Утверждено:
Правлением ПАО «ЧЕЛЯБИНВЕСТБАНК»
Протокол № 255 от «11» декабря 2018г.

Председатель Правления

_____С.М. Бурцев

ПРАВИЛА № 26-037-П

ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПАО «ЧЕЛЯБИНВЕСТБАНК»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Термины и определения (в алфавитном порядке)

Администратор безопасности – должностное лицо ПАО «ЧЕЛЯБИНВЕСТБАНК» (далее - Банк), отвечающее за эксплуатацию средств крипто-защиты информации (СКЗИ), средств электронной подписи (СЭП) и системы управления криптографическими ключами. Администратор безопасности Банка также отвечает за изготовление сертификатов ключей проверки электронной подписи (ЭП) Банка, генерацию ключей ЭП Банка, ведение реестра сертификатов ключей проверки ЭП, зарегистрированных Банком, выполнение операций по приостановлению действия и аннулированию сертификатов ключей проверки ЭП.

Владелец сертификата ключа проверки электронной подписи – уполномоченный представитель Клиента Банка, на имя которого выдан сертификат ключа проверки ЭП и который владеет соответствующим ключом ЭП, позволяющим с помощью СЭП создавать свою электронную подпись в электронных документах (подписывать электронные документы электронной подписью).

Декомпиляция – процедура получения исходного текста для программных загрузочных модулей.

Доставка ЭД – процесс перемещения электронного документа (ЭД) от отправителя к получателю.

Заявление на выпуск сертификата ключа проверки серверной ЭП - документ, содержащий самозаверенную заявку на выпуск сертификата ключа серверной подписи в рамках Системы «Инвест-Бизнес Онлайн».

Заявление на выпуск сертификата ключа проверки ЭП - документ, содержащий самозаверенную заявку на выпуск сертификата ключа.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи**.**

Ключевая информация – совокупность средств и способов аутентификации (электронной идентификации) Клиента и/или авторизации операции (проверки полномочий клиента на ее совершение). К ключевой информации относятся любая информация о банковской карте, ПИН-Код, срок действия и номер Карты, секретный код CVC2/CVV2, указываемый на оборотной стороне Карты либо в секретном конверте, криптографические ключи и электронно-ключевые носители с криптографическими ключами, одноразовые коды и средства их получения, а также различные пароли, используемые в рамках электронного средства платежа (далее - ЭСП) и/или в системах ЭДО.

Ключевой носитель – информационный носитель, содержащий криптографические ключи.

Ключи серверной подписи - ключ электронной подписи, сгенерированный Сервером Подписи, используется только для подписи документов из мобильного приложения системы «Инвест-Бизнес Онлайн», хранятся в Банке, в зашифрованном виде.

Ключи проверки серверной подписи – ключ проверки электронной подписи, используемый Сервером Подписи, для проверки подписи документов из мобильного приложения системы «Инвест-Бизнес Онлайн».

Компрометация ключевой информации – констатация Банком либо лицом, владеющим Ключевой информацией, обстоятельств, при которых возможно несанкционированное использование данной информации неуполномоченными лицами.

Корпоративная банковская карта – расчетная банковская карта какой-либо платежной системы, эмитированная (выпущенная) Банком, являющаяся одним из видов ЭСП, позволяющая Клиенту распоряжаться денежными средствами, находящимися на его счете, в порядке и на условиях, установленных договором между Банком и Клиентом.

Криптографические ключи – общее название ключа электронной подписи и ключа проверки электронной подписи и/или шифрования.

Неквалифицированная электронная подпись – электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; создается с использованием средств электронной подписи.

Отправитель ЭД – физическое или юридическое лицо, которое само непосредственно направляет или от имени которого направляется электронный документ.

Подсистема СЭД **(система «Интернет-Банк», в том числе с системой «Инвест-Бизнес Онлайн», «Клиент-Банк» или InvestPay)** – часть СЭД, являющаяся одним из видов ЭСП, представляющая собой совокупность программного, информационного и технического обеспечения Банка и Клиентов, позволяющая Клиентам составлять, удостоверять и передавать заявления, распоряжения, включая ЭД, в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации и иных технических устройств, а также осуществлять переписку между Клиентом и Банком.

Получатель ЭД – физическое или юридическое лицо, которому электронный документ отправлен самим отправителем или от имени отправителя.

Простая электронная подпись - электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Сервер Подписи – организационно-техническая система для юридических лиц, в которой реализованы механизмы ЭП, генерация ключей ЭП и ключей проверки ЭП для приложения Инвест-Бизнес Онлайн.

Сертификат ключа проверки электронной подписи – документ на бумажном носителе, содержащий ключ проверки электронной подписи, собственноручную подпись владельца ключа, проставленную в присутствии сотрудника Банка, и подписанный уполномоченным представителем Банка, или электронный документ с ключом проверки электронной подписи клиента и его идентификационными данными, подписанный ЭП Банка.

Система «Интернет-Банк» - организационно-техническая система для юридических лиц, позволяющая Клиенту осуществлять обмен электронными документами с Банком через Интернет с использованием веб-сайта ib.chelinvest.ru с целью совершения банковских операций, получения информации, подачи заявлений, распоряжений и т.д.

Система «InvestPay» - организационно-техническая система для физических лиц, позволяющая Клиенту осуществлять обмен электронными документами с Банком через Интернет с использованием веб-сайта investpay.ru либо с использованием специального приложения для мобильных устройств (мобильное приложение) с целью совершения банковских операций, получения информации, подачи заявлений, распоряжений и т.д.

Система «Клиент-Банк» - организационно-техническая система для юридических лиц, позволяющая Клиенту осуществлять обмен электронными документами с Банком с использованием специализированного программного комплекса, устанавливаемого на компьютер Клиента, с целью совершения банковских операций, получения информации, подачи заявлений, распоряжений и т.д.

Система «Инвест-Бизнес Онлайн» - мобильное приложение, предназначенное для доступа юридических лиц к услугам системы

«Интернет-Банк» посредством мобильных устройств.

Система электронного документооборота (СЭД) – организационно-техническая система, представляющая собой совокупность программного, информационного и аппаратного обеспечения Банка и Клиентов, реализующая электронный документооборот. СЭД является корпоративной информационной системой, в которой Банк осуществляет управление сертификатами ключей проверки ЭП.

Средства криптографической защиты информации (СКЗИ) – совокупность программно-технических средств, обеспечивающих применение ЭП и шифрования при организации электронного документооборота. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Средства электронной подписи (СЭП) – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание ЭП в электронном документе с использованием ключа ЭП, подтверждение с использованием сертификата ключа проверки ЭП подлинности электронной подписи в электронном документе, создание криптографических ключей. СЭП могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Участник СЭД – Банк, а также Клиент Банка (физическое лицо или юридическое лицо, действующее в лице своих уполномоченных представителей, а также индивидуальный предприниматель или физическое лицо, занимающееся частной практикой, действующие лично и (или) в лице своих уполномоченных представителей), который присоединился к участию в СЭД на основании договора присоединения к СЭД либо на ином основании, установленном настоящими Правилами и его Приложениями.

Формат электронного документа – структура содержательной части электронного сообщения, на основе которого сформирован электронный документ.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного ЭД.

Электронный документ (ЭД) – логически целостная совокупность структурированных данных, имеющих смысл для участников информационного взаимодействия, закодированная способом, позволяющим обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации, которая соответствует установленному формату, подписана ЭП и может быть преобразована в форму, пригодную для однозначного восприятия содержания.

Электронный документооборот (ЭДО) – обмен электронными документами в соответствии с настоящими Правилами.

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Видами электронных подписей, используемых в рамках ЭДО, являются простая электронная подпись и неквалифицированная электронная подпись.

OTP-токен - компактное электронное устройство, предназначенное для генерации одноразовых паролей.

USB- токен - компактное электронное устройство, предназначенное для выработки ЭП и хранения не извлекаемого ключа пользователя.

Verified by Visa – сервис, обеспечивающий дополнительное подтверждение операции в процессе приобретения товаров/услуг через Интернет по Корпоративной банковской карте путем запроса у Клиента одноразового пароля, отправляемого в SMS-сообщении.

1.2. Предмет регулирования настоящих Правил

1.2.1. Настоящие Правила, Приложения к настоящим Правилам, а также Порядок использования электронных средств платежа юридическими лицами (Приложение № 10) / Правила использования электронных средств платежа Клиентами-физическими лицами устанавливают общие принципы осуществления электронного документооборота между Банком и Клиентом, являющимися Участниками СЭД. Все Приложения к Правилам являются неотъемлемой частью Правил. Для присоединения к Порядку использования электронных средств платежа юридическими лицами Клиент - юридическое лицо оформляет Заявление о заключении договора об использовании электронного средств платежа юридическими лицами в соответствии с Приложением № 9. Для присоединения к Правилам использования электронных средств платежа Клиентами – физическими лицами Клиент – физическое лицо оформляет Заявление о присоединении к Правилам использования электронных средств платежа Клиентами - физическими лицами.

1.2.2. Положения настоящих Правил применяются, если иное не предусмотрено законодательными или иными правовыми актами РФ, включая нормативные акты Банка России.

1.2.3. В соответствии с настоящими Правилами в электронный документооборот включаются все виды электронных документов, направляемых сторонами друг другу, в том числе:

- расчетные документы (платежные поручения, платежные требования, инкассовые поручения);
- письма, заявления, касающиеся расчетно-кассового обслуживания, обслуживания операций в иностранной валюте;
- письма, связанные с отношениями, вытекающими из Договора присоединения к системе электронного документооборота ПАО «ЧЕЛЯБИНВЕСТБАНК»;
- заявки на покупку - продажу валюты за счет средств Клиента, находящихся на счете;
- анкеты, заявления и иные документы, связанные с кредитованием;
- заявки на выдачу очередного транша кредита;
- заявления на получение кредитного отчета в БКИ;
- документы, связанные с предоставлением банковских гарантий, заключением рамочных соглашений о предоставлении банковских гарантий, заявлений о предоставления гарантии по заключенному рамочному соглашению о предоставлении банковских гарантий,
- любые уведомления Банка, направленные в рамках заключенных кредитных договоров, в том числе о досрочном погашении кредита, о возникновении просроченной задолженности по кредиту, о получении требования Бенефициара о выплате по гарантии, о возмещении денежных средств, выплаченных по гарантии;
- согласия на обработку персональных данных;
- уведомления, направляемые Клиентом Банку об утрате ЭСП и (или) о его использовании без согласия Клиента;
- сообщения, направляемые Банком Клиенту о совершении каждой операции с использованием ЭСП;
- сканированные копии документов, необходимых для проведения идентификации Клиента, в том числе: договоры аренды (субаренды), свидетельства о праве собственности на объект недвижимости, решения (протоколы), свидетельства, паспорта, анкеты, финансовую отчетность и т.п., за исключением Устава (изменений в Устав), карточек с образцами подписей и оттиска печати, которые предоставляются в Банк нотариально заверенные либо заверяются уполномоченным сотрудником Банка.

1.3. Регулирование электронного документооборота

1.3.1. Электронный документооборот в СЭД регулируется следующими документами:

- договором присоединения к СЭД, заключаемым между Банком и Клиентом;
- настоящими Правилами;
- другими договорами и соглашениями Банка и Клиента, предусматривающими обмен между ними электронными документами.

1.4. Порядок и условия допуска Клиента к СЭД:

1.4.1. Клиент допускается к осуществлению документооборота в СЭД после выполнения им всей совокупности следующих действий (если иной порядок допуска (присоединения) к СЭД не установлен настоящими Правилами и его Приложениями):

- заключения Договора присоединения к СЭД ПАО «ЧЕЛЯБИНВЕСТБАНК» и / или подписание соответствующего заявления, предусматривающего присоединение к подсистеме СЭД;
- установки необходимых аппаратных средств, программного обеспечения на месте Клиента в соответствии с требованиями Приложения №1 к настоящим Правилам и инструкций по эксплуатации упомянутых аппаратных средств и программного обеспечения;
- получения необходимых паролей и идентификаторов для доступа к СЭД в Банке;
- выработки криптографических ключей Участника СЭД;
- подписание сертификата ключа проверки электронной подписи в присутствии сотрудника Банка;
- регистрацией Банком сертификата ключа проверки электронной подписи для уполномоченного лица - Участника СЭД.

1.5. Порядок вступления в действие настоящих Правил, а также внесения в них изменений

1.5.1. Настоящие Правила утверждаются Правлением Банка. Изменения и дополнения в настоящие Правила вносятся Банком в одностороннем порядке по решению Правления Банка. Правление Банка вправе определять сроки и порядок вступления в силу изменений и дополнений в настоящие Правила.

1.5.2. Настоящие Правила вступают в силу в отношении Участника СЭД в результате подписания заявления, включающего в себя присоединение к подсистеме СЭД (для физических лиц) либо для юридических лиц - подписания заявления о присоединении к подсистеме СЭД (Приложение №8) и заключения между Участником – юридическим лицом и Банком Договора присоединения к СЭД ПАО «ЧЕЛЯБИНВЕСТБАНК», если иной порядок вступления в силу Правил в отношении Участника СЭД не установлен настоящими Правилами и его Приложениями.

