – физическое лицо, заключившее (заключающее) с Банком Договор об электронных расчетах в порядке, предусмотренном настоящими Правилами;

Ключ ЭП – уникальная последовательность символов, предназначенная для создания электронной подписи электронного документа с использованием средств ЭП;

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с Ключом ЭП, предназначенная для проверки подлинности с использованием средств ЭП электронной подписи электронного документа;

Код мобильного приложения – 5-значный цифровой код, присваиваемый Клиентом для авторизации доступа к Мобильному приложению и Ключу ЭП, для подписания электронного документа;

Кодовое слово – заявленное Клиентом в Банк слово, используемое Банком для подтверждения того, что обратившееся в Банк по телефону с заявлением о компрометации или для сброса пароля, лицо является Клиентом. Кодовое слово используется исключительно в случае компрометации или при необходимости сброса пароля для доступа к Системе;

Компрометация ключа ЭП (Компрометация) – факт несанкционированного доступа или подозрение на несанкционированный доступ к носителю ключевой информации (Ключу ЭП). К событиям, связанным с компрометацией, относятся, включая, но не ограничиваясь:

- утрата носителя ключевой информации, в том числе с последующим его обнаружением;
- доступ посторонних лиц к носителю ключевой информации;
- несанкционированный удаленный доступ к носителю ключевой информации;
- утрата Мобильного устройства, на которое установлено мобильное приложение и/или телефона сотовой связи (SIM-карты), на который направляются Одноразовые пароли, в том числе с последующим обнаружением;
- получение доступа, в том числе удалённого, или подозрение на получение доступа третьим лицом к Учётным данным, телефону сотовой связи (SIM-карте), на который направляются Одноразовые пароли, Мобильному устройству или к АРМ Клиента;
- выявление наличия на телефоне сотовой связи, на который направляются Одноразовые пароли, или на АРМ Клиента вредоносных программ;
- прекращение, в том числе временное, пользования Клиентом номером телефона сотовой связи (SIM-картой), указанным в Сведениях о Клиенте, по любой причине, в том числе в результате недобросовестных действий третьих лиц;
- иные обстоятельства, когда нельзя достоверно установить, что произошло с носителем ключевой информации, и прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа;

Корректная ЭП – ЭП электронного документа, дающая положительный результат её проверки с помощью Ключа проверки ЭП;

Криптографическая защита – защита Электронного документа от несанкционированного изменения и доступа к его содержимому посторонних лиц при помощи алгоритмов криптографического преобразования. В рамках Системы под криптографической защитой понимается шифрование, электронная подпись и вычисление хэш-функций программного обеспечения;
Логин – последовательность символов, являющаяся идентификатором Клиента в Системе;
Люди с инвалидностью (ЛСИ) – люди, которые имеют нарушение здоровья со стойким расстройством функций организма, обусловленное заболеваниями, последствиями травм или дефектами, приводящее к ограничению жизнедеятельности;
Маломобильные группы населения (МГН) – люди, испытывающие затруднения при самостоятельном передвижении, получении услуги, необходимой информации или при ориентировании в пространстве (люди с временным нарушением здоровья, беременные женщины, люди пожилого возраста, люди с детскими колясками и т.п.);
Мобильное приложение - канал дистанционного доступа, представляющий собой версию программного обеспечения, созданную для установки на Мобильных устройствах под управлением операционных систем Android и iOS и позволяющую осуществлять доступ через
Интернет с таких мобильных устройств к Системе ДБО «UBS-HOME». Мобильное приложение размещается Банком только в магазинах приложений RuStore, GooglePlay, Huawei AppGallery и AppStore;
Мобильное устройство - смартфон, планшетный компьютер, мобильный телефон и прочие электронные устройства;
Носитель ключевой информации (носитель ключа ЭП, USB-токен) – отчуждаемое (извлекаемое из компьютера) персональное средство аутентификации и защищенного хранения данных, исключающее возможность просмотра, изменения, копирования и печати содержимого. Использование USB-токенов является обязательным условием при работе в Системе в рамках Договора об электронных расчетах; В Системе используются сертифицированные ФСБ России USB-токены Рутокен ЭЦП с аппаратной поддержкой российских криптографических алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012;
Одноразовый пароль (SMS-код) – средство подтверждения, цифровая последовательность, направляемая Клиенту посредством SMS-сообщения на номер телефона сотовой связи, указанный Клиентом в Сведениях о Клиенте;
Пароль – известная только Клиенту последовательность символов, используемая Клиентом совместно с Логином для получения доступа к Системе;
Подлинность ЭД – положительный результат проверки ЭП, позволяющий установить авторство и факт неизменности содержания ЭД, включая все его реквизиты;
Подразделение – головной офис, дополнительные офисы или иные структурные подразделения Банка, осуществляющие операции по банковским счетам физических лиц;
Программное обеспечение (ПО) – комплекс программ, обеспечивающий обработку и передачу данных, предназначенных для многократного использования и применения Сторонами;
Простая электронная подпись (ПЭП) – это электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом;
Руководство пользователя – инструкция о порядке доступа и совершения операций Клиентом с использованием Системы ДБО;
Сертификат ключа проверки ЭП (Сертификат) – Электронный документ или документ на бумажном носителе, сформированной Системой и подтверждающий принадлежность Ключа проверки ЭП владельцу Сертификата Ключа проверки ЭП;
Система дистанционного банковского обслуживания «UBS-HOME» для физических лиц (Система ДБО, Система) –система дистанционного банковского обслуживания Банка, включающая программно-аппаратный комплекс, состоящий из средств формирования, обработки, хранения и передачи электронных документов, а также средств электронной подписи, позволяющая Сторонам осуществлять защищенный обмен Электронными документами посредством сети Интернет. Система не имеет локальной базы данных Клиента на АРМ Клиента, доступ к базе данных Системы на сервере Банка осуществляется непосредственно с АРМ Клиента. В качестве Системы ДБО Банком используется модуль ДБО автоматизированной банковской системы "UBS.NET" (ЮниСАБ). Разработчиком системы является ООО «Юнион Бизнес Софт»;
Система Антифрод (фрод-мониторинг) – установленная в Банке интеллектуальная система, предназначенная для оценки финансовых транзакций на предмет подозрительности с точки зрения мошенничества и предлагающая рекомендации по их дальнейшей обработке;
Согласительная комиссия – комиссия, создаваемая для разрешения разногласий и споров между Клиентом и Банком при исполнении Договора об электронных расчетах;
Средства ЭП – средства криптографической защиты информации (СКЗИ), используемые для создания ЭП, проверки ЭП, создания ключа ЭП и ключа проверки ЭП. В системе используется СКЗИ «КриптоПро CSP» (разработчик ООО «КРИПТО-ПРО»), соответствующее ГОСТ Р 34.10-2012 и требованиям нормативных актов Российской Федерации;
Специальный карточный счёт (СКС) – банковский счет Клиента в Банке, открытый для отражения операций, совершаемых с использованием платежных карт;
Стороны – Банк и Клиент;
Счет – счет Клиента в Банке (текущий счет, счет по вкладу, специальный карточный счет), доступ к которому осуществляется с использованием Системы;
Тарифы – Перечень тарифов за оказываемые Банком услуги по расчетно-кассовому обслуживанию юридических лиц, установленный Банком;
Удостоверяющий центр (УЦ) – невыделенное подразделение АО «ТелеПорт Банк», осуществляющее функции по созданию и выдаче сертификатов ключа проверки ЭП, а также иные функции, предусмотренные законодательством Российской Федерации. Удостоверяющий центр АО «ТелеПорт Банк» является не аккредитованным удостоверяющим центром и действует в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи". УЦ расположен по месту нахождения Головного офиса Банка. В УЦ Банка используется программно-аппаратный комплекс Удостоверяющий центр «КриптоПро УЦ» версии 2.0 (Исполнение 15) класс КС2» (разработчик ООО «КРИПТО-ПРО»), имеющий сертификат ФСБ России;
Учётные данные - Логин и Пароль;
Хэш-функция – определенный математический способ проверки целостности ЭД, результат которого изображается в виде последовательности шестнадцатеричных цифр. Реализованный в Системе алгоритм вычисления хэш-функции соответствует стандарту ГОСТ Р 34.11-2012;
Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, которая используется для определения лица, подписавшего информацию;

При использовании **Веб-приложения** в Системе применяется усиленная неквалифицированная электронная подпись (УНЭП), созданная с использованием средств электронной подписи (КриптоПро CSP) и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, при осуществлении регулирования в соответствии с пунктом "ш" части первой статьи 13 Федерального закона от 3 апреля 1995 года N 40-ФЗ "О федеральной службе безопасности";

