УТВЕРЖДАЮ:

Директор ЗАО «ЦЦС»

_____

(Гудков А.В.)

«21» сентября 2021 г.

ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «BeSafe»

Правила вступают в силу с «05» октября 2021 г.

ОБЩИЕ ПОЛОЖЕНИЯ

1. Цели и сфера деятельности Системы

Система «BeSafe» - корпоративная информационная система, организованная Закрытым акционерным обществом «Центр Цифровых Сертификатов» ИНН 5407187087 (далее – «*Оператор*») для обеспечения договорных и технологических условий формирования и развития финансового и информационного электронного обслуживания, предоставляемого *Оператором* и *Организаторами сервисов Клиентам*.

Участником Системы «BeSafe» может быть только ограниченный круг лиц, присоединившихся к *Системе «BeSafe»* и Правилам электронного документооборота корпоративной информационной *Системы «BeSafe»* (далее – «Правила») в соответствии с порядком, установленным Правилами (Статья 4 Правил). Присоединение возможно только в случае, если *Участник* полностью согласен с Правилами и условиями присоединения к *Системе «BeSafe»*, удовлетворяет содержащимся в Правилах критериям.

Обратившемуся лицу может быть отказано в присоединении с направлением соответствующего уведомления, без указания причин отказа.

2. Термины и определения

Система «BeSafe» (далее - «Система») – корпоративная информационная система, представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот в соответствии с настоящими Правилами.

Участник *(Участник Электронного документооборота,* Участник *ЭДО*) – *Оператор, Организатор сервиса, Удостоверяющий центр* или *Клиент* в соответствии с настоящими Правилами.

Электронный документооборот (ЭДО) – обмен *Электронными документами* и *Простыми электронными документами* в *Системе* в соответствии с настоящими Правилами.

Оператор – владелец *Системы*.

Клиент – физическое лицо (в том числе индивидуальный предприниматель) или юридическое лицо, присоединившееся к *Системе* в соответствии с порядком, установленном Правилами.

Сервис – часть *Системы*, предназначенная для финансового и/или информационного электронного обслуживания *Организатором сервиса Клиентов*.

Организатор сервиса – юридическое лицо или индивидуальный предприниматель, заключившие с *Оператором* или уполномоченным лицом *Оператора* договор о присоединении в качестве *Организатора сервиса* и осуществляющие в рамках *Системы* функции финансового и/или информационного электронного обслуживания *Клиентов*, участвующих в работе *Сервиса Организатора сервиса*. *Организатор сервиса* может осуществлять привлечение *Клиентов* к работе в *Системе* и в *Сервисе*, а также производить присоединение их к *Системе* и *Регистрацию* в *Сервисе.*

Удостоверяющий центр (УЦ) – юридическое лицо, заключившее с *Оператором* соответствующий договор и осуществляющее изготовление *Сертификатов Участников*. *Удостоверяющий центр* или уполномоченные им представители (*Агенты*) осуществляют проверку *Клиентов* и других *Участников*, необходимую для создания *Сертификатов Участников*. *Удостоверяющий центр* в рамках своей деятельности осуществляет привлечение *Агентов* и заключает с ними договор, соглашение о присоединении к настоящим Правилам.

Агент – уполномоченный представитель *Удостоверяющего центра*, заключивший с *Удостоверяющим центром* договор, в соответствии с которым *Агент* осуществляет от имени *Удостоверяющего центра* проверку *Клиентов*, документов *Клиентов*, предшествующую изготовлению *Удостоверяющим центром Сертификатов*, а также направляет *Удостоверяющему центру* запросы на изготовление *Сертификатов* и передаёт *Клиентам Сертификаты*, изготовленные *Удостоверяющим центром*.

Администратор безопасности – должностное лицо *Организатора сервиса*, которое отвечает за управление *Сертификатами Участников* в рамках *Сервиса*, а также за назначение прав и полномочий доступа к данным и совершения операций *Участников* и их уполномоченных лиц в рамках *Сервиса*.

Ключ электронной подписи (Ключ ЭП, Закрытый / Секретный ключ) - последовательность символов, известная *Владельцу сертификата* и предназначенная для создания в *Электронных документах Электронной подписи* с использованием *Средств электронной подписи*, а также расшифровывания *Электронных сообщений*.

Ключ проверки электронной подписи (Ключ проверки ЭП, Открытый ключ) - последовательность символов, соответствующая *Ключу электронной подписи*, предназначенная для подтверждения (проверки) с использованием *Средств электронной подписи* подлинности *Электронной подписи* в *Электронном документе*, а также зашифровывания *Электронных сообщений*, предназначенных владельцу *Ключа электронной подписи*.