1.6. Порядок уведомления о внесении изменений в настоящие Правила

1.6.2. Если иное не предусмотрено решением Банка, изменения и дополнения в настоящие Правила доводятся Банком до сведения Клиентов посредством размещения новой редакции Правил и Приложений на сайте Банка, но не позднее, чем за 14 дней до даты вступления в силу данных изменений и дополнений.

1.6.3. Тексты настоящих Правил и всех изменений и дополнений к ним на бумажном носителе должны храниться Банком в течение 5 лет после прекращения их действия.

1.6.4. Клиент имеет право запрашивать копии недействующих копий Правил и всех изменений и дополнений к ним на бумажном носителе. Указанные документы предоставляются Клиенту на платной основе в соответствии с тарифами Банка в течение 15 дней после получения соответствующего запроса от Клиента.

2. ЭЛЕКТРОННЫЙ ДОКУМЕНТ

2.1. Требования, предъявляемые к электронному документу

2.1.1. Электронный документ, сформированный в СЭД в соответствии с настоящими Правилами, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия.

Электронный документ в виде сканированной копии документа имеет юридическую силу копии документа при условии ее удостоверения лицом – владельцем ЭП.

2.1.2. Электронный документ, используемый в СЭД, считается оформленным надлежащим образом при условии его соответствия законодательству Российской Федерации, настоящим Правилам, правилам Банка, а также договорам, заключаемым между Банком и Клиентом.

2.1.3. Электронный документ должен быть сформирован в одном из форматов, определенных в настоящих Правилах, правилах Банка, а также договорах, заключенных между Банком и Клиентом, и подписан электронной подписью либо другим аналогом собственноручной подписи, предусмотренным в отдельных подсистемах СЭД.

2.1.4. Электронный документ, имеющий формат, не отвечающий установленным правилам, в качестве электронного документа в соответствии с настоящими Правилами не рассматривается.

2.2. Использование электронной подписи и шифрования в электронном документообороте

2.2.1. ЭД может быть подтвержден простой электронной подписью или подписан неквалифицированной ЭП в соответствии с особенностями подсистем СЭД.

2.2.2. Для неквалифицированной ЭП могут применяться только те ключи ЭП, для которых Банк зарегистрировал сертификат ключа проверки неквалифицированной ЭП для Клиента или его уполномоченного лица.

2.2.3. ЭД, подписанный неквалифицированной ЭП, считается подписанным лично тем лицом, которое является владельцем ключа неквалифицированной ЭП, при условии успешной проверки неквалифицированной ЭП ЭД. ЭД, подтвержденный простой ЭП, считается подтвержденным лично тем лицом, которое получило в Банке ключевую информацию для простой ЭП.

2.2.4. Замена ключей ЭП неквалифицированной ЭП не влияет на юридическую силу электронного документа, если он был подписан действующим на момент подписания ключом ЭП неквалифицированной ЭП в соответствии с настоящими Правилами. Замена ключевой информации простой ЭП не влияет на юридическую силу ЭД, если он был подтвержден простой ЭП с действующей на момент подтверждения ключевой информацией в соответствии с настоящими Правилами.

2.2.5. Клиент обязан лично применять ключевую информацию простой ЭП и ключи ЭП неквалифицированной ЭП, владельцем которых он является.

2.2.6. Для осуществления документооборота Клиент может иметь несколько одновременно действующих ключей ЭП неквалифицированной ЭП и шифрования, при условии регистрации соответствующих им сертификатов в Банке, а также несколько наборов ключевой информации для простой ЭП.

2.2.7. ЭД, содержащий конфиденциальную информацию, подлежит шифрованию. Конфиденциальность ЭД определяется отправителем.

2.2.8. При получении зашифрованного ЭД он расшифровывается в соответствии с применяемой технологией, затем проверяется ЭП ЭД.

2.2.9. Предусмотренные для данного документа правовые последствия могут наступить, только если получен положительный результат проверки ЭП.

2.2.10. С целью уменьшения объемов передаваемой информации при транспортировке электронных документов могут использоваться специальные алгоритмы сжатия информации. В случае необходимости может выполняться шифрование сжатого электронного документа.

2.3. Использование электронного документа

2.3.1. Все юридические действия, оформляемые посредством электронных документов в соответствии с настоящими Правилами, а также внутренними нормативными документами Банка, признаются совершенными в письменной форме и не могут быть оспорены только на том основании, что они совершены в электронном виде.

2.3.2. ЭД вступает в силу с момента его получения участником СЭД при условии, что он подписан ЭП Банка или уполномоченного лица Клиента.

2.4. Подлинник электронного документа

2.4.1. ЭД документ может иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа. Для создания дополнительного экземпляра существующего ЭД осуществляется воспроизводство содержания документа вместе с электронной подписью.

2.4.2. Все экземпляры ЭД являются подлинниками данного ЭД.

2.4.3. ЭД не может иметь копий в электронном виде.

2.4.4. Подлинник электронного документа считается не существующим в случаях, если:

- не существует ни одного учтенного Банком экземпляра данного электронного документа и восстановление таковых невозможно и (или)
- не существует способа установить подлинность электронной подписи, которой подписан данный документ.

2.5. Копии электронного документа на бумажном носителе

2.5.1. Копии электронного документа могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью лица, уполномоченного Банком или Клиентом, являющимся отправителем или получателем ЭД.

2.5.2. Копии ЭД на бумажном носителе должны соответствовать требованиям действующего законодательства и государственным стандартам.

2.5.3. Электронный документ и его копии на бумажном носителе должны быть аутентичными.

2.5.4. Программные средства, осуществляющие преобразование ЭД для изготовления (распечатки) в виде бумажного документа, являются составной частью программного обеспечения, используемого в подсистемах СЭД.

3. ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

3.1. Электронный документооборот

Электронный документооборот включает:

- формирование электронного документа;
- отправку и доставку электронного документа;
- проверку электронного документа;
- возврат электронного документа;
- отзыв электронного документа;
- учет электронных документов (регистрацию входящих и исходящих ЭД);
- хранение электронных документов (ведение архивов ЭД);
- создание дополнительных экземпляров электронного документа;
- создание бумажных копий электронного документа.

3.2. Формирование электронного документа

Формирование электронного документа осуществляется в следующем порядке:

- формирование электронного документа сообщения в формате, установленном для данного электронного документа;
- подписание сформированного ЭД электронной подписью уполномоченного лица.

3.3. Отправка и доставка электронного документа

3.3.1. В отношениях между отправителем и получателем ЭД считается исходящим от отправителя, если электронный документ отправлен:

- самим отправителем;
- лицом, уполномоченным действовать от имени отправителя в отношении данного ЭД;
- информационной системой, используемой отправителем и действующей автоматически.

3.3.2. ЭД не считается исходящим от отправителя, если:

- получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что ЭД не исходит от отправителя, или
- получатель знал или должен был знать, в том числе в результате выполнения проверки, о том, что получен искаженный ЭД.

3.3.3. Особенности отправки, доставки и получения электронных документов могут устанавливаться настоящими Правилами и правилами Банка.

3.4. Проверка подлинности доставленного электронного документа

3.4.1. Проверка электронного документа включает:

- проверку электронного документа на соответствие установленному для него формату;
- проверку подлинности всех ЭП электронного документа для систем Клиент-Банк, Интернет-Банк, «Инвест-Бизнес Онлайн» или иного аналога собственноручной подписи в рамках установленных лимитов для системы «InvestPay»;

3.4.2. В случае положительного результата проверки ЭД данный электронный документ принимается к исполнению или подлежит дальнейшей обработке. В противном случае данный ЭД считается не полученным, о чем получатель должен уведомить отправителя в любой доступной форме.

3.4.3. При получении зашифрованного ЭД для проведения проверки подлинности ЭД сначала выполняется расшифрование электронного документа. В случае невозможности расшифровывания электронного документа данный ЭД считается не полученным, о чем получатель должен уведомить отправителя в любой доступной форме.

3.4.4. При получении расчетных банковских документов по системам дистанционного банковского обслуживания проведение операций осуществляется только при следующих условиях:

- при наличии необходимого минимального количества действующих электронных подписей под документом: одной первой подписи (руководителя) и при наличии - одной второй подписи (подписи главного бухгалтера, заместителя, при наличии);

- при строгом соответствии лиц, обладающих правом электронной подписи, лицам, внесенным в бумажную карточку с образцами подписей и оттиска печати, предоставленную в Банк;
- при действительности полномочий лиц, обладающих правами электронной подписи, на момент совершения операций;
- при отсутствии необходимого количества подписей, истечения срока действия подписей, их несоответствии подписям в карточке с образцами подписей и оттиска печати, при истечении сроков полномочий лиц, указанных в карточке с образцами подписей и имеющих право подписывать расчетные документы, или подписании документов неуполномоченными лицами Банк отказывает в проведении расчетных документов.

3.4.5. Банк имеет право отказать в проведении расчетных документов, в получении электронных писем, других документов в случае невыполнения клиентами настоящих Правил.

3.5. Отзыв электронного документа

3.5.1. Участник СЭД вправе отозвать отправленный электронный документ путем отправки получателю электронного документа "Уведомление об отзыве".

3.5.2. В "Уведомлении об отзыве" должно указываться основание отзыва электронного документа.

3.5.3. Электронный документ может быть отозван отправителем только до начала его исполнения получателем.

3.5.4. Порядок отзыва и формат электронного документа, уведомляющего об отзыве ЭД, устанавливается правилами Банка.

3.6. Учет электронных документов

3.6.1. Учет электронных документов осуществляется путем ведения электронных журналов учета или традиционных бумажных журналов учета. Технология ведения электронных журналов учета включает программно-технологические процедуры заполнения и администрирования электронных журналов и средства хранения этой информации. Программные средства ведения электронных журналов учета являются составной частью программного обеспечения, используемого для организации электронного документооборота.

3.6.2. Для выполнения текущих работ по ведению учета электронных документов в СЭД Банк назначает ответственное лицо.

3.6.3. Особенности учета электронных документов в СЭД определяются правилами Банка.

3.6.4. При учете исходящего электронного документа Банк обеспечивает учет следующих данных:

- уникальный исходящий номер документа, формируемый путем использования префикса конкретной электронной системы обработки данных и уникального номера, присваиваемого в рамках конкретного электронного журнала учета;
- тип документа или его код, используемый в конкретной электронной системе обработки данных или название документа (для документов общего назначения, не имеющих установленных стандартных типов);
- идентификатор исполнителя или код подготовившей документ электронной системы обработки данных (для автоматически подготавливаемых документов);
- дата и время подготовки документа (дата и время проставления электронной подписи исполнителем документа);
- идентификатор отправителя документа (может совпадать с идентификатором исполнителя);
- идентификатор адресата;
- отметка об отправке документа (дата и время отправки документа может совпадать с датой и временем подготовки документа);
- отметка о доставке документа;
- исходящий номер отзываемого документа (для документов "Уведомление об отзыве");
- иные данные по усмотрению Банка.

3.6.5. При учете входящего электронного документа Банк обеспечивает учет следующих данных:

- уникальный входящий номер документа;
- дата и время получения документа;
- исходящий номер полученного документа;
- идентификатор отправителя документа;
- дата и время подготовки документа (дата и время проставления электронной подписи исполнителем документа);
- отметка об отправке документа (дата и время отправки документа может совпадать с датой и временем подготовки документа);
- тип документа или его код, используемый в конкретной электронной системе обработки данных или название документа (для документов общего назначения, не имеющих установленных стандартных типов);
- входящий номер отзываемого документа (для документов "Уведомление об отзыве");
- исходящий номер отзываемого документа (для документов "Уведомление об отзыве");
- иные данные по усмотрению Банка.

3.6.6. Банк обеспечивает защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах учета электронных документов. Срок хранения учетных данных определяется внутренними положениями Банка.

3.7. Хранение электронных документов

3.7.1. Все электронные документы, учтенные в СЭД, хранятся в течение сроков, предусмотренных нормативными документами Банка. Электронные документы хранятся либо в электронных архивах, либо в виде копий электронных документов на бумажных носителях, заверенных уполномоченным лицом.

3.7.2. Если правилами Банка не предусмотрено иное, электронные документы хранятся в том же формате, в котором они были сформированы, отправлены или получены. Срок хранения электронных документов - не менее 5 лет.

3.7.3. Хранение электронных документов сопровождается хранением соответствующих электронных или бумажных журналов учета, сертификатов ключей проверки электронной подписи и программного обеспечения, обеспечивающего возможность работы с электронными журналами и проверки электронной подписи хранимых электронных документов.

3.7.4. Ключи ЭП хранятся в электронных архивах только в случае хранения электронных документов в зашифрованном на этих ключах виде.

3.7.5. При хранении электронных документов обеспечивается привязка (синхронизация) электронных документов и соответствующих сертификатов ключей проверки электронной подписи для проведения процедуры разрешения конфликтных ситуаций.

3.7.6. Обязанности хранения электронных документов возлагаются на Банк и Клиентов.

3.7.7. Электронные архивы и архивы бумажных копий электронных документов подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

4. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Средства обеспечения информационной безопасности

4.1.1. Информация, содержащая персональные данные, и конфиденциальная информация в системе электронного документооборота должна быть защищена.