При использовании **Мобильного приложения** в Системе применяется одноключевая усиленная неквалифицированная электронная подпись (имитозащита информации с аутентификацией отправителя), создаваемая с использованием Программного комплекс «Signal-COM AuthKey Server», реализованного с использованием СКЗИ «Signal-COM JCP 3.1», имеющего сертификат ФСБ России, обеспечивающего создание и проверку электронной подписи на основе симметричных ключей ЭП;
Электронный документ (ЭД) – документ в электронной форме, формируемый в формате Системы и/или посредством вложения файла формата Microsoft Word, Microsoft Excel или файла, содержащего графический экземпляр документа, подписанный (защищенный) ЭП,

и имеющий равную юридическую силу с документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным оттиском печати;
Электронный платежный документ (ЭПД) – ЭД, подписанный ЭП, являющийся основанием для совершения операций по Счету Клиента;
Электронное средство платежа – средство и (или) способ, позволяющие Клиенту Банка составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно – коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств;
Push-уведомление – сообщение, состоящее из буквенно-цифровых символов, направляемое Банком на Мобильное приложение Клиента, ранее зарегистрированное в Банке. Для передачи Push-сообщений необходимо наличие подключения Мобильного устройства Клиента к сети Интернет;
SMS-сообщение - сообщение, состоящее из буквенно-цифровых символов, направляемое Банком на номер телефона сотовой связи, указанный Клиентом в Заявлении.

2. КРАТКОЕ ОПИСАНИЕ СИСТЕМЫ ДБО

2.1. Система предназначена для предоставления Банком услуг по удалённому управлению Клиентом своими Счетами и обмена сопутствующей информацией посредством сети Интернет с использованием Электронных документов в соответствии с Документацией. Документация размещена на сайте Банка в сети Интернет по адресу https://teleportbank.ru. Клиент обязан руководствоваться Документацией, если настоящими Правилами не предусмотрено иное.

Доступ к Системе ДБО осуществляется с использованием:

- Веб-приложения;
- Мобильного приложения.

2.2. Для использования Веб-приложения Клиент должен иметь АРМ – компьютер или ноутбук, подключённый к сети Интернет. Браузер желательно обновить до последней (актуальной) версии.

Для использования Мобильного-приложения Клиент должен иметь Мобильное устройство с операционной системой Android или iOS.

2.3. Перед началом работы в Системе Клиенту необходимо:

- заключить Договор об электронных расчетах;
- предоставить номер мобильного телефона для получения SMS-сообщений (возможно использование только одного телефонного номера);

2.3.1. Для использования Веб-приложения Клиенту необходимо:

- получить в Банке USB-токен - носитель ключа ЭП (**ПИН-код к носителям установлен производителем по умолчанию, Клиенту настоятельно рекомендуется сменить ПИН-код в соответствии с инструкцией, размещенной на сайте Банка**);
- получить в Банке логин для входа в Систему;
- Пароль для первого входа в Систему поступит в SMS-сообщении.
- зарегистрироваться в Системе;
- обеспечить создание ЭП, хранение Ключа ЭП на носителе Ключа ЭП;
- сформировать с помощью Системы Заявление на создание сертификата ключа проверки усиленной неквалифицированной электронной подписи (Заявление), проверить и подтвердить корректность данных, указанных в Заявлении. Система автоматически формирует запрос на выпуск Сертификата и передает его в УЦ. Далее Клиенту необходимо распечатать по один экземпляр указанного Заявления.
- УЦ в течение одного рабочего дня создает Сертификат ключа проверки усиленной неквалифицированной электронной подписи Клиента и загружает его в Систему. Сертификат действует до истечения срока либо до его отмены
- Далее Клиенту необходимо войти в Систему с использованием логина и полученного ранее в SMS-сообщении пароля и распечатать два экземпляра Сертификата ключа проверки усиленной неквалифицированной электронной подписи Клиента.
- Клиенту необходимо в течение 5 (пяти) рабочих дней предоставить в Банк Заявление и Сертификат, которые должны быть подтверждены (заверены) подписью Клиента. После подписания Сертификата Банком один экземпляр передается Клиенту, а второй остается в Банке. Заявление остается в Банке.
- После подписания Сертификата Банком и Клиентом, Банк активирует ЭП Клиента в Системе. После активации, при входе в Систему, Клиенту будет предложено установить свой пароль для входа в Систему.
- Если в течение 5 (пяти) рабочих дней Клиент не предоставил в банк Заявление и Сертификат, Сертификат аннулируется.
- Допускается передача в Банк Заявления и Сертификата в электронном виде, заверенных действующей Усиленной неквалифицированной электронной подписью, выданной Банком или Усиленной квалифицированной электронной подписью.

2.3.2. Для использования Мобильного приложения Клиенту необходимо:

- В зависимости от используемой мобильной операционной системы, скачать из магазина приложений приложение «ТелеПорт Банк» и установить на свое Мобильное устройство.
- В случае, если Клиент уже является пользователем Веб-приложения, для доступа к мобильному приложению используются уже имеющиеся логин и пароль к Веб-приложению, в противном случае необходимо пройти самостоятельную регистрацию. При самостоятельной регистрации пароль для первого входа в Систему поступит в SMS-сообщении.
- Создать ключ ЭП и подтвердить «Акт признания ключа электронной подписи» посредством введения Кода подтверждения, отправленного на номер телефона Клиента, зарегистрированного в АБС Банка. Ключ ЭП выпускается и записывается в защищенную область памяти Мобильного устройства Клиента.

2.3.3 При самостоятельной регистрации Клиент в автоматическом режиме дает свое согласие на заключение Договора об электронных расчетах и присоединение к настоящим Правилам.

2.4. Система позволяет Клиенту вводить, редактировать, удалять, подписывать и отправлять в Банк Электронные документы, перечисленные в п. 4.6 настоящих Правил, а также, по согласованию Сторон, просматривать информацию о состоянии своих Счетов в Банке и получать выписки по Счетам в электронном виде.

2.5. При обмене информацией для ее шифрования используется SSL-протокол.

2.6. Стороны признают, что:

- используемая Сторонами система защиты информации, обеспечивающая шифрование Электронных документов, формирование ЭП и контроль целостности ЭД, достаточна для защиты Системы от несанкционированного доступа, а также для подтверждения подлинности ЭД;
- Банк не гарантирует невозможность несанкционированного доступа к Системе третьими лицами, а Клиент принимает на себя соответствующие риски;
- если после заверения ЭД Электронной подписью этот ЭД был изменён, то эта ЭП становится некорректной, то есть её проверка даёт отрицательный результат;
- подделка ЭП, то есть создание корректной ЭП ЭД, направленного Клиентом, невозможна без использования ключа ЭП и пароля;

➢ ЭД, не подписанные ЭП или подписанные некорректной ЭП, не имеют юридической силы, не принимаются и не рассматриваются Банком.

2.7. Подлинниками ЭД являются:

2.7.1. Файл, который содержит текст этого ЭД и электронную подпись при условии положительного результата проверки корректности этой ЭП, произведённой программными средствами Системы с использованием Ключа проверки ЭП, зарегистрированной и принятой Банком в установленном порядке.

2.7.2. Бумажная распечатка этого ЭД, произведённая посредством Системы и заверенная собственноручными подписями уполномоченных лиц Стороны.

2.8. В случае использования Веб - приложения, Ключ ЭП записывается Системой в зашифрованном виде на носитель ключа ЭП. Ключ ЭП должен храниться на носителе Ключа ЭП и используется владельцем ЭП в целях подписи ЭД, подготовленных с помощью Системы, Ключ проверки ЭП после регистрации Клиента в Системе хранится Банком в базе данных Системы.

2.9. В случае использования Мобильного-приложения один ключ из ключевой пары симметричных ключей записывается в защищенную область памяти Мобильного устройства Клиента, а другой хранится Банком в базе данных сервера хранения ключей Программного комплекса «Signal-COM AuthKey Server», являющегося частью Системы.

2.10. Архив входящих и исходящих документов в электронной форме хранится Банком в базе данных Системы.

2.11. Проверка корректности ЭП осуществляется в автоматическом режиме программными средствами Системы.

2.12. Для целей настоящих Правил Банк является владельцем Системы и по вопросам, прямо не урегулированным Правилами, вправе принимать решения по порядку функционирования Системы.