Сертификат ключа проверки электронной подписи (Сертификат, Сертификат ключа проверки ЭП, Сертификат ключа электронной подписи) – *Электронный документ* или документ на бумажном носителе с *Электронной подписью Удостоверяющего центра*, доступный любому *Участнику*, включающий в себя *Ключ проверки электронной подписи Владельца сертификата*. *Сертификаты ключей проверки электронной подписи* выдаются *Удостоверяющим центром Участнику* для подтверждения подлинности *Электронной подписи* и идентификации *Владельца сертификата*, а также для обеспечения возможности шифрования предназначенных владельцу *Ключа электронной подписи Электронных сообщений*. *Сертификат ключа проверки электронной подписи* уникален в рамках выдавшего его *Удостоверяющего центра*.

Владелец сертификата ключа проверки электронной подписи (Владелец сертификата, Владелец сертификата ключа проверки ЭП) – физическое, либо юридическое лицо, которому *Удостоверяющим центром* выдан *Сертификат ключа проверки электронной подписи* и которое владеет соответствующим *Ключом электронной подписи*, позволяющим с помощью *Средств криптографической защиты информации* создавать *Электронную подпись* в *Электронных документах* (подписывать *Электронные документы*), а также расшифровывать *Электронные сообщения*.

Идентификатор владельца сертификата ключа проверки электронной подписи (Идентификатор владельца сертификата) – идентификационные данные *Владельца сертификата ключа проверки электронной подписи*, которые входят в состав *Сертификата ключа проверки электронной подписи*. *Идентификатор владельца сертификата ключа проверки электронной подписи* позволяет отличать и однозначно идентифицировать *Владельца сертификата ключа проверки электронной подписи* в рамках *Системы*. *Идентификаторы владельцев сертификатов* одного *Класса сертификата ключа проверки электронной подписи*, принадлежащие разным *Владельцам сертификатов ключей проверки электронной подписи*, уникальны в рамках выдавшего *Сертификаты Удостоверяющего центра*. Уникальность *Идентификаторов владельцев сертификатов* одного *Класса сертификата ключа проверки электронной подписи*, принадлежащих разным *Владельцам сертификатов ключей проверки электронной подписи*, обеспечена технологическими средствами *Удостоверяющего центра* при условии, что *Владелец сертификата ключа проверки электронной подписи* не допустил *Компрометации* собственных *Ключей электронной подписи*.

Электронное сообщение (ЭС) – логически целостная совокупность структурированных данных, имеющих смысл для участников информационного взаимодействия. Информация в *Электронном сообщении* представлена в электронно-цифровой форме, позволяющей обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.

Электронный документ (ЭД) – *Электронное сообщение*, заверенное *Электронной подписью*, в котором информация представлена в электронно-цифровой форме и соответствует установленному

Оператором или *Организатором сервиса* формату. *Электронный документ* может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

Простой электронный документ (Простой ЭД) – *Электронное сообщение*, заверенное *Простой электронной подписью* либо *Аналогом собственноручной подписи*, в котором информация представлена в электронно-цифровой форме и соответствует установленному *Организатором сервиса* формату. *Простой электронный документ* может быть преобразован в форму, пригодную для однозначного восприятия его содержания.

***Формат электронного документа/Простого электронного документа* (*Формат ЭД/Простого ЭД*)** – структура содержательной части *Электронного сообщения*, на основе которого сформирован *Электронный документ/Простой электронный документ*.

Отправитель электронного документа/Простого электронного документа (Отправитель ЭД/Простого ЭД) – *Участник*, который направляет *Электронный документ/Простой электронный документ* с использованием *Системы*.

Получатель электронного документа/Простого электронного документа (Получатель ЭД/Простого ЭД) – *Участник*, которому *Электронный документ/Простой электронный документ* отправлен с использованием *Системы*.

Доставка электронного документа/Простого электронного документа (Доставка ЭД/Простого ЭД) – процесс пересылки *Электронного документа/Простого электронного документа* от *Отправителя электронного документа/Простого электронного документа* к *Получателю электронного документа/Простого электронного документа*.

Криптографические ключи – общее название *Ключей электронной подписи и Ключей проверки электронной подписи*.

Ключевой носитель – информационный (материальный) носитель, на который записаны *Криптографические ключи*.

Усиленная неквалифицированная электронная подпись (Электронная подпись, ЭП, Электронная цифровая подпись, ЭЦП) – реквизит *Электронного документа*, предназначенный для защиты *Электронного документа* от подделки, полученный в результате криптографического преобразования информации с использованием *Ключа электронной подписи* и позволяющий идентифицировать *Владельца сертификата ключа проверки электронной подписи*, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в *Электронном документе* информации.

Подтверждение подлинности Электронной подписи в Электронном документе (проверка ЭП документа) - положительный результат проверки принадлежности *Электронной подписи* в *Электронном документе Участнику* и отсутствия искажений в данном *Электронном документе*. Подтверждение подлинности *Электронной подписи* должно осуществляться соответствующим средством *Электронной подписи* с использованием *Сертификата ключа проверки электронной подписи*.

Аналог собственноручной подписи (АСП) - персональный идентификатор *Участника,* являющийся контрольным параметром правильности составления всех обязательных реквизитов *Простого электронного документа* и неизменности их содержания, который удостоверяет факт составления и подписания *Простого электронного документа* от имени *Участника*, а также подлинность платежного документа, включая все его обязательные реквизиты. *Аналог собственноручной подписи* может быть использован *Участниками* – юридическими лицами и индивидуальными предпринимателями для подписания *Простых электронных документов*.