4.1.2. Соблюдение требований информационной безопасности при организации электронного документооборота обеспечивает:

- конфиденциальность информации (получить доступ к информации могут только уполномоченные лица);
- целостность передаваемой информации (гарантирование, что данные передаются без искажений и исключается возможность подмены информации);
- аутентификацию (когда передаваемую информацию может получить только то лицо, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).

4.1.3. Требования по информационной безопасности при организации электронного документооборота реализуются посредством применения программно-технических средств и организационных мер.

4.1.4. К программно-техническим средствам относятся:

- программные средства, специально разработанные для осуществления электронного документооборота;
- система паролей и идентификаторов для ограничения доступа пользователей и операторов к техническим и программным средствам системы электронного документооборота;
- средства электронной подписи;
- средства криптографической защиты информации;
- программно-аппаратные средства защиты от несанкционированного доступа;
- средства защиты от программных вирусов;
- средства защиты от атак.

4.1.5. К организационным мерам относятся:

- размещение технических средств в помещениях с контролируемым доступом;
- административные ограничения доступа к этим средствам;
- задание режима использования пользователями и операторами паролей и идентификаторов;
- допуск к осуществлению документооборота только специально обученных и уполномоченных на то лиц;
- поддержание программно-технических средств в исправном состоянии;
- резервирование программно-технических средств;
- обучение технического персонала;
- защита технических средств от повреждающих внешних воздействий (пожар, воздействие воды и т.п.).

4.1.6. Порядок использования средств криптографической защиты информации, применяемых в СЭД, определяется настоящими Правилами, включая Приложения к ним. Особенности использования средств криптографической защиты информации, применяемых в СЭД, могут также определяться правилами Банка.

4.1.7. Несоблюдение требований информационной безопасности может привести к хищению персональной, ключевой информации или использованию рабочего места клиента дистанционно третьими неуполномоченными лицами. Таким образом, в случае несоблюдения требований информационной безопасности Клиентом, недостаточного внимания Клиента к применению программно-технических средств и к реализации организационных мер, направленных на соблюдение информационной безопасности, Банк ответственности не несет.

4.2. Порядок действий при компрометации криптографических ключей

4.2.1. Порядок действий при Компрометации Ключевой информации.

4.2.2. В случае Компрометации Ключевой информации ее владелец обязан в установленном порядке незамедлительно уведомить Администратора безопасности о компрометации. Порядок действий при компрометации устанавливается в разделе 4 Приложения № 1 к настоящим Правилам.

4.2.3. В случае получения уведомления о компрометации Ключевой информации, датой и временем компрометации считаются дата и время, указанные в уведомлении о компрометации.

4.2.4. Уведомление о компрометации должно быть подтверждено в течение одного рабочего дня официальным уведомлением о компрометации в письменном виде. Уведомление должно содержать:

- идентификационные параметры скомпрометированной Ключевой информации;
- предварительно согласованные с Администратором безопасности дату и время, начиная с которого Ключевая информация считается скомпрометированной.

4.2.5. Дата и время компрометации, указываемые в уведомлении о компрометации, не могут быть ранее даты и времени получения данного уведомления Администратором безопасности или получения предварительного сообщения о компрометации Администратором безопасности по телефону.

4.2.6. После получения уведомления о компрометации получатель данного уведомления не должен использовать скомпрометированную Ключевую информацию в СЭД.

4.2.7. При получении электронного документа, подписанного (подтвержденного) скомпрометированной Ключевой информацией, данный ЭД считается не сформированным в соответствии с п. 2.1.1 настоящих Правил.

4.2.8. В случае установления Банком обстоятельств, установленных разделом 4 Приложения 1 к настоящим Правилам, и при которых возможна Компрометация Ключевой информации, Банк имеет право отключить Клиента от СЭД.

4.2.9. Подключение к СЭД в данном случае возможно только после устранения причин Компрометации Ключевой информации, подтверждения полномочий лиц, имеющих право использования Ключевой информации в рамках соответствующих подсистем СЭД, и личного присутствия указанных лиц в Банке.

4.2.10. Отключение Банком Клиента от СЭД в соответствии с п.4.2.7 настоящих Правил является уведомлением о компрометации Ключевой информации.

4.3. Условия и порядок отключения Банком Клиентов от СЭД в одностороннем порядке.

4.3.1. Банк имеет право отключить Клиента от СЭД в следующих случаях:

- подозрение в компрометации ключа в соответствии с п. 4.2.1 настоящих Правил;
- отсутствия Клиента по своему месту нахождения и (или) не предоставления документов, позволяющих установить местонахождения Клиента;

- не предоставление в срок документов, требование о предоставлении которых основано на договоре банковского счета;
- возникновения чрезвычайных ситуаций, установленных п.5.1 настоящих Правил;
- при установлении БАНКОМ в рамках мероприятий, предусмотренных Федеральным законом от 07.08.2001г. № 115-ФЗ, фактов совершения им операций, подпадающих под признаки сомнительных (необычных).
- предусмотренных иными документами.

4.3.2 Банк имеет право отключить Клиента от СЭД и расторгнуть с ним договор на ЭДО в следующих случаях:

- срок действия ключа ЭП истек более одного года назад;
- договор с Банком, взаимодействие в рамках которого осуществлялось с использованием СЭД, в том числе договор банковского счета, генеральное соглашение об условиях заключения депозитных сделок с юридическими лицами и индивидуальными предпринимателями, генеральное соглашение об общих условиях совершения сделок покупки-продажи безналичной иностранной валюты, договор об открытии и ведении корреспондентского счета, договор об организации выплаты заработной платы сотрудникам предприятия через картсчета, кредитный договор, договор с Поставщиком услуг, договор о предоставлении банковских гарантий, рамочное соглашение о предоставлении банковских расторгнут.

5. ЧРЕЗВЫЧАЙНЫЕ СИТУАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

5.1. Обстоятельства, которые могут послужить причиной возникновения чрезвычайных ситуаций, в том числе технических сбоев

5.1.1. К числу обстоятельств, которые способны послужить причиной возникновения чрезвычайных ситуаций, в том числе технических сбоев, могут быть отнесены следующие:

- любые события и/или обстоятельства, которые, по оценке Правления Банка, временно или на неопределенный срок сделали, делают или могут сделать невозможным или значительно затруднить осуществление электронного документооборота; к таким событиям/обстоятельствам, в том числе, могут быть отнесены:
  - пожары, наводнения, иные стихийные бедствия или техногенные катастрофы;
  - разрушения или значительные повреждения занимаемых указанными организациями помещений;
  - нестабильность или отключение электроэнергии, которое не может быть нейтрализовано имеющимися в распоряжении указанных организаций техническими средствами;
  - неработоспособность программного обеспечения, вычислительной техники, оргтехники, средств связи, включая средства телекоммуникаций;
  - массовые беспорядки, вооруженные столкновения, демонстрации;
  - террористические акты или диверсии;
- неспособность Банка выполнять свои функции;
- любые другие подобные события или обстоятельства, которые могут существенным образом затруднить или сделать невозможным осуществление электронного документооборота.

5.1.2. К числу обстоятельств, которые способны послужить причиной возникновения чрезвычайных ситуаций могут быть отнесены также следующие:

- принятие или любые изменения законодательных или иных актов государственных органов Российской Федерации или распоряжения данных органов, инструкции, указания, заявления, письма, телеграммы или иные действия (далее – акты), которые прямо или косвенно или при определенном их толковании или определенном стечении обстоятельств, начиная с момента утверждения данных актов или с иного срока, временно или на неопределенный срок сделали, делают или могут сделать невозможным или значительно затруднить дальнейшее осуществление электронного документооборота в том виде, форме и порядке, в которых он осуществлялся до принятия данных актов.

5.2. Порядок уведомления о наступлении обстоятельств, способных послужить причиной возникновения чрезвычайных ситуаций

5.2.1. В случае наступления хотя бы одного из обстоятельств, соответствующих перечисленным в п. 5.1 настоящих Правил:

- Клиент или Банк обязан незамедлительно с учетом сложившейся ситуации и способом, доступным в сложившихся обстоятельствах, известить Банк о возникших обстоятельствах;
- Банк обязан незамедлительно с учетом сложившейся ситуации и способом, доступным в сложившихся обстоятельствах, известить Клиентов о возникших обстоятельствах.

5.2.2. Впоследствии Клиент или Банк обязаны письменным сообщением подтвердить уведомление о возникших обстоятельствах, способных послужить причиной возникновения чрезвычайных ситуаций.

5.2.3. Банк незамедлительно после возникновения у него обстоятельств, соответствующих перечисленным в п. 5.1 настоящих Правил или получения уведомления, указанного в п.5.2.1, обязан рассмотреть возникшую ситуацию и принять квалифицирующее решение.

5.2.4. Для квалификации ситуации, связанной с наличием хотя бы одного из обстоятельств, соответствующих перечисленным в п. 5.1 настоящих Правил в качестве чрезвычайной ситуации, в том числе технического сбоя, достаточно решения Правления Банка.

5.2.5. Решение Правления Банка о квалификации обстоятельств из числа перечисленных в п. 5.1 настоящих Правил в качестве чрезвычайной ситуации (квалифицирующее решение Банка) оформляется документом, составленным в письменной форме.

5.3. Последствия принятия квалифицирующего решения Правлением Банка

5.3.1. В случае признания Правлением Банка ситуации, связанной с наличием хотя бы одного из обстоятельств, соответствующих перечисленным в п. 5.1 настоящих Правил в качестве чрезвычайной ситуации, Банк незамедлительно способом, наиболее удобным с учетом сложившейся ситуации, связывается с Клиентом/Клиентами и уведомляет о возникновении чрезвычайной ситуации.

5.3.2. В случае признания Исполнительным органом Банка ситуации, связанной с наличием хотя бы одного из обстоятельств, соответствующих перечисленным в статье 5.1 настоящих Правил в качестве чрезвычайной ситуации, электронный документооборот может быть прекращен по решению Исполнительного органа Банка.

5.3.3. Одновременно с признанием ситуации чрезвычайной Банк приступает к разработке мер по урегулированию сложившейся чрезвычайной ситуации в СЭД.

5.3.4. Возобновление электронного документооборота осуществляется по решению Исполнительного органа Банка.

5.4. Меры по урегулированию чрезвычайных ситуаций

5.4.1. В качестве мер по урегулированию сложившейся чрезвычайной ситуации Банк вправе:

- прекратить или ограничить обращение всех или части электронных документов в СЭД;

- совместно с Клиентом определить порядок действий по устранению технического сбоя (договоренность сторон о порядке совместных действий оформляется Протоколом, составленным в письменной форме и подписанным уполномоченными представителями сторон);
- потребовать от Клиентов, являвшихся отправителями электронных документов в рамках договоров между Клиентом и Банком о применении настоящих Правил, безвозмездного и незамедлительного с учетом сложившихся обстоятельств предоставления Банку копий на бумажных носителях всех или части электронных документов, обращавшихся в СЭД за определенный период времени;
- потребовать от Клиентов за их счет незамедлительного с учетом сложившихся обстоятельств восстановления, в том числе, в виде копий на бумажных носителях обращения всех или части электронных документов в СЭД;
- потребовать от Клиентов безвозмездного и незамедлительного с учетом сложившихся обстоятельств предоставления копий, в том числе и, в случае необходимости, нотариально заверенных копий журналов электронных документов, обращавшихся в СЭД за определенный период;
- предусмотреть иные меры, направленные на преодоление чрезвычайной ситуации.

5.4.2. При принятии решений по урегулированию чрезвычайных ситуаций Исполнительный орган Банка вправе:

- устанавливать сроки и форму уведомления Клиентов о своих решениях;
- устанавливать сроки и порядок исполнения своих решений;
- обуславливать порядок вступления в силу своих решений определенными обстоятельствами.

5.4.3. Решения Исполнительного органа Банка по урегулированию чрезвычайной ситуации в СЭД являются обязательными для исполнения Банком и Клиентами.

5.4.4. О решениях Исполнительного органа Банка о мерах по урегулированию чрезвычайной ситуации Клиенты уведомляются не позднее 14 дней со дня принятия данных мер в соответствии с данным решением.

6. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ, ВОЗНИКШИХ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СЭД

6.1. Возникновение конфликтных ситуаций в связи с осуществлением электронного документооборота в СЭД

6.1.1. В связи с осуществлением электронного документооборота возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронных документов, а также использованием в данных документах электронной подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- не подтверждение подлинности электронных документов средствами электронной подписи принимающей Стороны;
- оспаривание факта формирования электронного документа;
- оспаривание факта идентификации владельца сертификата ключа проверки электронной подписи, подписавшего документ;
- заявление Участника об искажении электронного документа;
- оспаривание факта отправления и/или доставки электронного документа;
- оспаривание времени отправления и/или доставки электронного документа;
- оспаривание аутентичности экземпляров электронного документа и/или подлинника и копии электронного документа на бумажном носителе;
- иные случаи возникновения конфликтных ситуаций, связанных с функционированием СЭД.

6.1.2. Конфликтная ситуация возникает также в случае, если Клиент или Банк:

- высказывает недоверие к составу и формату электронных документов, хранящихся в локальном архиве рабочего места Клиента или Банка, или
- высказывает недоверие к программному обеспечению, функционирующему на данном рабочем месте.