2.13. Все подключения к Системе, а также этапы обработки ЭД в Системе, фиксируются в электронных журналах Системы в автоматическом режиме. Стороны доверяют содержимому электронных журналов Системы.

3. УСЛОВИЯ ОРГАНИЗАЦИИ ОБМЕНА ЭД. ОСНОВАНИЯ ПРИОСТАНОВЛЕНИЯ ОБМЕНА ЭД

3.1. Стороны на условиях Договора об электронных расчетах осуществляют обмен ЭД, предусмотренными п. 4.6 настоящих Правил и подписанными (защищенными) ЭП, с использованием Системы.

3.2. Обмен ЭД осуществляется посредством направления документов, формируемых в шаблоне Системы ДБО, а также документов произвольного формата.

3.3. Проведение расчетных операций по Счетам Клиента осуществляется в соответствии с законодательством Российской Федерации, нормативными актами Банка России и договором банковского счета.

3.4. Стороны признают юридическую силу ЭД, подписанных (защищенных) ЭП (при установлении корректности ЭП), равной юридической силе документов на бумажном носителе, оформленных в соответствии с требованиями законодательства Российской Федерации и с нормативными актами Банка России.

3.5 Для организации обмена ЭД Клиент выполняет следующие действия:

3.5.1. Самостоятельно и за свой счет комплектует АРМ или Мобильное устройство необходимыми программно-техническими средствами в соответствии с п. 2.2 настоящих Правил.

3.5.2. Самостоятельно и за свой счет устанавливает отношения с организацией, обеспечивающей его доступ к Системе по телекоммуникационным каналам связи посредством сети Интернет.

3.5.3. Выполняет действия в соответствии с п. 2.3 настоящих Правил.

3.6. Для организации обмена ЭД Банк выполняет следующие действия:

3.6.1. Вносит сведения о Клиенте в Систему ДБО.

3.6.2. Обеспечивает реализацию функционала Системы по автоматическому формированию Логина для доступа Клиента в Систему при использовании Веб-приложения или регистрации пароля Клиента при самостоятельной регистрации в Мобильном приложении.

3.6.3. Передает Клиенту запечатанный конверт, содержащий Логин для доступа Клиента в Систему ДБО и пароль для первоначального входа в Систему с использованием Веб-приложения на бумажном носителе.

3.6.4. В случае использования Веб-приложения в течение 2-х рабочих дней после создания Клиентом нового Ключа ЭП, поступления в Систему выпущенного УЦ Сертификата Ключа Проверки ЭП и получения Банком подписанного Клиентом Сертификата Ключа Проверки ЭП, активировать этот Сертификат.

3.6.5 Одновременно с активацией нового Сертификата Ключа Проверки ЭП блокирует ранее действовавший Сертификат Ключа проверки ЭП, при наличии такового.

3.6.6. Оказывает консультации по вопросам формирования и эксплуатации АРМ и Системы.

3.7. Стороны начинают осуществлять обмен ЭД с момента совершения действий, предусмотренных п.п. 3.5, 3.6.1 – 3.6.5 настоящих Правил.

3.8. Основаниями для приостановления Банком обмена ЭД являются:

3.8.1. Несоблюдение Клиентом требований к обмену ЭД и обеспечению информационной безопасности при обмене ЭД, предусмотренными Договором об электронных расчетах.

3.8.2. Получение от Клиента уведомления о приостановлении обмена ЭД.

3.8.3. Компрометация Ключа ЭП. Обмен ЭД с Клиентом приостанавливается с момента получения Банком информации о компрометации Ключа ЭП.

3.8.4. Выход из строя или проведение регламентных работ в отношении программно-технических средств Системы или средств, обеспечивающих функционирование телекоммуникационных каналов связи.

3.8.5. Отсутствие возможности списания Банком денежных средств с расчетного счета Клиента в Банке без дополнительного распоряжения Клиента для оплаты услуг Банка по Договору об электронных расчетах согласно п. 6 настоящих Правил.

3.8.6. Ограничение прав Клиента на осуществление операций по расчетным счетам Клиента в Банке.

3.8.7. Осуществление Клиентом деятельности, противоречащей законодательству Российской Федерации, нормативным актам Банка России, настоящим Правилам и договорам, заключенным с Банком.

3.8.8. Получение информации от Банка России о наличии сведений о Клиенте в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента. В этом случае, Банк вправе приостановить использование Клиентом Электронных средств платежа до получения информации от Банка России об удалении сведений о Клиенте из вышеуказанных баз данных

3.8.9. Получение информации от Банка России о наличии сведений о Клиенте в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, содержащей сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях. В этом случае, Банк приостанавливает использование Клиентом Электронных средств платежа до получения информации от Банка России об удалении сведений о Клиенте из вышеуказанных баз данных.

3.8.10. Получение Банком информации о наличии сведений о Клиенте в Реестре контролируемых лиц. В этом случае, Банк приостанавливает использование Клиентом Электронных средств платежа до получения информации об исключении сведений о Клиенте из Реестра контролируемых лиц.

3.8.11. Принятие Банком решения о приостановлении обмена ЭД по собственной инициативе.

3.9. Обмен ЭД возобновляется по решению Банка после устранения причин его приостановления.

3.10. Основаниями для прекращения обмена ЭД (одностороннего отказа Банка от Договора об электронных расчетах) являются:

3.10.1. Закрытие последнего Счета Клиента в Банке, распоряжение денежными средствами на котором осуществляется с использованием Системы ДБО. Договор об электронных расчетах прекращает свое действие с даты закрытия указанного Счета.
3.10.2. Получение от Клиента уведомления об отказе от пользования Системой ДБО.
3.10.3. Отсутствие возможности списания Банком денежных средств с расчетного счета Клиента в Банке без дополнительного распоряжения Клиента для оплаты услуг Банка по Договору об электронных расчетах согласно п. 6 настоящих Правил.
3.10.4. Осуществление Клиентом деятельности, противоречащей законодательству Российской Федерации и нормативным актам Банка России.
3.10.5. Наличие сведений о Клиенте в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.
3.10.6. Наличие сведений о Клиенте в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, содержащей сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях.
3.10.7. Наличие сведений о Клиенте в Реестре контролируемых лиц.
3.10.5. Принятия Банком решения о прекращении обмена ЭД по собственной инициативе.
3.11. О приостановлении или о прекращении обмена ЭД (одностороннего отказа от Договора об электронных расчетах) Сторона-инициатор уведомляет другую Сторону письменно или направлением ЭД. Данный порядок не распространяется на п. 3.8.6, 3.10.1 настоящих Правил. Банк вправе уведомить Клиентов о прекращении обмена ЭД посредством размещения уведомления на сайте Банка в сети Интернет.

4. ОБЩИЕ ПРИНЦИПЫ ОБМЕНА ЭД

4.1. Стороны признают в качестве единой шкалы времени при направлении ЭД с использованием Системы Московское поясное время. Контрольным является время системных часов аппаратных средств Банка.
4.2. Стороны признают, что моментом поступления информации в Систему является текущее время по системным часам сервера Системы в момент полного помещения информации на жесткий магнитный диск сервера Системы.
4.3. Программно-технические средства Банка, обеспечивающие работоспособность Системы ДБО, функционируют в автоматическом режиме. Для входа в систему ДБО с использованием Веб-приложения Клиент должен ввести корректные Логин и пароль, а также использовать действующий ключ ЭП. Для входа в систему ДБО с использованием Мобильного приложения Клиент должен ввести корректные Логин и пароль или использовать биометрический метод идентификацией, предусмотренный Мобильным приложением.
4.4. Обмен ЭД между Банком и Клиентом осуществляется с обязательным применением средств ЭП.
4.5. Статус ЭД, переданных в Банк, отслеживается АРМ или Мобильным приложением автоматически при проведении Клиентом сеансов связи. Получение Клиентом ЭД из Банка осуществляется АРМ или Мобильным приложением автоматически при проведении Клиентом сеансов связи.

Информирование Клиента о совершении обмена ЭД осуществляется направлением Клиенту соответствующего уведомления путем изменения статуса ЭД в Системе ДБО. Получение уведомлений производится путем ежедневного проведения Клиентом сеансов связи.

В случае не проведения или ненадлежащего проведения Клиентом сеансов связи, в том числе окончания сеанса связи до присвоения ЭД, переданному в Банк, статуса «принят», все связанные с этим негативные последствия возлагаются на Клиента.
4.6. Стороны признают, что ЭД, подписанные Клиентом и переданные в Банк равнозначны документам, подписанным собственноручной подписью Клиента на бумажном носителе, скан-копии документов, подписанные ЭП признаются сторонами равнозначными оригиналам.