6.2. Уведомление о конфликтной ситуации

6.2.1. В случае возникновения конфликтной ситуации Клиент или Банк, предполагающий возникновение конфликтной ситуации, должен незамедлительно, но не позднее чем в течение трех рабочих дней или в иной более короткий срок, указанный в правилах Банка, после возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации Банку (Клиенту).

6.2.2. Уведомление о предполагаемом наличии конфликтной ситуации должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации. Независимо от формы, в которой составлено уведомление (письменная или электронный документ), оно должно содержать все реквизиты электронного документа, предусмотренные настоящими Правилами. Кроме того, в нем должны быть указаны фамилия, имя и отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

6.2.3. Уведомление о наличии конфликтной ситуации составляется в письменной форме и направляется с нарочным либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

6.2.4. Сторона, которой направлено уведомление, обязана незамедлительно, однако не позднее чем в течение следующего рабочего дня (или в иной более короткий срок, указанный в правилах Банка), проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

6.3. Разрешение конфликтной ситуации в рабочем порядке

6.3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Клиента или Банка, которому было направлено уведомление.

6.3.2. В случае если уведомитель не удовлетворен информацией, полученной от Клиента или Банка, которому направлялось уведомление, для рассмотрения конфликтной ситуации формируется техническая комиссия.

6.4. Формирование технической комиссии, ее состав

6.4.1. В случае, если конфликтная ситуация не была урегулирована в рабочем порядке, техническая комиссия должна быть сформирована не позднее чем на следующий рабочий день после того, как принято решение о необходимости сформировать техническую комиссию, или не позднее, чем на шестой рабочий день после получения уведомления о конфликтной ситуации.

6.4.2. Если Клиент и Банк, являющиеся сторонами в конфликтной ситуации не договорятся об ином, в состав конфликтной комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих сторон.

6.4.3. В состав технической комиссии, как правило, назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности сторон. Лица, входящие в состав технической комиссии, должны обладать необходимыми знаниями в области построения системы криптозащиты, работы компьютерных информационных систем.

6.4.4. Право представлять в комиссии соответствующую Сторону должно подтверждаться доверенностью, выданной каждому представителю на срок работы комиссии.

6.4.5. По инициативе любой из сторон к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, соответствующие требованиям, указанным в п.6.4.3 настоящих Правил, Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

6.5. Компетенция и полномочия технической комиссии

6.5.1. Сформированная техническая комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки электронного документа, его подлинности, а также о подписании электронного документа конкретной электронной подписью, аутентичности отправленного документа полученному.

6.5.2. Комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению комиссии, для выяснения причин и последствий возникновения конфликтной ситуации.

6.5.3. Комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.

6.5.4. Для проведения необходимых проверок и документирования данных, используемых при указанных проверках, применяется специальное программное обеспечение с соблюдением порядка, установленного настоящими Правилами.

6.6. Протокол работы технической комиссии

6.6.1. Все действия, предпринимаемые комиссией для выяснения фактических обстоятельств, а также выводы, сделанные комиссией, заносятся в Протокол работы технической комиссии. Протокол работы технической комиссии должен содержать следующие данные:

- состав комиссии с указанием сведений о квалификации каждого из членов комиссии;
- краткое изложение обстоятельств возникшей конфликтной ситуации;
- мероприятия, проводимые комиссией для установления причин и последствий возникшей конфликтной ситуации, с указанием даты времени и места их проведения;
- выводы, к которым пришла комиссия в результате проведенных мероприятий;
- подписи всех членов комиссии.

6.6.2. В случае, если мнение члена (или членов) комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов комиссии, об этом в Протоколе составляется соответствующая запись, которая подписывается членом (или членами комиссии), чье особое мнение отражает соответствующая запись.

6.6.3. Протокол составляется в одном подлинном экземпляре на бумажном носителе, который находится на хранении в Банке. По требованию любой из сторон в конфликтной ситуации или любого из членов технической комиссии им может быть выдана заверенная Банком копия Протокола.

6.7. Акт по итогам работы технической комиссии

6.7.1. По итогам работы технической комиссии составляется Акт, в котором содержится краткое изложение выводов технической комиссии. Помимо изложения выводов о работе технической комиссии Акт должен также содержать следующие данные:

- состав комиссии;
- дату и место составления Акта;
- даты и время начала и окончания работы комиссии;
- краткий перечень мероприятий, проведенных комиссией;
- подписи членов комиссии;
- указание на особое мнение члена (или членов комиссии), в случае наличия такового.

6.7.2. Акт составляется в таком количестве экземпляров, чтобы каждая из сторон в конфликтной ситуации имели по одному подлинному экземпляру составленного акта. По требованию члена комиссии ему может быть выдана заверенная Банком копия Акта.

6.7.3. К Акту может прилагаться особое мнение члена (или членов комиссии), не согласных с выводами технической комиссии, указанными в Акте. Особое мнение составляется в произвольной форме в таком же количестве подлинных экземпляров, что и Акт, и составляет приложение к Акту.

6.7.4. Акт по итогам работы технической комиссии направляется сторонам в конфликтной ситуации с нарочным либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

6.8. Согласительный порядок урегулирования споров и разногласий

6.8.1. Все споры и разногласия, которые могут возникнуть в связи с применением, нарушением, толкованием настоящих Правил, признанием недействительными настоящих Правил или их части, стороны будут стремиться разрешить, используя механизмы согласительного урегулирования споров и разногласий.

6.8.2. В случае, если конфликтная ситуация не урегулирована в процессе переговоров, стороны разрешают спор в порядке, предусмотренном действующим законодательством РФ.

Настоящие Правила вступают в силу с 26.12.2018 г. Правила электронного документооборота ПАО «ЧЕЛЯБИНВЕСТБАНК» № 26-037-П, утвержденные Правлением банка (Протокол № 238 от «23» ноября 2018г..), считать с 26.12.2018 г. недействительными.

Правление Банка

Приложение № 1
к Правилам электронного документооборота

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ЭЛЕКТРОННЫЕ ПОДПИСИ В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПАО «ЧЕЛЯБИНВЕСТБАНК»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Банк обеспечивает защиту электронных документов, обрабатываемых в подсистемах электронного документооборота, используя ЭП и другие аналоги собственноручной подписи.

1.2. Клиенты признают, что используемые в СЭД неквалифицированные ЭП и другие аналоги собственноручной подписи обеспечивают достаточную конфиденциальность электронного документооборота и позволяют идентифицировать владельца сертификата ключа проверки ЭП, а также другого аналога собственноручной подписи.

1.3. Ключи ЭП и шифрования Клиента и соответствующие им сертификаты ключей проверки ЭП, зарегистрированные в СЭД, имеют ограниченный срок действия. Применяемые СКЗИ в процессе их использования автоматически выполняют контроль срока действия криптографических ключей и актуальности сертификатов ключей проверки ЭП.

1.4. Клиент не может подписать электронный документ своей ЭП или произвести зашифрование/расшифрование информации в текущий момент времени, если к этому времени истек срок действия его ключей ЭП. Также Клиент не может произвести расшифрование информации в случае истечения срока действия сертификата ключа проверки ЭП, необходимого для выполнения соответствующей операции.

1.5. При использовании технологии шифрования электронных документов Клиент не должен хранить электронные документы в архивах в зашифрованном виде. Шифрование электронных документов (ЭД) осуществляется только для обеспечения конфиденциальности информации при транспортировке ЭД от Клиента к Банку и обратно.

1.6. Клиент не обязан получать какую-либо дополнительную лицензию государственных органов на право эксплуатации используемых СКЗИ.

1.7. В процессе эксплуатации СКЗИ Клиент обязуется соблюдать лицензионные ограничения разработчика СКЗИ и программных средств для работы с сертификатами ключей проверки ЭП, а также выполнять рекомендации по обеспечению безопасности информации при эксплуатации СКЗИ (раздел 7 настоящего документа).

1.8. Владельцем сертификата ключа проверки ЭП является Клиент - физическое лицо или полномочный представитель Клиента - юридического лица.

1.9. Банк обеспечивает хранение сертификатов ключей проверки ЭП Клиентов в форме электронных документов и возможность получения сертификатов ключей проверки ЭП Клиентов в форме электронных документов в течение всего срока действия упомянутых выше сертификатов.

2. ПОРЯДОК ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТА КЛЮЧА ЭП КЛИЕНТА, ИНОГО АНАЛОГА ЭЛЕКТРОННОЙ ПОДПИСИ

2.1. Для подсистемы Клиент-Банк:

2.2. До начала процедуры генерации ключевой информации Клиент должен оформить Договор о присоединении к системе электронного документооборота и получить (лично или по доверенности) в подразделении Банка ключ транспортного шифрования (приложение № 3) и/или электронный ключевой носитель - USB-токен (приложение № 3) с оформлением акта приема-передачи. Дальнейшие операции Клиент производит на своем рабочем месте.

2.3. Инсталляция СКЗИ и программных средств для работы с сертификатами ключей неквалифицированной ЭП на клиентском рабочем месте (при необходимости) производится Клиентом самостоятельно в соответствии с передаваемой ему документацией либо представителями Банка в соответствии с утвержденными тарифами, а так же инсталляционным программным обеспечением и актом проверки контрольных сумм исполняемых файлов.

2.4. Используя программное обеспечение «Клиент-Банк» и транспортный ключ шифрования, Клиент получает из Банка список лиц, включенных в карточку с образцами подписей и оттиска печати Клиента, предъявленную в Банк, которые могут в полном объеме распоряжаться счетом Клиента. Для осуществления документооборота Клиент – юридическое лицо обязан сформировать как минимум два ключа ЭП, если иное не установлено двусторонним соглашением с Банком. Клиент – индивидуальный предприниматель, лицо, занимающееся частной практикой, физическое лицо может сформировать только один ключ ЭП.

2.5. Клиент может сформировать сертификат ключей проверки ЭП на иное лицо, не включенное в карточку образцов подписей, с целью формирования ЭД и просмотра выписок по счету. В указанном случае владелец ЭП вместе с сертификатом ключей проверки ЭП должен предоставить в Банк доверенность, выданную от имени Клиента на право формирования ЭД и просмотра выписок по счету, копию паспорта, предоставить согласие Банку на обработку его персональных данных.

2.6. В соответствии с руководством пользователя системы «Клиент-Банк» уполномоченный сотрудник Клиента формирует свой личный ключ ЭП, содержащий ключ ЭП и ключ проверки ЭП. Ключ проверки ЭП по защищенному на ключе транспортного шифрования соединению передается в Банк (необходимо произвести сеанс связи с Банком);

2.7. Клиент /(уполномоченное лицо Клиента) распечатывает ключ проверки ЭП на бумажном носителе (в двух экземплярах) в виде Сертификата ключа проверки электронной подписи в системе «Клиент-Банк» (Приложение № 2), который подписывается его владельцем в присутствии сотрудника Банка и регистрируется в Банке. Один экземпляр распечатки Сертификата ключа проверки электронной подписи остается на хранении в Банке, а ее электронный аналог находится в каталоге ключей Банка и Клиента;

2.8. По истечении срока действия Клиент оформляет новый Сертификат в порядке, указанном в п.2.15 настоящего Приложения.

2.9. Сертификат ключа проверки ЭП может быть оформлен в электронном виде. В данном случае Клиент формирует новый Сертификат ключа проверки ЭП, распечатывает его на бумажном носителе, подписывает подписью, которая внесена в карточку образцов подписей, предъявленную в Банк, сканирует его и направляет указанный файл в Банк, подписанный действующим ЭП.

2.10. После завершения процедуры регистрации ключа проверки ЭП Клиента в Банке Клиент должен произвести контрольное соединение с Банком (сеанс связи) и получить из Банка подписанный на ключе расчетного центра Банка сертификат зарегистрированного ключа Клиента. После успешного завершения данной операции Клиент может использовать ключ ЭП для подписи ЭД в системе ЭДО.

2.11. Для подсистемы Интернет-Банк:

2.11.1. До начала процедуры генерации ключевой информации Клиент должен оформить Договор о присоединении к системе электронного документооборота и получить (лично или по доверенности) в подразделении Банка электронный ключевой носитель - USB-токен (приложение № 3) с оформлением акта приема-передачи. Дальнейшие операции Клиент производит на своем рабочем месте.

2.11.2. В процессе предварительной регистрации Клиент самостоятельно создает ключ ЭП неквалифицированной ЭП и парный ему ключ проверки ЭП. Ключ ЭП Клиента формируется и сохраняется на электронном носителе Клиента (токене). Процедура генерации ключа предполагает передачу ключа проверки ЭП по защищенному соединению в Банк и его предварительную регистрацию. Для осуществления документооборота Клиент – юридическое лицо обязан сформировать как минимум два ключа ЭП, если иное не установлено двусторонним соглашением с Банком. Клиент – индивидуальный предприниматель, лицо, занимающееся частной практикой, физическое лицо может сформировать только один ключ ЭП. Клиент может сформировать сертификат ключа проверки ЭП на иное лицо, не включенное в карточку образцов подписей, с целью формирования ЭД и просмотра выписок по счету. В указанном случае владелец ЭП вместе с сертификатом ключа проверки ЭП должен предоставить в Банк доверенность (приложение № 4), выданную от имени Клиента на право формирования ЭД и просмотра выписок по счету, копию паспорта, предоставить согласие Банку на обработку его персональных данных.

2.11.3. Клиент / (уполномоченное лицо Клиента) распечатывает ключ проверки ЭП на бумажном носителе (в двух экземплярах) в виде Сертификата ключа проверки электронной подписи в системе ИБ (Приложение № 2), который подписывается владельцем ЭП в

присутствии сотрудника Банка и регистрируется в Банке. Один экземпляр распечатки Сертификата ключа проверки ЭП подписи остается на хранение в Банке, а ее электронный аналог размещается в каталоге ключей Банка и Клиента.

2.11.4. После успешного завершения регистрации ключа ЭП в Банке Клиент может использовать ключ ЭП для подписи ЭД в системе ЭДО.

2.11.5. В подсистеме Интернет-Банк использование USB-токена является обязательным.

2.12. Для подсистемы Инвест-Бизнес Онлайн:

2.12.1. Клиент должен быть включен в систему Интернет-банк.

2.12.2. Для просмотра счета достаточно заявления (заявление о подключении Инвест-Бизнес Онлайн).

2.12.3. Для управления счетом требуются Ключи серверной подписи.

2.12.4. Клиент из мобильного приложения инициирует процесс генерации ключа.

2.12.5. Клиенту предлагается подтвердить, что его ранее сохраненные в системе паспортные данные актуальны. Клиент подтверждает актуальность или неактуальность паспортных данных.

2.12.6. Клиент в приложении на мобильном устройстве указывает пароль для создаваемого ключа серверной подписи.

2.12.7. На Сервере Подписи генерируются ключ ЭП и ключ проверки ЭП. Ключ ЭП помещается в хранилище на Сервере Подписи.

2.12.8. Мобильное приложение создает документ Заявление на выпуск сертификата ключа проверки серверной ЭП. В документ добавляется самозаверенная заявка на выпуск сертификата ключа проверки серверной подписи. В документ добавляется доверенность от Клиента Банку на хранение и использование ключа серверной подписи. Текст доверенности: «Настоящим доверяем банку хранить ключ ЭП в защищенном хранилище и использовать его для формирования ЭП под документами системы "iBank 2".»

2.12.9. Ответственный сотрудник Клиента подписывает заявление на выпуск сертификата.

2.12.10. При необходимости (при создании первого ключа, при смене паспорта) сотрудник, для которого был создан ключ, совершает визит в Банк, чтобы предоставить документы, удостоверяющие личность.

2.12.11. Ответственный сотрудник Банка проверяет паспортные данные сотрудника Клиента и исполняет документ.

2.13. Для подсистемы «InvestPay»:

2.14. До начала процедуры генерации Ключевой информации Клиент должен присоединиться к системе электронного документооборота путем подписания Заявления и получить аналог собственноручной подписи (простую электронную подпись) - логин (имя пользователя) и первичный пароль для доступа к подсистеме. Логин является постоянным идентификатором Клиента в подсистеме. Первичный пароль направляется Клиенту на указанный в заявлении адрес электронной почты. Первичный пароль Клиент обязан сменить, используя соответствующие функции в подсистеме.

2.14.1. В качестве дополнительных аналогов собственноручной подписи в подсистеме применяются одноразовые коды подтверждения. Одноразовый код может быть направлен в виде SMS-сообщения на телефон, номер которого указан в заявлении Клиента. Кроме того, Клиент может получить OTP-токен для получения одноразовых кодов.

2.14.2. Клиент может использовать в подсистеме ЭП для подписи ЭД. В этом случае сотрудник Банка, обслуживающий Клиента-физическое лицо, создает клиенту временный ключ ЭП. Ключ ЭП Клиента формируется и сохраняется на электронном носителе Клиента (токене). Сотрудник Банка распечатывает сертификат ключа проверки ЭП на бумажном носителе (в двух экземплярах) с указанием срока его действия, передает Клиенту для подписи. Один экземпляр передается Клиенту с целью контроля срока для регистрации основного ключа. В течение срока, указанного в сертификате, Клиент обязан сформировать самостоятельно новый ключ ЭП, направить сформированный сертификат в Банк по каналам связи, подписанный временным ключом, для принятия и регистрации сертификата Банком в системе. При этом временный ключ в течение срока действия сертификата может быть использован для выработки ЭП в соответствии с п. 2.2 Правил.

2.15. В процессе формирования секретный ключ защищается паролем, который является конфиденциальной информацией соответствующей Стороны. Смена пароля на одной копии файла секретных ключей ЭП не приводит к невозможности использования старого пароля на другой, сделанной ранее копии этого же файла секретных ключей ЭП. Исключение составляют ключи, размещенные на электронном токене, для которого изготовление копий секретного ключа невозможно.

2.16. Владельцы ключей ЭП и других аналогов собственноручной подписи несут персональную ответственность за обеспечение сохранности ключевой информации и защиту ключевых носителей от несанкционированного доступа и копирования. Банк не несет ответственности за убытки Клиента, возникшие в результате несанкционированного доступа к ключевой информации.

2.17. При активации ключа проверки ЭП Клиента в Банке производится:

2.18. сверка электронной копии ключа проверки ЭП Клиента, полученного системой, с ключом проверки ЭП, представленным Клиентом в напечатанном виде в Сертификате ключа проверки электронной подписи;

2.19. проверка полномочий лиц на право удаленного распоряжения счетом (просмотра движения денежных средств по счету), на имя которых сформированы ключи.

2.20. Ключ активируется в течение не более 3-х рабочих дней после получения заверенного Клиентом Сертификата ключа проверки ЭП и положительных результатов проверки данных, указанных в п. 2.6. Подписанный уполномоченным сотрудником Банка экземпляр сертификата ключа проверки ЭП передаются Клиенту через операционную группу либо полномочного представителя Клиента по доверенности.

2.21. Клиент устанавливает порядок хранения и использования ключевых носителей с ключами ЭП своих полномочных представителей, а также количество и порядок хранения резервных копий этих ключевых носителей в соответствии с рекомендациями раздела 7 настоящего Приложения.

3. ПОРЯДОК ДЕЙСТВИЙ КЛИЕНТА ПРИ ПРОВЕДЕНИИ ПЛАНОВОЙ ЗАМЕНЫ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ.

3.1. Срок действия ключей ЭП при формировании сертификата ключа проверки ЭП полномочного представителя Клиента устанавливается в Сертификате.

3.2. За месяц до окончания срока действия своих ключей ЭП Клиент должен произвести формирование новых ключей ЭП в соответствии с разделом 2 настоящего Приложения либо в электронном виде. В данном случае Клиент формирует новый Сертификат ключа проверки ЭП, распечатывает его на бумажном носителе, подписывает подписью, которая внесена в карточку образцов подписей, предъявленную в Банк, сканирует его и направляет указанный файл в Банк, подписанный действующим ЭП.

3.3. В подсистеме «Интернет-Банк» единоличный исполнительный орган юридического лица /индивидуальный предприниматель (далее уполномоченный представитель Клиента) могут в электронном виде создать и направить в Банк Заявление на выпуск сертификата ключа проверки ЭП как на себя лично, так и на любое лицо, допущенное к распоряжению счетом и внесенное в карточку с образцами подписей и оттиска печати Клиента. Для этого уполномоченный представитель Клиента инициирует в подсистеме «Интернет-Банк» процесс генерации ключа. Уполномоченный представитель Клиента проверяет актуальность паспортных данных лица, на чье имя будет изготовлен сертификат ключа проверки ЭП. В случае, если данные не актуальны, направляет в Банк копию действующего документа, удостоверяющего личность. По итогам генерации ключа ЭП и ключа проверки ЭП создается документ - Заявление на выпуск

сертификата ключа проверки ЭП (Приложение № 11), который должен быть подписан уполномоченным сотрудником Клиента. Полученное Банком заявление на выпуск ключа проверки ЭП является основанием для выпуска сертификата Ключа на данное лицо и дальнейшего использование сформированного ключа ЭП в подсистеме «Интернет-Банк».

3.4. В подсистеме «Клиент-Банк» Клиент получает сформированный Банком новый сертификат ключа проверки ЭП из сетевого справочника сертификатов ключей проверки ЭП в виде обновления локального справочника сертификатов ключей проверки ЭП. По завершению установки обновления справочника сертификатов Клиент может использовать новый ключ ЭП.

3.5. В подсистемах «Интернет-Банк» и InvestPay сертификаты ключей проверки ЭП хранятся на сервере Банка и доступны сразу после активации.

3.6. Срок действия ключей ЭП Банка устанавливается равным 5-ти годам, срок действия сертификатов ключей проверки электронной подписи – не ограничен.

3.7. За два месяца до окончания срока действия ключей ЭП Расчетного центра Банк формирует новые ключи ЭП и сертификаты ключей проверки ЭП. Новые сертификаты ключей проверки ЭП Расчетного центра Банка размещаются в сетевом справочнике сертификатов проверки ключей электронной подписи для подсистем «Интернет-Банк» и InvestPay и рассылаются в виде обновления справочника локальных сертификатов всем Клиентам подсистемы Клиент-Банк.

4. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

4.1. К событиям, на основании которых принимается решение о компрометации Ключевой информации, относятся, включая, но, не ограничиваясь, следующие:

- информация о несанкционированном доступе к подсистемам;
- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение в СЭД;
- нарушение правил хранения ключевой информации;
- получение информации о смерти владельца Ключевой информации;
- получение информации о передаче Ключевой информации третьим лицам;
- получение информации о нахождении владельца ключа вне места передачи ЭД, заверенных ЭП;
- получения информации о смене постоянно действующего исполнительного органа;
- увольнение сотрудников, имевших доступ к ключевым носителям.

4.2. В случае принятия решения о компрометации Ключевой информации Клиент обязан по телефону сообщить в Банк о факте компрометации и прекратить использование скомпрометированной Ключевой информации.

4.3. В течение одного рабочего дня Клиент обязан направить в Банк письменное уведомление, подписанное руководителем организации и заверенное печатью Клиента, о факте компрометации в письменной форме (Приложение № 6 к Правилам электронного документооборота).

4.4. Клиент может одновременно иметь несколько ключей ЭП и соответствующих им сертификатов ключей проверки ЭП, часть из которых использовать в качестве рабочих, а часть – в качестве резервных на случай компрометации рабочих криптографических ключей. Это обеспечивает Клиенту возможность оперативного перехода на использование резервных криптографических ключей в случае компрометации рабочих криптографических ключей.

4.5. При наличии у Клиента резервных криптографических ключей, он продолжает работу на этих ключах. В случае отсутствия резервных криптографических ключей для системы «Клиент-Банк» Клиент должен обратится в Банк для получения нового ключа транспортного шифрования и сформировать новые ключи ЭП в соответствии с порядком раздела. 2 настоящего Приложения, для системы «Интернет-Банк» Клиент должен сформировать новые ключи ЭП, оформить сертификат ключа проверки ЭП.

4.6. После получения уведомления о компрометации Ключевой информации Банк блокирует применение скомпрометированной Ключевой информации в СЭД.

4.7. Банк может самостоятельно принять решение о компрометации ключевой информации, в случае возникновения события, указанного в п.4.1. настоящего раздела. При фиксировании данного события Банк блокирует ключ Клиента.

5. АННУЛИРОВАНИЕ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ КЛИЕНТА

5.1. Банк аннулирует сертификат ключа проверки ЭП Клиента в следующих случаях:

- по истечении срока его действия;
- в случае прекращения действия договора о присоединении Клиента к электронному документообороту;
- по заявлению в письменной форме владельца сертификата ключа проверки ЭП (полномочного представителя Клиента), подписанного владельцем сертификата ключа проверки ЭП, руководителем организации Клиента и заверенного печатью Клиента (Приложение № 5 к Правилам электронного документооборота) или в случае компрометации ключа (Приложение № 6 к Правилам электронного документооборота);
- в случае исключения уполномоченного лица Клиента из карточки с образцами подписей и оттиска печати;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- получение информации о смерти владельца Ключевой информации;
- получение информации о передаче Ключевой информации третьим лицам;
- получение информации о нахождении владельца ключа вне места передачи ЭД, заверенных ЭП;
- получения информации о смене постоянно действующего исполнительного органа;
- увольнение сотрудников, имевших доступ к ключевым носителям.

5.2. В случае аннулирования сертификата ключа проверки ЭП Клиента Банк блокирует использование соответствующего ключа проверки ЭП в СЭД.

6. ПОРЯДОК ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ РАЗРЕШЕНИИ КОНФЛИКТНЫХ СИТУАЦИЙ

6.1. В случае возникновения конфликтной ситуации при применении ЭП такая ситуация подлежит разрешению в порядке, установленном

Правилами электронного документооборота с учетом особенностей, установленных настоящим Приложением.

6.2. Клиент представляет Банку заявление, содержащее существо претензии с указанием на документ с электронной цифровой подписью, на основании которого Банк выполнил операции по счёту Клиента.

6.3. Банк обязан в течение не более десяти рабочих дней от даты подачи заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии могут быть включены представители Клиента, представители Банка, в качестве экспертов - представители компании-разработчика системы "iBank2" ООО "БИФИТ", при необходимости – другие независимые эксперты. Выбор членов комиссии осуществляется по согласованию со всеми участниками. При невозможности согласованного выбора, последний проводится по жребию.