Стороны используют следующие ЭД в формате Системы ДБО и в произвольном формате в соответствии с п. 3.1 настоящих Правил:
- ЭД Клиента: платежное поручение, поручение на продажу иностранной валюты, поручение на покупку иностранной валюты, поручение на перевод иностранной валюты, запрос на получение выписки, запрос на отзыв ЭД, документ произвольного формата, документы (копии документов), заявления, иные документы по согласованию с Банком;
- ЭД Банка: выписка, приложение к выписке, документ произвольного формата.
- Дополнительное соглашение к договору банковского счета (ДС) - посредством направления Банком в качестве оферты текста ДС как документа свободного формата, подписанного ЭП лица, уполномоченного от Банка на подписание (заключение) ДС, и ответного направления Клиентом в качестве акцепта текста ДС как документа свободного формата, подписанного ЭП лица, уполномоченного от Клиента на подписание (заключение) ДС. Оферта действует в течение дня её направления Клиенту.

4.7. Прием (отказ в приеме) ЭД подтверждается Банком, при этом происходит изменение статуса ЭД в Системе ДБО. Время приема (отказа в приеме) ЭД фиксируется в Системе ДБО.
4.8. Клиент имеет право отозвать составленный им и неисполненный Банком ЭПД, являющийся основанием для совершения операции по Счету Клиента в Банке, путем направления в Банк соответствующего ЭД.
4.9. Обмен ЭД между Банком и Клиентом осуществляется с использованием телекоммуникационных каналов связи; при невозможности их использования документооборот между Сторонами осуществляется в общем порядке на бумажных носителях.
4.10. После поступления в Банк ЭПД Клиента Система формирует SMS-сообщение, содержащее реквизиты ЭПД, в зависимости от его типа и код подтверждения. Для подтверждения корректности полученных Банком данных владелец ЭП вводит в Системе код подтверждения и ЭПД принимается Банком в обработку. При отсутствии кода подтверждения или вводе некорректного кода, ЭПД не считается доставленным и не принимается Банком в обработку.
4.11. Клиент полностью несет все риски, связанные с подключением АРМ к сети Интернет.
4.12. Стороны в рамках Договора об электронных расчетах вправе осуществлять обмен ЭД в соответствии с Федеральным законом от 10.12.2003 года № 173-ФЗ «О валютном регулировании и валютном контроле», Инструкцией Банка России от 16.08.2017 года №181-И «О порядке представления резидентами и нерезидентами уполномоченным банкам подтверждающих документов и информации при осуществлении валютных операций, о единых формах учета и отчетности по валютным операциям, порядке и сроках их представления».

5. ИСПОЛЬЗОВАНИЕ ЭП ПРИ ОБМЕНЕ ЭД

5.1. Стороны признают, что:
- используемые Сторонами в соответствии с Договором об электронных расчетах Система ДБО (логин и пароль), средства ЭП, которые реализуют подписание ЭП и шифрование ЭД, достаточны для обеспечения конфиденциальности, а также подтверждения подлинности и контроля целостности ЭД;
- внесение изменений в ЭД после его подписания ЭП дает отрицательный результат проверки ЭП;
- создание корректной ЭП возможно только с использованием ключа ЭП;
- по содержанию ЭД, подписанного ЭП, и ключа проверки ЭП невозможно определить ключ ЭП;
- каждая Сторона несет ответственность за сохранность своих Ключей ЭП, действия своих владельцев ЭП и своего персонала.

5.2. Для создания ЭП, подписания ЭД и проверки ЭП Стороны используют СКЗИ и признают ее достаточной для подтверждения подлинности ЭД.

5.3. При использовании Веб-приложения плановый срок действия Сертификата Ключа проверки ЭП определяется Банком и составляет 1 год. Плановая смена ключа ЭП производится владельцем ЭП и Клиентом самостоятельно. После даты окончания действия Сертификата Ключа проверки ЭП, ЭП не действует и, соответственно, передача документов через Систему не производится. В случае наступления даты окончания срока действия Сертификата Ключа проверки ЭП в нерабочий день, смена Ключа может быть проведена ранее срока истечения действия Сертификата Ключа проверки ЭП.

При использовании Мобильного приложения смена Ключа ЭП, не вызванная компрометацией ключей ЭП, производится с периодичностью, установленной Банком и составляет 360 дней. На одного Клиента одновременно может быть зарегистрировано не более трех Мобильных устройств с действующей ЭП. В случае генерации ЭП на новом Мобильном устройстве, Банк деактивирует Ключ ЭП на Мобильном устройстве, по которому Ключ ЭП не использовался наиболее продолжительное время.

5.4. Внеплановая смена Ключей ЭП производится в случае их компрометации, а также в любое время по инициативе любой из Сторон в течение 5 (Пяти) рабочих дней с оплатой услуг Банка в соответствии с Тарифами. Внеплановая смена Ключей ЭП может производиться без оснований.

При изменении Клиентом Кода мобильного приложения на Мобильном устройстве, необходимо регистрировать новый Ключ ЭП.

5.5. Запрещается предпринимать попытки:

- копирования информации с носителя ключевой информации;
- ознакомиться с содержанием носителя ключевой информации;
- вывести Ключи ЭП на дисплей (монитор) компьютера или принтер;
- устанавливать носитель ключевой информации в компьютеры, не являющиеся АРМ;
- записать на носитель ключевой информации постороннюю информацию;
- осуществлять попытки извлечь ключ ЭП из защищенной памяти Мобильного устройства.

5.6. В случае принятия решения о компрометации ключа ЭП Клиент обязан любым доступным способом сообщить Банку о факте компрометации и прекратить использование скомпрометированного Ключа.

5.7. Банк имеет право производить замену средств ЭП и других средств, используемых при обмене ЭД, о чем уведомляет Клиента не менее чем за 30 (Тридцать) календарных дней. Клиент, при необходимости, обязан в установленный Банком срок приобрести и установить необходимые средства.

6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ

6.1. Банк предоставляет услуги с использованием Системы в соответствии с настоящими Правилами. По вопросам, не урегулированным настоящими Правилами, Стороны руководствуются договорами.

6.2. Подключение Клиента к Системе ДБО «UBS-HOME» и предоставление услуг осуществляется на основании подписанного Заявления на подключение. Выдача носителя ключевой информации включается в услугу подключения к Системе.

6.3. Подписание Клиентом Заявления на подключение является подтверждением ознакомления и согласия Клиента с настоящими Правилами.

6.4. Обязательными условиями предоставления услуг является:

- наличие у Клиента открытых счетов в Банке.
- указание Клиентом в Сведениях о Клиенте номера телефона сотовой связи, который будет им использоваться для обмена информацией в рамках Системы, в том числе для получения одноразовых паролей.

6.5. Доступ в Систему и возможность инициирования операций предоставляются Клиенту круглосуточно, за исключением перерывов для проведения технических работ.

6.6. Доступ к Веб-версии Системы осуществляется через сайт Банка – www.teleportbank.ru, с которого происходит защищенное соединение по ссылке https://www.dbo.teleportbank:7887.

6.7. Клиент самостоятельно и за свой счет обеспечивает технические, программные и коммуникационные ресурсы, необходимые для доступа к сети Интернет и подключения к Системе, а также в целях информационной безопасности. Правила информационной безопасности установлены в Приложении №1 к настоящим Правилам и Руководстве пользователя.

6.8. Факт совершения Клиентом операций в Системе является подтверждением его согласия с действующими на момент проведения данной операции Тарифами Банка. Оплата услуг осуществляется путем списания Банком денежных средств со Счета без дополнительных распоряжений Клиента. При отсутствии на Счете для расчетов суммы, достаточной для оплаты услуг, или невозможности списания Банком денежных средств со Счета для расчетов, Клиент поручает Банку списать денежные средства в оплату услуг с любых иных Счетов Клиента в Банке без дополнительных распоряжений Клиента.

6.9. Действия Клиента в Системе (Аутентификация Клиента, отправка ЭД, результаты проверки ЭД, а также иные действия) фиксируются в Журнале аудита. Журнал аудита ведется Системой в автоматическом режиме в электронном виде на оборудовании Банка.

6.10. В случае передачи Клиентом в Банк ЭД их последующее предоставление в Банк на бумажном носителе не требуется.

6.11. Хранение ЭД, переданных Клиентом в Банк, осуществляется в течение 5 (Пяти) лет в установленном Банком порядке, за исключением случаев, предусмотренных законодательством и нормативными документами регуляторов.