6.4. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение стороны, несущей ответственность согласно выводу об истинности электронной цифровой подписи Клиента под приложенным документом.

6.5. Разрешительная комиссия в течение не более пяти рабочих дней проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:

- Разрешительная комиссия проводит техническую экспертизу электронного документа, заверенного электронной цифровой подписью Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия с его счетом;
- Разрешительная комиссия проводит техническую экспертизу ключа проверки ЭП Клиента, период действия и статус ключа проверки ЭП Клиента, и установление его принадлежности Клиенту;
- Разрешительная комиссия проводит техническую экспертизу корректности электронной подписи Клиента в электронном документе;
- На основании данных технической экспертизы разрешительная комиссия составляет акт.

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

- Банк не предъявляет электронного документа, переданного Клиентом, на основании которого Банк выполнил операции по счёту Клиента;
- Электронная цифровая подпись Клиента в электронном документе оказалась некорректной;
- Клиент предоставляет Заявление об аннулировании секретного и соответствующего ему ключей проверки ЭП Клиента, подписанное должностным лицом Банка и имеющим оттиск печати Банка. При этом указанная в заявлении дата окончания действия пары ключей ЭП Клиента раньше даты, указанной в рассматриваемом электронном документе;

6.7. В случае, когда Банк предъявляет электронный документ, корректность ЭП Клиента признана разрешительной комиссией, принадлежность Клиенту ключа проверки ЭП Клиента подтверждена, Банк перед Клиентом по выполненным операциям со счётом Клиента ответственности не несёт.

7. РЕКОМЕНДАЦИИ КЛИЕНТУ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИ ПРИ ЭКСПЛУАТАЦИИ СКЗИ.

7.1. Режим эксплуатации СКЗИ устанавливается в соответствии с "Требованиями к средствам криптографической защиты конфиденциальной информации" по уровню "КС1" (система «Интернет-Банк»).

7.2. Рекомендации по организационному обеспечению безопасности СКЗИ:

- в организации Клиента выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ;
- в организации Клиента разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ;
- к работе с СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.

7.3. Рекомендации по размещению СКЗИ и режиму охраны:

- помещения, в которых размещаются технические средства клиентского рабочего места со встроенными СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ;
- размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;
- размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
- входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;
- окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией;
- размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна;
- в режимные помещения допускаются руководители организации Клиента, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов;
- системные блоки компьютеров с СКЗИ оборудуются средствами контроля вскрытия;
- ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ.

7.4. Рекомендации по обеспечению безопасности ключевой информации:

- ключевые носители с ключами ЭП и инсталляционные гибкие магнитные носители с программным обеспечением СКЗИ в организации Клиента берутся на поэкземплярный учет в выделенных для этих целей журналах;
- учет и хранение ключей ЭП поручается руководством организации Клиента специально выделенным сотрудникам;
- для хранения ключевых носителей с ключами ЭП выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
- хранение ключей и инсталляционных гибких магнитных носителей с программным обеспечением СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение;
- рабочие и резервные криптографические ключи хранятся раздельно с обеспечением условия невозможности их одновременной компрометации;
- при транспортировке ключевых носителей с закрытой (секретной) ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

Примечание: Настоящие рекомендации Клиенту определяются условиями лицензирования ФАПСИ деятельности Банка, а также правилами эксплуатации СКЗИ.

8. ОБЯЗАННОСТИ КЛИЕНТА

8.1. С целью исключения возможности хищения персональной и/или ключевой информации третьими лицами, а также несанкционированного доступа третьих лиц к счету и хищения денежных средств Клиент обязан:

- установить актуальное антивирусное программное обеспечение на рабочий компьютер и регулярно обновлять вирусные базы данных;
- исключить возможность разглашения персональной информации инсайдерам (сотрудникам Клиента) путем строгого ограничения доступа к ней: хранения ключевой информации в зашифрованном виде, электронных носителей ключевой информации - в сейфах, организации использования системы контроля доступа к компьютеру, к электронным носителям и т.п.;
- подключиться к услуге по передаче информации о проведенных операциях по расчетному счету с использованием SMS или E-mail - сообщений с обязательным информированием обо всех расходных операциях, совершаемых по счету Клиента (Для подключения к услуге необходимо обратиться к экономисту);
- установить на рабочих местах программное обеспечение, исключающее использование рабочего места Клиента дистанционно третьими неуполномоченными лицами;
- осуществлять информационное взаимодействие с Банком только с использованием средств связи и реквизитов, предусмотренных в договорах с Банком;
- рассмотреть возможность и зафиксировать интернет-адреса, с которых осуществляется доступ к системе удаленного управления счетом, с целью запрета доступа к системе со стороны возможных злоумышленников (Приложение № 7). В случае необходимости обратиться с заявлением к экономисту, обслуживающему счет Клиента;
- при возникновении сомнений в авторстве почтовых сообщений, посланных от лица технической поддержки или иных служб Банка, удалять такие сообщения, ни в коем случае не открывать вложенные в письме материалы и не открывать указанные в письме ресурсы в сети Интернет;
- регулярно обновлять используемое программное обеспечение на рабочем компьютере;
- при подозрении в краже персональной информации, несанкционированном списании денежных со счетов - незамедлительно обращаться в службу технической поддержки Банка (263-16-41) или по телефонам, указанным на сайте Банка http://www.chelinvest.ru/about/phones.html.

8.2. В случае невыполнения Клиентом требований п.8.1 настоящих Правил Банк не несет ответственность за несанкционированное списание денежных средств со счета Клиента (принятия поручения от неуполномоченного лица, в результате которого у клиента возникли убытки), за исключением случаев, когда вина Банка будет доказана.

Приложение № 2
к Правилам электронного документооборота

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭП СОТРУДНИКА КЛИЕНТА
В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
ПАО "ЧЕЛЯБИНВЕСТБАНК"

1. Наименование организации _____
2. Юридический адрес _____
3. ОГРН _____ дата внесения в ЕГРЮЛ (ЕГРИП) "____"_____ года
4. Тел. _____ 5. ИНН _____ 6. КПП _____
7. Факс* _____ 8. E-mail* _____
9. Сведения о владельце ключа
Фамилия, Имя, Отчество _____
Должность _____
Документ, удостоверяющий личность _____ , серия _____
Номер _____ , дата выдачи "____" _____ г.,
кем выдан - _____
10. Примечания* _____
* необязательно для заполнения

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа _____ Идентификатор токена _____
Наименование криптосредств _____
Алгоритм _____
Дата начала действия _____
Дата окончания действия _____
Представление ключа проверки ЭП в шестнадцатеричном виде

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Подтверждаю, что ключ ЭП был сформирован мною лично и является аналогом моей собственноручной подписи.
Личная подпись владельца ключа ЭП

Сертификат ключа проверки ЭП сотрудника действует в рамках договора о присоединении к ЭДО
№___ от "____"_____ 20___ г.

Группа подписи (А/Б)* _____

Достоверность приведенных данных подтверждаю

Уполномоченный представитель банка

_____/_____/
подпись ф.и.о.

Оттиск печати Банка

Дата приема сертификата ключа проверки ЭП
"___"_____200__г.

_____/_____/
подпись ф.и.о.

Дата регистрации сертификата ключа проверки ЭП
"___"_____200__г.

*** Группа А** – это лицо, которое указано в двухстороннем соглашении между Клиентом и Банком в списке А;

- лицо, являющееся единственным распорядителем по счету в соответствии с двусторонним соглашением между Клиентом и Банком;
- индивидуальный предприниматель и/ или лицо, являющееся по двустороннему соглашению с Банком доверенным лицом индивидуального предпринимателя;
- лицо, которое указано первым в карточке образцов подписей, при условии, что в карточке всего два лица, имеющих право подписи.

Группа Б – это лицо которое указано в двустороннем соглашении между Клиентом и Банком в списке Б;

- лицо, которое указано вторым в карточке образцов подписей, при условии, что в карточке всего два лица, имеющих право подписи.

Приложение № 3
к Правилам электронного документооборота

Доверенность № _____

г. _____ _____
(место выдачи) (дата выдачи)

_____, далее – Клиент,
(полное наименование организации)

в лице _____, действующего на
(должность, фамилия, имя, отчество)

основании _____, уполномочивает _____
(должность, фамилия, имя, отчество полномочного представителя)

_____
паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи; телефон для связи,

на получение ключа транспортного шифрования в системе «Клиент-Банк».

Настоящая доверенность действительна до "___" _____ 200__ года.

Подпись (фамилия, инициалы) _____ удостоверяю.
(личная подпись представителя)

Руководитель _____ _____ (инициалы, фамилия)
(наименование должности) (личная подпись)

М.П.

Доверенность № _____

г. _____ _____
(место выдачи) (дата выдачи)

_____, далее – Клиент,
(полное наименование организации)

в лице _____, действующего
(должность, фамилия, имя, отчество)

на основании _____, уполномочивает _____
(должность, фамилия, имя, отчество полномочного представителя)

_____
паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи; телефон для связи,

на получение электронного ключевого носителя (USB-токен).

Настоящая доверенность действительна до "___" _____ 200__ года.

Подпись (фамилия, инициалы) _____ удостоверяю.
(личная подпись представителя)

Руководитель _____ _____ (инициалы, фамилия)
(наименование должности) (личная подпись)

М.П.

Приложение № 4
к Правилам электронного документооборота

Доверенность № _____

г. _____ _____
(место выдачи) (дата выдачи)
_____, далее – Клиент,
(наименование юридического лица)
в лице _____, действующего
(должность, фамилия, имя, отчество)
на основании _____, уполномочивает _____
(должность, фамилия, имя, отчество полномочного представителя)
_____
(паспортные данные: серия, номер, орган, выдавший паспорт, дата выдачи; телефон для связи)
на право:

- просмотра документов и информации о движении денежных средств с использованием систем электронного документооборота ПАО "ЧЕЛЯБИНВЕСТБАНК" (Клиент-Банк, Интернет-Банк), по всем счетам, открытым в ПАО "ЧЕЛЯБИНВЕСТБАНК";
- формирования информации о движении денежных средств по всем счетам на бумажном носителе;
- формирования электронных документов;
- просмотра информации обо всех владельцах ключей ЭП, зарегистрированных в системе электронного документооборота, о сроках действия и их правах данных ключей.

Настоящая доверенность действительна до "____" _____ 20___ года.

Подпись (фамилия, инициалы) _____ удостоверяю.
(личная подпись представителя)

Руководитель _____ _____
(наименование должности)
(личная подпись)

М.П.

Приложение № 5
к Правилам электронного документооборота

(Оформляется на бланке организации)

Администратору

информационной безопасности

ПАО «ЧЕЛЯБИНВЕСТБАНК»

Заявление об аннулировании сертификата ключа проверки электронной подписи

№_____ " ___" _____ 200_ г.

Прошу Вас в соответствии с Правилами электронного документооборота аннулировать сертификат ключа проверки электронной подписи, идентифицируемый перечисленными ниже параметрами:

Серийный номер сертификата ключа проверки электронной подписи	Наименование подразделения банка, выдавшего ключ
	ПАО «ЧЕЛЯБИНВЕСТБАНК»

использовавшийся в

_____
(полное наименование организации Клиента)

владельцем сертификата ключа проверки электронной подписи

_____
(фамилия, имя, отчество полномочного представителя Клиента)

.

Данный сертификат прошу считать аннулированным и выведенным из действия (помещенным в список отозванных сертификатов) с "_____" _____ 200__ г.

Руководитель организации
_____ / Фамилия И.О. /

М.П.

Приложение № 6
к Правилам электронного документооборота

(Оформляется на бланке организации)

Администратору

информационной безопасности

ПАО «ЧЕЛЯБИНВЕСТБАНК»

Уведомление о компрометации криптографических ключей

№_____ " ___" _____ 200_ г.

Настоящим уведомляю о компрометации криптографических ключей, идентифицируемых перечисленными ниже параметрами:

Серийный номер сертификата ключа проверки электронной подписи	Наименование подразделения банка, выдавшего ключ
	ПАО «ЧЕЛЯБИНВЕСТБАНК»

использовавшихся в

_____
(полное наименование организации)

владельцем сертификата ключа проверки электронной подписи

_____
(фамилия, имя, отчество полномочного представителя)

в соответствии с Правилами электронного документооборота.

Данные криптографические ключи прошу считать скомпрометированными и выведенными из действия с даты получения банком настоящего уведомления.

Руководитель организации _____ / Фамилия И.О. /

М.П.

Приложение № 7
к Правилам электронного документооборота

ЗАЯВЛЕНИЕ НА ОГРАНИЧЕНИЕ СПИСКА IP-АДРЕСОВ КЛИЕНТА
(ПОДСИСТЕМА «iBank2»)

Клиент просит Банк с «____»_____200__г. ограничить доступ к системе «iBank2» с помощью принадлежащих ему ключей ЭП и соответствующих им ключей проверки ЭП следующим списком постоянных внешних IP-адресов:

_____
_____
_____
_____
_____

С вышеуказанной даты соединения с любых других IP-адресов считать недействительными и доступ к системе не предоставлять.