6.12. Банк информирует Клиента о совершении каждой финансовой операции с использованием Системы путем направления Клиенту извещения об исполнении распоряжения Клиента при осуществлении операций с использованием электронного средства платежа (далее по тексту - Уведомление о совершении операции) в следующем порядке:

- Уведомление о совершении операции направляется Банком Клиенту в электронном виде с использованием Системы ДБО «UBS-HOME» не позднее рабочего дня, следующего за датой операции.
- Банк вправе направлять Клиенту дополнительные уведомления о совершении операции с помощью SMS–сообщений. В этомслучае SMS–сообщение является дополнительным уведомлением по отношению к уведомлению о совершении операции в электронном виде с использованием Системы ДБО, и направляется на номер телефона сотовой связи, указанный Клиентом в его Заявлении на подключение к Системе, в дату совершения каждой операции непосредственно после её совершения.

6.13. Уведомление о совершении операции, направленное Банком Клиенту с помощью SMS–сообщений, безусловно, и, в любом случае, считается полученным Клиентом в дату совершения операции. При этом временем получения такого уведомления о совершении операции Клиентом является время, отраженное оператором сотовой связи в протоколах отражения направленных SMS–сообщений.

7. ПРАВА И ОБЯЗАННОСТИ БАНКА

7.1. Банк вправе:

7.1.1. Консультировать Клиента по вопросам осуществления обмена ЭД.

7.1.2. Отказывать Клиенту в приеме ЭД с указанием причины отказа.

7.1.3. Отказать в регистрации сертификатов в случае невыполнения Клиентом условий, предусмотренных Договором об электронных расчетах.

7.1.4. Приостанавливать обмен ЭД при наличии оснований, предусмотренных п. 3.8 настоящих Правил.

7.1.5. Прекратить обмен ЭД (отказаться от Договора об электронных расчетах) при наличии оснований, предусмотренных п. 3.10 настоящих Правил.

7.1.6. Запрашивать у Клиента, при необходимости, копии ЭД на бумажном носителе.
7.1.7. Запрашивать у Клиента подтверждение или разъяснение совершаемых операций, а также в одностороннем порядке:
- установить для Клиента необходимость подтверждения исполнения ЭПД;
- ограничить общую сумму или количество неподтвержденных ЭПД.

Подтверждение или разъяснение запрашивается Банком у Клиента с использованием Системы либо иным образом. В этом случае ЭПД исполняется Банком только после получения требуемого подтверждения или разъяснения. Срок предоставления подтверждений и разъяснений устанавливается Банком.

7.1.8. В одностороннем порядке досрочно прекратить действие Ключа ЭП Клиента с последующим уведомлением об этом Клиента и потребовать от Клиента смены ключей ЭП. При этом обслуживание Клиента через Систему приостанавливается. Возобновление передачи ЭД с использованием Системы после её приостановления по инициативе Клиента или в связи с нарушением Клиентом условий Настоящих Правил возможно только после устранения причин, которые были основанием такой приостановки работы с использованием Системы и получения Банком от Клиента заявления в письменной форме о возобновлении передачи ЭД с использованием Системы, при наличии у Банка возможности.

7.1.9. В одностороннем порядке вносить изменения в Правила, Документацию и Тарифы. Информация об этом размещается на информационных стендах Банка и/или на сайте Банка в сети Интернет не позднее чем за 10 (Десять) календарных дней до вступления изменений в силу.

7.1.10. Привлекать к работе по устранению недостатков Системы (если таковые будут установлены) её разработчика. Разработчик может привлекаться также при возникновении спорных ситуаций, связанных с использованием Системы, и к работе в Согласительной комиссии.

7.2. Банк обязан:

7.2.1. Исполнять поступившие от Клиента заверенные корректной ЭП ЭПД, оформленные в соответствии с законодательством и иными нормативными актами Российской Федерации, условиями заключенных между Банком и Клиентом договора банковского счета и Договора об электронных расчетах.

7.2.2. При получении от Клиента ЭД проверить корректность ЭП Электронного документа. При неудовлетворительном результате проверки ЭП отказать в проведении операции и/или приёме документа, при этом в Системе формируется сообщение о принятом решении.

7.2.3. После успешной проверки корректности ЭП провести первоначальный контроль правильности заполнения ЭД, проверить законность операции Клиента, соответствие договору банковского счета и Договору об электронных расчетах. Результатом этой работы является решение Банка о приёме или отказе в приеме ЭД Клиента.

7.2.4. Вести архивы входящих и исходящих ЭД в соответствии со следующими требованиями:
- входящие ЭД, прошедшие проверку корректности ЭП, хранятся с указанием даты и времени получения;
- все исходящие ЭД хранятся с указанием даты и времени их отправки;
- сроки хранения ЭД должны соответствовать срокам хранения, установленным для расчетных документов на бумажных носителях;
- порядок хранения ЭД должен обеспечивать оперативный доступ к ЭД и возможность распечатки их копий на бумажном носителе.

7.2.5. Обеспечивать своевременную смену ключей ЭП.

7.2.6. Незамедлительно информировать Клиента обо всех случаях возникновения технических неисправностей или других обстоятельствах, препятствующих обмену ЭД.

7.2.7. Осуществлять контроль ЭД, полученных от Клиента, и сообщать Клиенту об обнаруженных ошибках и причинах невозможности исполнения ЭД.

7.2.8. При получении от Клиента документа, извещающего о неуспешной выверке согласно п. 8.1.5. настоящих Правил, активизировать процедуры проверки, в том числе производить контроль входящих и исходящих ЭД, устанавливать причину расхождения и, при обнаружении ошибок со своей стороны, передавать Клиенту исправленные документы.

7.2.9. Изготавливать, при необходимости, бумажные копии ЭД.

7.2.10. Предоставлять Клиенту по его запросу бумажные копии ЭД.

7.2.11. Консультировать Клиента по вопросам осуществления обмена ЭД.

7.2.12. Исключить доступ неуполномоченных лиц к Системе, средствам ЭП, Ключам ЭП и Ключам проверки ЭП.

7.2.13. В случае выявления с помощью системы Антифрод или иным способом подозрительной операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, Банк приостанавливает прием к исполнению распоряжения Клиента на два дня и незамедлительно направляет по Системе ДБО «UBS-HOME» Клиенту уведомление о необходимости подтверждения данной операции также по Системе ДБО «UBS-HOME» не позднее одного дня, следующего за днем приостановления приема к исполнению указанного распоряжения. В случае получения подтверждения от Клиента Банк принимает к исполнению вышеуказанное распоряжение. При неполучении от Клиента подтверждения распоряжения, указанное распоряжение считается не принятым к исполнению.

7.2.14. В случае, если, несмотря на направление Клиентом подтверждения распоряжения Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, Банк приостанавливает прием к исполнению подтвержденного распоряжения Клиента на два дня со дня направления Клиентом подтверждения распоряжения. Банк, незамедлительно направляет Клиенту по Системе ДБО «UBS-HOME» уведомление о приостановлении приема к исполнению подтвержденного распоряжения Клиента с указанием причины такого приостановления и срока такого приостановления. По истечении двух дней со дня направления Клиентом подтверждения распоряжения, Банк принимает к исполнению подтвержденное распоряжение Клиента при отсутствии иных установленных законодательством Российской Федерации оснований.

8. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

8.1. Клиент обязуется:

8.1.1. Ознакомиться с настоящими Правилами и Руководством пользователя до заключения Договора об электронных расчетах.

8.1.2. Использовать Систему ДБО «UBS-HOME» в соответствии с Правилами и Руководством пользователя.

8.1.3. Оплачивать услуги Банка в соответствии с Тарифами.

8.1.4. Заполнять ЭД в Системе ДБО «UBS-HOME» в соответствии с требованиями Банка и Руководством пользователя.

8.1.5. Контролировать правильность реквизитов, указываемых в ЭД, контролировать изменение статуса ЭД о принятии к исполнению, исполнении (обработке) или отказе в принятии к исполнению ЭД, осуществлять контроль полученных от Банка ЭД и при обнаружении ошибок незамедлительно информировать о них Банк письменно или направлением ЭД.

8.1.6. Предоставлять по запросу Банка документы и сведения, необходимые в соответствии с требованиями законодательства Российской Федерации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

8.1.7. Не разглашать учетные данные (Логин и Пароль), а также обеспечить невозможность использования третьими лицами телефона сотовой связи, зарегистрированного в Системе ДБО «UBS-HOME» и USB-токена, содержащего Ключ ЭП.