Правильность указанных постоянных внешних IP-адресов, подтверждаю

Руководитель Клиента

_____/_____/

М.П.

Отметка банка

Должностное лицо банка

_____/_____/

М.П.

Приложение № 8
к Правилам электронного документооборота

В ПАО «ЧЕЛЯБИНВЕСТБАНК»
от _____
_____
(наименование клиента)

З А Я В Л Е Н И Е
на присоединение КЛИЕНТА к Системе электронного документооборота
АКЦИОНЕРНОГО ЧЕЛЯБИНСКОГО ИНВЕСТИЦИОННОГО БАНКА
«ЧЕЛЯБИНВЕСТБАНК» (ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО)

Прошу присоединить _____
_____
(наименование клиента по Уставу)
к Системе электронного документооборота на следующих условиях:

1. Обмен электронными платежными документами с использованием СЭД может осуществляться по счетам, открытым в ПАО «ЧЕЛЯБИНВЕСТБАНК»:
_____
_____
_____

1. Область действия ключей электронной подписи (сведения об отношениях, при осуществлении которых электронные документы с электронной подписью, сформированной при помощи соответствующих ключей электронной подписи, будут иметь юридическое значение)

Варианты значений для области действия		Отметка о выборе подсистемы
Электронный документооборот «Клиент-Банк»		
Электронный документооборот «Интернет-Банк»		
Электронный документооборот «Инвест-Бизнес Онлайн» (только для Клиентов, подключенных к системе «Интернет-Банк»)		
Должность	ФИО	Номер мобильного телефона
1.		
2.		
3.		

3. Контактное лицо участника СЭД, ответственное за эксплуатацию программного обеспечения:

Фамилия И.О. _____
Телефоны (рабочий, мобильный) _____

4. Программное обеспечение просим установить по адресу (только для «Клиент-Банк):
_____
_____.

«___»_____20___г. Руководитель _____
м.п.

Приложение № 9
к Правилам электронного документооборота

в ПАО «ЧЕЛЯБИНВЕСТБАНК»
от _____
_____
(наименование клиента)

ЗАЯВЛЕНИЕ

о заключении договора об использовании электронного средства платежа
юридическими лицами

1. Настоящим заявляем о заключении с ПАО «ЧЕЛЯБИНВЕСТБАНК» Договора об использовании электронного средства платежа, на условиях, содержащихся в Правилах электронного документооборота, его Приложениях (далее – Правила) и в настоящем заявлении, без каких-либо оговорок, изъятий и ограничений, в связи с чем принимаем на себя в полном объеме права и обязанности, вытекающие из указанных Правил.

2. В целях получения от Банка информации о совершенных операциях с использованием подсистемы СЭД *«Клиент-Банк»/«Интернет-Банк»* (нужное подчеркнуть) просим направлять уведомления о совершенных операциях в указанную подсистему СЭД в виде выписок по счету или отчетов, подтверждающих проведение операций.

3. В целях получения от Банка информации о совершенных операциях с использованием *Корпоративной банковской карты* просим подключить к нижеуказанным услугам информирования и направлять уведомления о совершенных операциях путем направления электронных сообщений (ЭС) одним из следующих способов (или двумя допустимыми способами):

Идентификационные данные	**Способы направления сообщений**	
	SMS	**E-mail**
	Абонентский номер телефона	Адрес электронной почты
_____ номер Карты _____ номер счета	услуга «SMS-информирование по банковской карте» на абонентский номер: +7_____	услуга «E-mail-информирование по банковской карте» на адрес электронной почты: _____@_____

Клиент уведомлен и согласен с тем, что за указанные услуги информирования Банком взимается плата согласно действующим тарифам Банка путем списания денежных средств со счета без распоряжения Клиента. Клиент уведомлен и согласен с тем, что сообщения передаются в открытом виде по каналам общего пользования. Банк не несет ответственности за получение третьими лицами информации, переданной Банком, ставшей им известной в результате несанкционированного подключения к каналам связи или к другим источникам информации. Банк не несет ответственность за неполучение Клиентом сообщения по вине сотового оператора или Провайдера или иных третьих лиц, участвующих в доставке сообщений.

4. Клиент согласен с тем, что стоимость услуг Банка по информированию о совершенных операциях с использованием ЭСП устанавливается в соответствии с утвержденными Банком Тарифами.

5. Клиент подтверждает, что до предоставления Банку настоящего заявления Банк проинформировал Клиента об условиях использования ЭСП, в частности о любых ограничениях способов и мест использования, а также случаях повышенного риска использования ЭСП.

6. Просим направлять SMS-сообщения с одноразовыми паролями для подтверждения операций по ***Корпоративной банковской карте*** в сети Интернет в рамках сервиса ***Verified by Visa**** по следующим реквизитам:

Идентификационные данные	**Абонентский номер телефона**
_____ номер карты _____ номер счета	+7_____
	отказываемся от предоставления Банку абонентского номера телефона
_____ номер карты _____ номер счета	+7_____
	отказываемся от предоставления Банку абонентского номера телефона

* Сервис Verified by Visa – **бесплатный** сервис, обеспечивающий дополнительную безопасность при оплате товаров и услуг через Интернет по Корпоративной банковской карте.

7. После принятия Банком настоящего заявления Клиент просит считать утратившими силу имеющиеся у Банка Реквизиты для информирования о совершенных операциях с использованием ЭСП и реквизиты для направления SMS-сообщений с одноразовыми паролями в рамках сервиса Verified by Visa, указанные в ранее предоставленных заявлениях (если такие заявления Банку предоставлялись).

8. Клиент согласен с порядком вступления в силу Правил электронного документооборота и вносимых в них изменений, а также с порядком уведомления Клиента о внесении изменений в данные Правила, установленные п.п. 1.5 и 1.6 указанных Правил электронного документооборота.

9. С Правилами электронного документооборота ПАО «ЧЕЛЯБИНВЕСТБАНК», включая все их Приложения, размещенными на сайте Банка (www.chelinvest.ru) Клиент ознакомлен и согласен.

«___»_____20___г. Клиент_____
м.п.

Заявление принял:

_____ _____ «___»_____20__г.
(подпись) (Фамилия И.О.) (дата)

М.Ш.

ПОРЯДОК
использования электронных средства платежа
юридическими лицами

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок использования электронных средств платежа (далее - Порядок) устанавливает правила взаимодействия Клиента и Банка по использованию Клиентом электронного средства платежа (далее - ЭСП), регулирует порядок использования Клиентом ЭСП, а также определяет права и обязанности обеих сторон, связанные с использованием Клиентом ЭСП.

1.2. Настоящий Порядок распространяется на Клиентов, предоставивших Банку заявление по форме, установленной Приложением № 9 к настоящим Правилам.

1.3. Для Клиента, не подключенного к СЭД (не имеющего подсистему СЭД «Клиент-Банк» или «Интернет-Банк»), но уже использующего или желающего использовать Корпоративную банковскую карту, настоящие Правила вступают в силу и Клиент допускается (присоединяется) к участию в СЭД на основании Договора об использовании ЭСП, заключаемого Банком и Клиентом в порядке, установленном пунктами 1.5-1.7 настоящего Порядка. Такой Клиент допускается (присоединяется) к участию в СЭД с момента заключения с Банком указанного договора.

1.4. Клиент предоставляет заявление по форме, установленной Приложением № 9 к настоящим Правилам, при каждом подключении к ЭСП того же или иного вида, а также в случае изменений Реквизитов Клиента для направления ему сообщений Банком о совершенных операциях с использованием ЭСП.

1.5. Передача Клиентом Банку заявления по форме, установленной Приложением № 9 к настоящим Правилам, означает принятие Клиентом всех без исключения положений, установленных настоящим Порядком, настоящими Правилами и Приложениями к ним, без каких-либо оговорок и ограничений, и удостоверяет факт заключения между Банком и Клиентом договора об использовании электронного средства платежа (далее – Договор об использовании ЭСП) на условиях, содержащихся в настоящем Порядке, настоящих Правилах и Приложениях к ним, и в тексте заявления (Приложение № 9).

1.6. Клиент, не имеющий ЭСП, считается заключившим с Банком Договор об использовании ЭСП с момента подключения Клиента к соответствующему ЭСП на основании предоставленного Банку заявления по форме, установленной Приложением № 9 к настоящим Правилам.

1.7. Клиент, подключенный к ЭСП до заключения с Банком Договора об использовании ЭСП, считается заключившим Договор об использовании ЭСП со следующего рабочего банковского дня после предоставления Банку заявления по форме, установленной Приложением № 9 к настоящим Правилам.

1.8. До заключения между Клиентом и Банком Договора об использовании ЭСП Банк ознакомил Клиента с условиями использования ЭСП, в частности, уведомил о любых ограничениях способов и мест использования и случаях повышенного риска использования ЭСП.

1.9. Банк вправе отказать Клиенту в заключении Договора об использовании ЭСП путем отказа в подключении (выдаче) ЭСП.

1.10. Все, что не урегулировано настоящим Порядком, настоящими Правилами и Приложениями к ним, регулируется действующим законодательством Российской Федерации.

2. ПОРЯДОК УВЕДОМЛЕНИЯ БАНКА ОБ УТРАТЕ КЛИЕНТОМ ЭСП И (ИЛИ) НЕСАНКЦИОНИРОВАННОМ ИСПОЛЬЗОВАНИИ ЭСП

2.1. Клиент направляет Банку уведомление, предусмотренное п.4.1.1 настоящего Порядка, одним из следующих способов (или всеми способами):

- по телефону № (351) 268-00-88 (круглосуточно);

- путем предоставления заявления Клиентом непосредственно в подразделение Банка (в рабочее время Банка);
- по подсистеме СЭД (системе «Клиент-Банк» или системе «Интернет-Банк» (круглосуточно).

2.2. В случае изменения способов для направления Банку уведомлений Банк уведомляет Клиентов об этом путем внесения изменений в настоящие Правила.

3. ПОРЯДОК УВЕДОМЛЕНИЯ КЛИЕНТА О СОВЕРШЕННЫХ ОПЕРАЦИЯХ

3.1. Банк уведомляет Клиента в максимально короткие сроки об операциях, совершаемых с использованием ЭСП, путем направления сообщений либо выписок по счету или отчетов по реквизитам, указанным Клиентом в заявлении, предоставленном Клиентом по форме, установленной Приложением № 9 к настоящим Правилам (далее Реквизиты Клиента).

3.2. Клиент считается уведомленным о совершенной операции с использованием ЭСП с момента отправки Банком сообщения либо выписки по счету или отчета по Реквизитам Клиента независимо от факта получения/неполучения Клиентом сообщения.

3.3. В случае изменения Реквизитов Клиента Клиент уведомляет об этом Банк путем предоставления заявления по форме, установленной Приложением № 9 к настоящим Правилам.

3.4. Банк не несет ответственность за неполучение Клиентом сообщений по причинам не предоставления последним верных (актуальных) реквизитов, действий третьих лиц, включая, но не ограничиваясь сотовым оператором, провайдером.

4. ОБЯЗАННОСТИ КЛИЕНТА ПО ИСПОЛЬЗОВАНИЮ ЭСП

4.1. **Клиент обязан:**

4.1.1. В случае утраты Клиентом ЭСП и (или) его использования без согласия Клиента, Клиент обязан направить Банку соответствующее уведомление в соответствии с порядком, установленным в разделе 2 настоящего Порядка, незамедлительно после обнаружения факта утраты ЭСП и (или) его использования без согласия Клиента, но не позднее дня, следующего за днем получения от Банка ЭС о совершенной операции.

4.1.2. Выполнять требования и рекомендации по использованию ЭСП, предусмотренные настоящим Порядком, настоящими Правилами и Приложениями к ним.

4.1.3. В случае использования ЭСП без согласия Клиента и хищения денежных средств незамедлительно, при первой возможности, направить в соответствующий орган полиции заявление о преступлении по факту хищения денежных средств с его банковского счета.

4.1.4. Ни при каких обстоятельствах не передавать ЭСП и не сообщать Ключевую информацию третьим лицам.

4.1.5. При использовании Корпоративной банковской карты не сообщать Ключевую информацию третьим лицам, в том числе неуполномоченным сотрудникам Клиента, родственникам, знакомым, работникам Банка и сотрудникам иных кредитных организаций, кассирам и лицам, помогающим Клиенту в использовании Карты.

4.1.6. Хранить Корпоративную банковскую карту и ПИН-код к ней, электронно-ключевой носитель, ПИН- и ПАК-коды к нему отдельно друг от друга в недоступном для третьих лиц месте и обеспечить их безопасное хранение.

4.1.7. Предпринимать меры для предотвращения потери, хищения ЭСП и Ключевой информации и ее несанкционированного использования. Исключать возможность копирования, переписывания Ключевой информации Корпоративной банковской карты при оформлении любых документов (в т.ч. в гостиницах, при оформлении аренды автомобилей, оплате страховых услуг, при совершении любых покупок, депонировании средств и прочих действиях).

4.1.8. Предоставить Банку Реквизиты для направления Клиенту сообщений для информирования о совершаемых операциях.

4.1.9. В случае изменения Реквизитов Клиента своевременно предоставлять их Банку путем предоставления Заявления по форме, установленной в Приложении № 9 к настоящим Правилам.