8.1.8. Незамедлительно информировать Банк в случае утраты USB-токена, компрометации или при подозрении на компрометацию Учетных данных Клиента, зарегистрированных в Системе ДБО «UBS-HOME» (Логин, Пароль, SIM карта с номером телефона сотовой связи и т.д.) при этом Клиент должен назвать Кодовое слово.
8.1.9. Информировать Банк об изменении своих персональных данных (в т.ч. данных документа, удостоверяющего личность) Клиента в течение 10 (Десяти) календарных дней с момента изменения данных.
8.1.10. Выполнить настройку оборудования и программного обеспечения в соответствии с Руководством пользователя и требованиями по информационной безопасности, приведенными в Приложении № 1 к настоящим Правилами, в срок не позднее следующего рабочего дня после заключения Договора об электронных расчетах.
8.1.11. Своевременно исполнять требования Банка по обновлению собственного технического и программного обеспечения.
8.1.12. Соблюдать требования информационной безопасности.
8.1.13. Перед совершением операций в Системе ДБО «UBS-HOME» самостоятельно ознакомиться с действующими на текущую дату Тарифами и Правилами.
8.1.14. В случае обнаружения Клиентом Компрометации, Клиент обязан выполнить действия, предусмотренные разделом 9 настоящих Правил.
8.1.15. Незамедлительно уведомлять Банк о компрометации ключа ЭП, а также сообщать Банку о всех ошибках при совершении переводов средств и о несанкционированных переводах средств в письменном виде после их обнаружения немедленно (в день обнаружения). При обращении в Банк с сообщением о компрометации по телефону, Клиент использует Кодовое слово.
Под ошибкой понимается, но не ограничивается этим:
- неверный перевод средств со счёта Клиента;
- ошибка в компьютерных или бумажных расчётах, выполняемых Банком в связи с переводом средств;
- неправильное указание суммы перевода или получателя платежа в выписке по счёту Клиента.

Под несанкционированным переводом средств понимается, но не ограничивается этим, перевод средств со счёта Клиента, произведённый лицами, не имеющими права распоряжаться Счетами Клиента. Это включает в себя любой перевод средств, если он:
- совершен любым лицом, которому носитель ключевой информации не принадлежит на законном основании;
- совершен без поручения Клиента и при отсутствии законных оснований для этого

8.1.16. По требованию Банка в течение 3 (Трех) дней передавать Банку письменное изложение обстоятельств, связанных с отправкой документов, ЭП которых не была признана Банком корректной, и со всеми случаями ошибок и несанкционированных переводов средств или таких попыток, а также все относящиеся к таким случаям документы и файлы с информацией.
8.1.17. Немедленно сообщать Банку в письменном виде обо всех случаях, свидетельствующих о попытках неуполномоченных лиц получить доступ к Счетам Клиента с использованием Системы, а также о любой потере контроля над носителем Ключа ЭП и/или Сертификатом. При выявлении указанных выше фактов и другой компрометации или подозрении на компрометацию своего Ключа ЭП Клиент обязан немедленно поменять Ключи ЭП. Новые Ключи проверки ЭП регистрируются и передаются в Банк в соответствии с п.п. 3.5.5 –3.5.8 настоящих Правил.
8.2. Клиент имеет право:
8.2.1. Получить в Банке экземпляр платежного документа на бумажном носителе, по операции совершенной с использованием Системы ДБО «UBS-HOME» в соответствии с Тарифами Банка.
8.2.2. Обратиться в Банк с письменной просьбой об отмене или приостановлении обслуживания с использованием Системы ДБО «UBS-HOME».
8.2.3. Отказаться от дальнейшего использования Системы ДБО «UBS-HOME» при несогласии с дополнениями и/или изменениями Правил и/или Тарифов, предоставив Заявление на изменение по форме Банка, не позднее чем за один рабочий день до даты введения дополнений и/или изменений. Не воспользовавшись данным правом, Клиент подтверждает свое согласие с новыми Правилами и/или Тарифами Банка.
8.2.4. Отозвать ЭД до момента его исполнения с использованием Системы ДБО «UBS-HOME» в соответствие с Руководством пользователя.
8.2.5. Предоставить в Подразделение Банка распоряжение на бумажном носителе в случае отказа Банка в приеме от Клиента ЭД на проведение операции по Счету с использованием Системы ДБО «UBS-HOME».
8.2.6. Получать консультации по вопросам использованием Системы ДБО «UBS-HOME», техническим и иным вопросам в рабочее время Банка по телефонам Банка, указанным на официальном сайте Банка.
8.2.7. Подтверждение личности Клиента при его обращении в Банк по телефону осуществляется по Кодовому слову, указанному в Сведениях о Клиенте. Сотрудник Банка вправе запросить дополнительные сведения для подтверждения личности Клиента.
8.2.8. Самостоятельно осуществить блокировку своих Учетных данных в Системе ДБО «UBS-HOME» путем троекратного ввода неверного пароля.
8.2.9. На основании письменного Заявления на изменение устанавливать ограничения на осуществление операций либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени. Ограничения по операциям могут быть установлены как на все операции Клиентов, так и в разрезе видов операций.
8.2.10. Клиенты из числа ЛСИ и МГН дополнительно к пункту 8.2.9 имеют право (возможность) на основании письменного заявления:
• устанавливать лимиты по сумме операций и/или запрет на совершение переводов денежных средств, по Счету с использованием Системы ДБО «UBS-HOME»;
• вводить запрет дистанционного доступа и/или отображения информации по всем либо отдельным счетам Клиента с использованием Системы ДБО «UBS-HOME»;
• формировать закрытый перечень лиц, в пользу которых возможно осуществление перевода денежных по Счету с использованием Системы ДБО «UBS-HOME».

9. ПОРЯДОК ДЕЙСТВИЙ КЛИЕНТА В СЛУЧАЕ КОМПРОМЕТАЦИИ

9.1. В случае обнаружения факта компрометации, Клиент обязан незамедлительно после обнаружения факта выполнить следующие действия:
9.1.1. В случае использования Веб-приложения - обесточить АРМ (принудительно отключить электропитание в обход штатной процедуры завершения работы, при наличии технической возможности извлечь аккумуляторную батарею), отключить компьютер от информационных сетей (если было подключение, например по USB, Lan и др.). При отсутствии возможности обесточивания компьютера, осуществить отключение по штатной процедуре и зафиксировать указанный факт;
В случае использования Мобильного-приложения – перевести Мобильное устройство в «режим полета» и выключить устройство. В случае невозможности осуществить эти действия, зафиксировать указанный факт.
9.1.2. Отозвать перевод денежных средств следующими способами:
- при наличии возможности - отозвать перевод с использованием иного компьютера, после чего заблокировать доступ к Системе ДБО «UBS-HOME» путем троекратного ввода неверного пароля;
- при отсутствии возможности - обратиться в Банк в рабочее время по телефонам,

указанным на официальном сайте Банка, с Заявлением на изменение, произнеся Кодовое слово, указанное в Сведениях о Клиенте с

обязательным предоставлением в Банк письменного заявление об отзыве перевода денежных средств не позднее следующего рабочего дня;

9.1.3. Обеспечить сохранность (целостность) АРМ или Мобильного устройства, как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры АРМ или Мобильного устройства, поместить его в непрозрачный пакет.

9.1.4. Обеспечить сохранность в памяти телефона сотовой связи полученные от Системы SMS-сообщения.

9.1.5. Заблокировать свои Учетные данные в Системе ДБО «UBS-HOME», обратившись в Банк в рабочее время по телефонам, указанным на официальном сайте Банка, и произнеся Кодовое слово;

9.1.6. Направить в Банк письменное Заявление на изменение о компрометации по форме Банка в срок не позднее следующего рабочего дня, за днем выявления факта компрометации.

9.1.7. При обращении в правоохранительные органы с заявлением о возбуждении уголовного дела по факту несанкционированного доступа и использования Системы ДБО «UBS-HOME» представить в Банк документы, свидетельствующие об обращении в правоохранительные органы.

9.1.8. Принимать участие в работе согласительной комиссии в соответствии с разделом 10 настоящих Правил.

9.2. Возобновление работы Клиента в Системе ДБО «UBS-HOME» осуществляется после устранения причин компрометации и после подачи в Банк Заявления на изменение по форме Банка.

9.3 Клиент, по запросу Банка, обязуется запросить у обслуживающего Интернет-провайдера(ов), через которых осуществлялось подключение к сети Интернет при работе Клиента в Системе ДБО «UBS-HOME» и оператора сотовой связи, в сети которого зарегистрирован его телефон (для получения SMS-сообщений), необходимые данные и предоставить их Банку.

9.4 При возникновении у Банка подозрений на Компрометацию Банк вправе совершать любые необходимые действия, направленные на пресечение противоправного использования Системы ДБО «UBS-HOME», в том числе отказать в приёме или исполнении ЭД.

10. ОТВЕТСТВЕННОСТЬ СТОРОН

10.1. За неисполнение или ненадлежащее исполнение своих обязательств, принятых на себя в рамках настоящих Правил, Стороны несут ответственность в соответствии с действующим законодательством РФ.

10.2. Клиент несёт ответственность за содержание любого ЭД, подписанного Владельцем ЭП, вне зависимости от того, кто подписал документ - лицо уполномоченное, распоряжаться Счетом, или нет. Банк несет ответственность за содержание любого ЭД, подписанного его ЭП.

10.3. При несвоевременном сообщении в Банк об ошибках, о несанкционированных переводах средств, о случаях утраты или компрометации ключей ЭП, Сертификата ключа, раскрытия пароля, а также о других подобных обстоятельствах ответственность за связанные с этим убытки несёт Клиент. Все действия Банка, совершенные до получения от Клиента письменного уведомления о вышеуказанных случаях, считаются совершёнными Банком на законном основании и не влекут ответственности Банка.

10.4. Клиент несет полную ответственность за все убытки, которые могут возникнуть у него или у Банка в результате неправильного перевода Банком средств Клиента из-за нарушения Клиентом условий Договора об электронных расчетах или Правил (вне зависимости от причин нарушения условий Договора об электронных расчетах или Правил). В этом случае Банк освобождается от возмещения убытков Клиенту.

10.5. Банк не несёт ответственности в случае причинения Клиенту убытков исполнением ЭД, подписанных корректной ЭП, в результате передачи этих документов с использованием Системы неуполномоченными на то лицами, включая использование пароля, Сертификата Ключа проверки ЭП и Ключей ЭП Клиента (вне зависимости от причин получения неуполномоченными лицами доступа к Ключам ЭП, информации о паролях, в том числе при их утере, добровольной передаче Клиентом неуполномоченным лицам, краже, грабеже, разбое и других обстоятельствах их передачи неуполномоченным лицам). В этом случае убытки Клиента образуются по вине Клиента и возмещению со стороны Банка не подлежат.

10.6. В случае несвоевременного приостановления Банком обмена ЭД с использованием Системы после получения письменного сообщения Клиента о хищении носителей Ключа ЭП, попытках совершения несанкционированных переводов средств Клиента и иных подобных сообщений Банк возмещает Клиенту причинённые этим убытки.

10.7. Убытки, образовавшиеся в связи с неисполнением или ненадлежащим исполнением Банком ЭД Клиента по причине наличия вирусов в компьютерном обеспечении одной из Сторон, ложатся на эту Сторону и другой Стороной не возмещаются. Убытки также не возмещаются Сторонами при одновременном наличии вирусов в компьютерном обеспечении двух Сторон.

10.8. Клиент самостоятельно несет ответственность за возможные убытки, возникшие в связи с передачей ЭД и получением информации с использованием Системы.

10.9. Стороны не несут ответственности за работу сети Интернет, ее программ и протоколов, а также иных телекоммуникационных каналов и систем связи, включая проводную и мобильную телефонную связь. Убытки, возникшие у одной из Сторон при их полной или частичной неработоспособности, другой Стороной не возмещаются.

Никакие претензии по работоспособности сети Интернет, ее программ и протоколов, иных телекоммуникационных каналов и систем Сторонами не принимаются и не рассматриваются.

10.10. Клиент согласен с тем, что Банк не несёт никакой ответственности за ошибки или сбои в работе Системы, если они произошли не по вине Банка (в том числе по вине разработчика Системы), даже если они повлекли убытки Клиента. Указанные убытки Банком не возмещаются.

10.11. Стороны освобождаются от ответственности в том случае, если используемые в Системе алгоритмы не соответствуют ГОСТам, указанным в технической документации к Системе и Правилах, а также при нарушении разработчиком установленных правил изготовления (разработки) Системы. Возникшие, в связи с этим убытки Сторонами не возмещаются.

10.12. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств, если это явилось следствием действия обстоятельств непреодолимой силы (форс-мажорные обстоятельства). В этом случае срок исполнения обязательств отодвигается соразмерно времени действия таких обстоятельств.

Понятие форс-мажорных обстоятельств охватывает внешние или чрезвычайные события, отсутствовавшие во время заключения Договора об электронных расчетах и возникшие помимо воли и желания Сторон; наступление этих событий Стороны не могли предотвратить разумными мерами и средствами, которые было бы оправдано ожидать от Стороны в конкретной ситуации, пострадавшей от воздействия форс-мажорных обстоятельств. К форс-мажорным обстоятельствам Стороны также относят следующее: отключение и/или перебои электроэнергии; наличие вирусов в сети Интернет; действия Центрального Банка РФ и иных органов власти, влияющие на осуществление платежей и/или использование Системы; принятие законодательных актов, изменяющих или отменяющих порядок осуществления платежей с использованием Электронных документов; вооруженные конфликты; стихийные бедствия; пожары; взрывы; отказы компьютерных систем; отказы или ненадлежащее функционирование телекоммуникационных линий связи, если указанные обстоятельства непосредственно повлияли на исполнение Сторонами своих обязательств.

Сторона, подвергшаяся воздействию форс-мажорных обстоятельств, должна незамедлительно, не позднее 5 (Пяти) рабочих дней, известить в письменной форме другую Сторону о типе, характере, возможной продолжительности и предположительных последствиях действия данных обстоятельств, а также принять все возможные меры с целью максимально ограничить отрицательные последствия, вызванные указанными обстоятельствами. Сторона, для которой создались форс-мажорные обстоятельства, должна также не позднее чем через 5 (Пять) рабочих дней известить в письменной форме другую Сторону о прекращении этих обстоятельств. В этом случае ни одна из Сторон не будет иметь права на возмещение другой Стороной любых возможных убытков.

Не извещение или несвоевременное извещение Стороной, для которой создалась невозможность исполнения обязательств по Договору об электронных расчетах, о наступлении форс-мажорных обстоятельств другой Стороны, влечет за собой утрату права ссылаться на эти обстоятельства.

10.13. За неисполнение или ненадлежащее исполнение своих обязательств по Договору об электронных расчетах Банк несёт ответственность перед Клиентом только при наличии своей вины.

10.14. В связи с тем, что Клиент в любом случае имеет возможность представлять в Банк расчётные документы на бумажном носителе, Банк не несёт ответственность перед Клиентом за несвоевременное представление Клиентом документов в Банк при невозможности передачи ЭД с использованием Системы, в том числе при её неработоспособности или приостановлении обслуживания.

Банк имеет право приостановить работу с использованием Системы ДБО до даты предоставления всех необходимых документов, требуемых Банком. Стороны признают, что все ЭД, направленные Клиентом в Банк с использованием Системы ДБО, принятые, успешно расшифрованные и исполненные Банком, считаются до момента внесения соответствующих изменений в Договор об электронных расчетах надлежащим образом оформленными и исполненными в соответствии с Договором об электронных расчетах.

10.15. Банк не несет ответственности за ЭД Клиента, проведенные по старым реквизитам, в случае несвоевременного непредставления Клиентом информации о произошедших изменениях и направления в Банк документально подтвержденных новых реквизитов.

10.16. Клиент несет ответственность за сохранность полученных в Банке носителей ключевой информации и средств доверенного отображения подписываемых данных. В случае выхода из строя носителя ключевой информации или средства доверенного отображения подписываемых данных, находящегося у Клиента менее 6 месяцев и не имеющего физических повреждений, Банк производит его замену бесплатно. Во всех остальных случаях Клиент оплачивает замену в соответствии с Тарифами.

11. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

11.1. Для разрешения возникших разногласий по операциям, совершенным с использованием Системы ДБО «UBS-HOME», Клиент подает в Банк Заявление на изменение с указанием сути претензии и детальным описанием оспариваемой операции, а также, при необходимости, документы и материалы, подтверждающие обоснованность претензии Клиента.

11.2. На основании полученного Банком Заявления на изменение и в целях совместного досудебного разрешения спорных (конфликтных) ситуаций, Банком в течение 5 (Пяти) рабочих дней с даты соответствующего обращения Клиента создается согласительная комиссия. О назначенной дате, времени и месте начала работы согласительной комиссии, Клиент уведомляется письменно не позднее 1 (Одного) рабочего дня до начала работы комиссии.