4.1.10. В целях направления Банку уведомления об утрате Клиентом ЭСП и (или) его использования без согласия Клиента использовать только каналы связи, указанные в разделе 2 настоящего Порядка.

4.1.11. Не отвечать на электронные письма, в которых от имени Банка или других кредитных организаций предлагается предоставить Ключевую информацию, не следовать по «ссылкам», указанным в письмах (включая «ссылки» на сайт Банка), т.к. они могут вести на сайты-двойники в целях хищения денежных средств («фишинг»).

4.1.12. Своевременно проверять сообщения, поступающие от Банка, проверять содержание электронного почтового ящика, используемого для получения от Банка уведомлений, ознакамливаться с содержанием полученных SMS-сообщений и электронных писем.

4.1.13. Внимательно просматривать SMS/E-mail и иные уведомления (сообщения) Банка о проводимых/проведенных операциях, сравнивать сумму и реквизиты получателя средств с информацией, указанной Клиентом при подготовке платежного документа.

4.1.14. Контролировать состояние счета (в том числе путем просмотра выписок по счету).

4.1.15. Контролировать дату и время входа в подсистемы СЭД путем просмотра журнала сеансов работы.

4.1.16. При возникновении сомнений в авторстве почтовых сообщений, посланных от лица технической поддержки или иных служб Банка, удалять такие сообщения, ни в коем случае не открывать вложенные в письме материалы и не открывать указанные в письме ресурсы в сети Интернет.

4.1.17. Выполнять требования и рекомендации по обеспечению безопасности использования ЭСП, в т.ч. информационной, установленные настоящим Порядком, настоящими Правилами и Приложениями к ним.

4.2. **При совершении операций в банкоматах с использованием Корпоративной банковской карты Клиент обязан:**

4.2.1. Проверять на банкоматах наличие посторонних накладок и других элементов, не предусмотренных конструкцией банкомата. Перед использованием банкомата осматривать его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН-Кода и в месте, предназначенном для приема Карты (прорезь). При наличии таких подозрительных устройств необходимо воздержаться от использования банкомата.

4.2.2. Осуществлять операции с использованием банкоматов, установленных в безопасных местах (например, в государственных и муниципальных учреждениях, подразделениях Банка, крупных торговых и сервисных комплексах).

4.2.3. Выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом, если поблизости от банкомата находятся посторонние лица.

4.2.4. Набирать ПИН-Код таким образом, чтобы люди (видеокамеры), находящиеся в непосредственной близости от банкомата, не смогли его увидеть (зафиксировать). При наборе ПИН-Кода прикрывать клавиатуру банкомата любым возможным способом.

4.2.5. После совершения операции в банкомате не забывать извлекать Карту из банкомата.

4.2.6. Не прислушиваться к советам третьих лиц при использовании Карты в банкоматах и терминалах, не принимать их помощь при совершении операций с Картой.

4.2.7. Отказаться от использования банкомата, отменить текущую операцию и дождаться возврата Карты, если банкомат работает некорректно (долгое время находится в режиме ожидания, самовольно перезагружается).

4.2.8. Не применять физическую силу, чтобы вставить Карту в банкомат. Если Карта не вставляется, необходимо воздержаться от использования такого банкомата.

4.3. **При совершении операций по оплате товаров и услуг с использованием Корпоративной банковской карты Клиент обязан:**

4.3.1. Не использовать Карту в организациях торговли и услуг, не вызывающих у Клиента доверия.

4.3.2. Требовать проведения операции с Картой только в своем присутствии. Это необходимо в целях исключения рисков, связанных с неправомерным получением Ключевой информации, указанной на Карте.

4.3.3. Убедиться в том, что люди, находящиеся в непосредственной близости при оплате товаров (услуг) с использованием Карты, не смогут увидеть данные, нанесенные на Карту, и информацию с чека, предоставленного организацией торговли (услуг) в подтверждение совершенной операции.

4.3.4. Не использовать ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

4.3.5. Не указывать Ключевую информацию (номер и срок действия Карты, код CVC2/CVV2, ПИН-Код) в документах, оформляемых при оплате товаров и услуг (в магазинах, в гостиницах, по телефону/факсу и т.д.).

4.3.6. Пользоваться Интернет-сайтами только известных и проверенных организаций торговли и услуг.

4.3.7. Убеждаться в правильности используемых для совершения покупок адресов Интернет-сайтов, т.к. похожие адреса могут использоваться для осуществления неправомерных действий («фишинг»).

4.3.8. Подключить к Корпоративной банковской карте платежной системы Visa International сервис Verified by Visa и для совершения операций в сети Интернет пользоваться только интернет-сайтами предприятий, поддерживающими сервис Verified by Visa (на интернет-сайте должен присутствовать логотип Verified by Visa). В момент совершения операции в сети Интернет одноразовый пароль, полученный в SMS-сообщении в рамках сервиса Verified by Visa, необходимо вводить только в случае согласия с операцией, реквизиты которой получены в SMS-сообщении вместе с одноразовым паролем.

4.3.9. Ни при каких обстоятельствах не сообщать третьим лицам одноразовый пароль, полученный в SMS-сообщении в рамках сервиса Verified by Visa.

4.3.10. Совершать покупки только со своего компьютера в целях сохранения конфиденциальности Ключевой информации и (или) информации о счете и Карте Клиента.

4.3.11. Установить актуальное антивирусное программное обеспечение на рабочий компьютер и регулярно обновлять его в целях снижения рисков от проникновения вредоносного программного обеспечения, снижения рисков хищения Ключевой и персональной информации.

5. ОБЯЗАННОСТИ БАНКА ПРИ ИСПОЛЬЗОВАНИИ КЛИЕНТОМ ЭСП

5.1. **Банк обязан:**

5.1.1. Информировать Клиента о каждой совершенной с использованием ЭСП операции при условии предоставления Клиентом Реквизитов для связи с ним. Данная информация предоставляется путем предоставления Банку заявления по форме, установленной Приложением № 9 к настоящим Правилам.

5.1.2. Фиксировать направленные Клиенту сообщения о совершенных с использованием ЭСП операциях, а также полученные от Клиента уведомления об утрате ЭСП и (или) его использовании без согласия Клиента, а также хранить соответствующую информацию не менее 3-х лет.

5.1.3. Обеспечить возможность направления Клиентом уведомления об утрате ЭСП и (или) о его использовании без согласия Клиента по каналам связи, указанным в разделе 2 настоящего Порядка.

5.1.4. Приостанавливать или прекращать (блокировать) использование Клиентом ЭСП на основании полученного от Клиента уведомления об утрате ЭСП и (или) его использовании без согласия Клиента.

5.1.5. Рассматривать заявления Клиента, в т.ч. при возникновении споров, связанных с использованием Клиентом его ЭСП, а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в т.ч. в письменной форме по требованию Клиента, не позднее 30 дней со дня получения Банком таких заявлений или не позднее 60 дней со дня получения заявлений в случае использования ЭСП для осуществления трансграничного перевода денежных средств.

6. ПРАВА КЛИЕНТА

6.1. **Клиент имеет право:**

6.1.1. Получать информацию о совершенных с использованием ЭСП операциях на условиях, установленных настоящим Порядком.

6.1.2. Получать от Банка консультации по вопросам использования ЭСП, а также информацию о способах и механизмах защиты Ключевой информации.

6.1.3. Обращаться в Банк для отключения (блокирования) ЭСП.

6.1.4. Осуществлять иные права, возникающие в соответствии с настоящим Порядком.

6.1.5. Расторгнуть договор об использовании ЭСП (отказаться от исполнения от настоящего Порядка), предоставив Банку соответствующее заявление. Такой договор считается расторгнутым с момента отключения Банком Клиента от ЭСП.

7. ПРАВА БАНКА

7.1. **Банк имеет право:**

7.1.1. В одностороннем порядке приостанавливать или прекращать (блокировать) использование Клиентом его ЭСП в случае нарушения Клиентом настоящего Порядка.

7.1.2. В одностороннем порядке устанавливать и изменять лимиты по сумме, по количеству операций за определенный период (при использовании Клиентом Корпоративной банковской карты), а также реализовывать иные механизмы и способы, снижающие риски Банка и Клиента.

7.1.3. Списывать со счета Клиента сумму комиссии за направление Банком Клиенту сообщений о совершенных операциях с использованием ЭСП, в размере и в порядке, установленными Тарифами Банка.

7.1.4. В одностороннем порядке приостанавливать работу (отключать, блокировать) ЭСП при выявлении фактов и признаков несанкционированного использования ЭСП, а также в случае наличия у Банка подозрений в несанкционированном использовании Ключевой информации.

7.1.5. Осуществлять запись телефонного разговора между Клиентом и Банком при поступлении от Клиента по телефону уведомления об утрате ЭСП и (или) его несанкционированном использовании.

8. ОТВЕТСТВЕННОСТЬ БАНКА, ОСВОБОЖДЕНИЕ БАНКА ОТ ОТВЕТСТВЕННОСТИ

8.1. **Банк несет ответственность за совершенные без согласия Клиента операции с использованием ЭСП, если:**

8.1.1. Клиент предоставил Банку заявление по форме, установленной Приложением № 9 настоящих Правил и надлежащим образом исполнял все предусмотренные настоящим Порядком и Правилами требования и рекомендации. Ответственность Банка в этом случае ограничивается возмещением суммы операции, совершенной без согласия Клиента. При этом обязанность Банка по возмещению суммы операции, совершенной без согласия Клиента, возникает только после предъявления Клиентом Банку надлежащим образом заверенной копии постановления компетентного органа об окончании предварительного расследования уголовного дела, возбужденного по факту хищения денежных средств Клиента, либо постановления о приостановлении производства по уголовному делу, либо постановления о прекращении уголовного дела, либо постановления об отказе в возбуждении уголовного дела, свидетельствующего об отсутствии со стороны Клиента действий, направленных на неисполнение либо ненадлежащее исполнение Клиентом обязанностей, установленных настоящим Порядком и Правилами.

8.2. **Банк освобождается от ответственности в случае использования ЭСП без согласия Клиента, если:**

8.2.1. Клиент не предоставил Банку Реквизиты для связи с ним для целей направления Банком сообщений о совершенных с использованием ЭСП операциях (заявление по форме, установленной Приложением № 9 к настоящим Правилам).

8.2.2. В случае изменения Реквизитов Клиента Клиент своевременно не предоставил их Банку для обеспечения своевременного направления Банком Клиенту сообщений о совершенных операциях с использованием ЭСП.

8.2.3. Клиент не выполнял или ненадлежащим образом выполнял требования и рекомендации по обеспечению безопасности использования ЭСП, в т.ч. информационной, установленные настоящим Порядком, настоящими Правилами и Приложениями к ним.

8.2.4. Клиент не исполнил или ненадлежащим образом исполнил обязанность по направлению Банку уведомления об утрате ЭСП и (или) его использовании без согласия Клиента.

8.2.5. Если у Клиента не работал по каким-либо причинам канал связи для направления ему сообщения о совершенной с использованием ЭСП операции (выключен компьютер, не работал телефон, не было при себе телефона, нахождение Клиента вне зоны доступа сети оператора связи или сети Интернет, не было доступа к электронной почте или она не работала и т.д.), что повлекло неполучение от Банка сообщения о совершенной операции с использованием ЭСП.

8.3. Банк не несет ответственность за невозможность использования Клиентом ЭСП, а также невозможность своевременной доставки Клиенту отправленного Банком сообщения о совершенной операции с использованием ЭСП, в ситуациях, находящихся вне его контроля и связанных со сбоями в работе внешних систем, в случае отказов в приеме Карты со стороны торговых или сервисных предприятий, в случае некачественной работы сотовых операторов и Интернет-провайдеров, а также за ошибки, произошедшие по вине Клиента или третьих лиц.

Банку ПАО "ЧЕЛЯБИНВЕСТБАНК", г.ЧЕЛЯБИНСК

от клиента _____

Просим выпустить сертификат проверки ключа ЭП в соответствии с идентификационными данными:

1. Сведения об организации		
1.1	**Наименование организации**	
1.2	**Место нахождения**	
1.3	**ОГРН**	
1.4	**Дата внесения в ЕГРЮЛ (ЕГРИП)**	
1.5	**ИНН (КИО)**	
1.6	**КПП**	
1.7	**Телефон**	
2. Сведения о владельце ключа		
2.1	**ФИО**	
2.2	**Должность**	
2.3	**Документ, удостоверяющий личность**	
2.4	**Серия**	
2.5	**Номер**	
2.6	**Дата выдачи**	
2.7	**Кем выдан**	
2.8	**Код подразделения**	
3. Сведения о ключе проверки ЭП		
3.1	**Идентификатор**	
3.2	**Наименование**	
3.3	**Алгоритм**	
3.4	**ID набора параметров алгоритма**	
3.5	**Представление ключа проверки ЭП**	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Настоящим доверяем банку хранить ключ ЭП в защищенном хранилище и использовать его для формирования ЭП под документами системы "iBank 2".

_____ Дата создания ключа ЭП: _____

_____

Доставлено по системе "iBank 2" 00.00.0000 00:00 ЭП ПОДЛИННА	
ID документа:	
	ID ключа проверки ЭП:
Распечатано 00.00.0000 00:00	