11.3. В состав согласительной комиссии включаются Клиент и (или) его представители и представители Банка. Количественный состав согласительной комиссии должен составлять не менее 2 (Двух) человек. По требованию любой из Сторон в состав согласительной комиссии могут быть включены независимые эксперты, а также представители разработчика (правообладателя) Системы ДБО «UBS-HOME». При этом независимый эксперт должен иметь высшее профессиональное образование или профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 (Пяти) лет.

11.4. Стороны обязуются способствовать работе согласительной комиссии и не допускать отказа от предоставления необходимых документов и подписания акта по итогам ее работы.

11.5. Стороны обязуются предоставить данные, подтверждающие соблюдение требований Приложения № 1 к настоящим Правилам.

11.6. В случае, если Клиент отказался и (или) не направил своих представителей для участия в работе согласительной комиссии, сформированной на основании Заявления на изменения от Клиента, рассмотрение спорной ситуации осуществляется без Клиента и (или) его представителей. В этом случае Акт согласительной комиссии должен содержать запись об отсутствии Клиента и (или) его представителей.

11.7. В результате рассмотрения Заявления на изменения от Клиента согласительная комиссия определяет корректность приема и исполнения спорного ЭД.

11.8. Согласительная комиссия проводит рассмотрение Заявления на изменения от Клиента в срок не более 5 (Пяти) рабочих дней с момента её формирования. Рассмотрение Заявления на изменения от Клиента включает следующие этапы:

11.8.1. Из Журнала аудита программно-аппаратного комплекса Системы ДБО «UBS-HOME» извлекаются:

- SMS-код, сгенерированный Системой ДБО «UBS-HOME» для данного ЭД;
- текст направленного Клиенту SMS-сообщения, содержащего детали операции (сумма, наименование получателя или назначение платежа);
- время отправки SMS-сообщения;
- номер телефона (для получения SMS-сообщений), на который было направлено SMS-сообщение;
- Одноразовый пароль, который был введен при подтверждении данного ЭД;
- Тип проводимой Клиентом операции (действия);
- Дата и время операции;
- Результат совершения операции (с расшифровкой ошибки, если она есть);
- IP-адрес Клиента, с которого был запрос на совершение операции;
- Идентификатор операции (документа) в Системе;
- и другие данные, согласно техническим возможностям.

11.8.2. Авторство ЭД подтверждается в случае соблюдения единовременно всех нижеперечисленных условий:

11.8.2.1 **Для операций с использованием Веб-приложения:**

- Электронная подпись корректна;
- Действующий Сертификат Ключа проверки ЭП;
- SMS-сообщение направлено на номер телефона (для получения SMS-сообщений), который зарегистрирован в Системе ДБО «UBS-HOME» для данного Клиента ;
- детали операции (сумма, наименование получателя или назначение платежа), указанные в SMS-сообщении, совпадают с таковыми в ЭД;
- введенный при подтверждении ЭД Одноразовый пароль совпадает с Одноразовым паролем, сгенерированным Системой ДБО «UBS-HOME» для данного ЭД и направленным на номер телефона (для получения SMS-сообщений), номер которого зарегистрирован в Системе ДБО «UBS-HOME» для данного Клиента;
- отправка SMS-кода и ввод SMS-кода были выполнены в пределах срока действия SMS -кода;
- отправка SMS-кода хронологически предшествовала вводу SMS-кода.

11.8.2.2 **Для операций с использованием Мобильного приложения:**

- Действующий Сертификат Ключа и Ключ ЭП, используемый в Мобильном приложении;
- SMS-сообщение с кодом подтверждения регистрации и выпуска сертификата Ключа ЭП направлялись на номер телефона (для получения SMS-сообщений), который зарегистрирован в Системе ДБО «UBS-HOME» для данного Клиента;
- Устройство, с которого отправлен ЭД зарегистрировано в системе ДБО.

11.9. На основании проведенных согласительной комиссией мероприятий, составляется Акт, содержащий:

- фактические обстоятельства, послужившие основанием возникновения разногласий;
- все реквизиты оспариваемого ЭД;
- порядок работы членов согласительной комиссии;
- вывод о подлинности ЭД и его обоснование.

Акт составляется непосредственно после завершения оценки всех обстоятельств, подлежащих установлению согласительной комиссией, в двух экземплярах по экземпляру для каждой Стороны и подписывается всеми членами согласительной комиссии. Члены согласительной комиссии, не согласные с выводом комиссии, вправе отразить свои возражения в Акте.

11.10. В случае отказа Клиента и/или его представителя, входящего в состав согласительной комиссии, от подписания Акта, Акт оформляется и подписывается остальными членами согласительной комиссии. Акт согласительной комиссии, оформленный в указанном порядке, считается оформленным надлежащим образом и достоверно подтверждающим выводы согласительной комиссии. Один экземпляр Акта вручается Клиенту (его представителю) под роспись или направляется Клиенту заказным письмом

11.11. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

11.11.1. Банк не предъявляет подтвержденный корректной ЭП ЭД, на основании которого Банк выполнил операции по Счёту Клиента.

11.11.2. Банк не предъявляет информацию по Одноразовому паролю, которым был подтвержден спорный ЭД.

11.11.3. Клиент предоставляет Заявления на изменения доступа к Системе ДБО «UBS-HOME», подписанное уполномоченным должностным лицом Банка, при этом указанное в заявлении время блокирования Клиента в Системе ДБО «UBS-HOME», раньше времени проведения Банком спорного ЭД.

11.12. В случае, когда подлинность ЭД подтвержденного корректной ЭП подтверждена согласительной комиссией, Банк не несёт ответственности перед Клиентом по выполненным операциям по Счёту Клиента.

11.13. Если Клиент настаивает на том, что спорный ЭД он не создавал и (или) не подтверждал с использованием ЭП, Клиент вправе направить в Банк претензию с приложением документов, подтверждающих позицию Клиента, которая рассматривается Банком в течение 30 (Тридцати) календарных дней. По итогам рассмотрения претензии Клиента Банк направляет Клиенту мотивированный ответ (заключение). В случае несогласия Клиента с мотивированным ответом Банка Клиент вправе обратиться в суд в установленном законом порядке.

11.14. Стороны признают, что ЭД с корректной ЭП Клиента, полученные Банком по Системе, являются доказательством для разрешения спорных вопросов по оспариваемым Клиентом ЭД.

11.15. В случае признания претензии Клиента обоснованной, Банк в течение 1 (Одного) рабочего дня с даты формирования заключения принимает решение о мерах и сроках удовлетворения претензии Клиента, о чем направляет Клиенту соответствующее уведомление в письменном виде. Уведомление может быть вручено Клиенту лично под роспись и (или) направлено по почте заказным письмом.

11.16. В случае не урегулирования спора Сторонами он передается на рассмотрение в суд общей юрисдикции месту нахождения головного офиса Банка.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1. Договор об электронных расчетах является неотъемлемой частью Договора банковского счета, заключенного между Банком и Клиентом.

12.2. Допускается заключение и расторжение Договора банковского счета (в части открытия второго и последующих счетов), Договора об электронных расчетах посредством направления в Банк документов в электронном виде, подписанных согласованной Сторонами ЭП в порядке, предусмотренном соглашением Сторон.

12.3. Первоначальное подключение к Системе ДБО Счетов Клиента осуществляется Банком согласно Заявлению на подключение к Системе ДБО. Открываемые в процессе обслуживания Клиента в Банке Счета добавляются в Систему ДБО Банком автоматически, за исключением случаев, определенных между Банком и Клиентом.

12.4. Сформированные до вступления в силу настоящей редакции Правил Ключи ЭП продолжают действовать до их замены в порядке, установленном настоящими Правилами.

12.5. Любая из Сторон вправе расторгнуть Договор об электронных расчетах в одностороннем (внесудебном) порядке, предупредив об этом другую Сторону письменно (в том числе посредством размещения Банком уведомления на сайте Банка в сети Интернет) не менее чем за 10 (Десять) календарных дней до предполагаемой даты расторжения Договора об электронных расчетах. До даты расторжения Договора об электронных расчетах Клиент обязан оплатить задолженность перед Банком, возникшую вследствие исполнения Договора об электронных расчетах.

12.6. Заявления, направляемые Клиентом в Банк в рамках Договора об электронных расчетах, оформляются по установленной Банком форме.

12.7. Настоящие Правила вступают в силу с даты их утверждения Банком.

Приложение №1 к Правилам организации и осуществления обмена электронными документами в системе «UBS-HOME»

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.

2. 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.

3. 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.