***Простая электронная подпись* (*Простая ЭП*)** – реквизит *Простого электронного документа*, предназначенный для защиты *Простого электронного документа* от подделки, посредством использования кодов, паролей или иных средств позволяет подтвердить факт формирования электронной подписи определенным лицом, а также установить отсутствие утраты, добавления, перестановки или искажения содержащейся в *Простом электронном документе* информации.

Регистрация – процедура, определенная правилами *Сервиса* и осуществляемая уполномоченным на то *Участником,* позволяющая *Клиенту* использовать *Сервис* для осуществления обмена *Простыми электронными документами*.

***Технология простой электронной подписи/аналога собственноручной подписи* (*Технология*)** – набор процедур, определенных *Организатором сервиса* и регламентирующих работу с *Простой электронной подписью/Аналогом собственноручной подписи*, включая, но не ограничиваясь: создание и проверку *Простой электронной подписи/Аналога собственноручной подписи*, *Регистрацию* в *Сервисе*.

Средства простой электронной подписи/аналога собственноручной подписи (Средства простой ЭП/АСП) – материально-технические средства и информация, принадлежащие Клиенту и

необходимые для создания *Простой электронной подписи/Аналога собственноручной подписи* согласно *Технологии простой электронной подписи/аналога собственноручной подписи* определенной *Сервисом*.

Средства электронной подписи (Средства ЭП) - аппаратные и(или) программные средства, являющиеся частью *Средств криптографической защиты информации* и реализующие хотя бы одну из следующих функций при организации *Электронного документооборота*: создание *Электронной подписи* в *Электронном документе* с использованием *Ключа электронной подписи*; подтверждение подлинности *Электронной подписи*, содержащейся в *Электронном документе*, с использованием *Ключа проверки электронной подписи*; создание *Ключей электронной подписи* и *Ключей проверки электронной подписи*.

Средства криптографической защиты информации (СКЗИ) – аппаратные и(или) программные средства, обеспечивающие применение *Электронной подписи* и *Шифрования* при организации *Электронного документооборота*. *Средства криптографической защиты информации* могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение. В *Системе* допускается использование только *Средств криптографической защиты информации*, разрешённых к использованию в *Системе* (сертифицированных) *Оператором*.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного *Электронного сообщения*.

Класс сертификата ключа проверки электронной подписи (Класс) – атрибут *Сертификата ключа проверки электронной подписи*, характеризующий процедуру проверки, которую прошёл *Владелец сертификата ключа проверки электронной подписи* при создании *Сертификата ключа проверки электронной подписи*.

Создание сертификата – осуществляемая *Удостоверяющим центром* процедура изготовления, выдачи и занесения в реестр *Сертификата ключа проверки электронной подписи*.

Регистрация сертификата ключа проверки электронной подписи (Регистрация сертификата) – осуществляемая *Организатором сервиса* процедура регистрации *Идентификатора владельца сертификата ключа проверки электронной подписи*, которая производится при условии предоставления *Владельцем сертификата ключа проверки электронной подписи* своего *Сертификата ключа проверки электронной подписи*, и, при необходимости, доказательств, подтверждающих факт принадлежности этого *Сертификата ключа проверки электронной подписи Владельцу сертификата ключа проверки электронной подписи*, доказательств, подтверждающих его права на осуществление действий в рамках *Системы, Сервиса*, определяемых условиями регистрации.

Компрометация ключа электронной подписи (***Компрометация ключа ЭП***) – нарушение конфиденциальности *Ключа электронной подписи*, констатация *Владельцем сертификата ключа проверки электронной подписи* обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование *Ключа электронной подписи* неуполномоченными лицами.

Компрометация средств простой ЭП/АСП – нарушение конфиденциальности *Средств простой электронной подписи/Аналога собственноручной подписи*, констатация их владельцем обстоятельств, или наступление обстоятельств, при которых возможно несанкционированное использование *Средств простой электронной подписи/Аналога собственноручной подписи* неуполномоченными лицами.

Уполномоченное лицо участника – сотрудник или иной представитель *Участника*, действующий от его имени на основании устава, договора, доверенности на право совершения соответствующих операций.

Программное обеспечение Сервиса (далее – «ПО Сервиса») – программное обеспечение, необходимое для обеспечения работоспособности Сервиса, устанавливаемое на стороне Организатора Сервиса, Агента, либо Клиента.

3. Предмет регулирования настоящих Правил

3.1. Настоящие Правила, а также Приложения к настоящим Правилам устанавливают общие принципы осуществления информационного взаимодействия с использованием *ЭДО* между *Участниками*. Требования к оформлению и содержанию *ЭД/Простых ЭД,* их форматы и реквизиты, особенности порядка их обработки, исполнения и хранения определяются настоящими Правилами, а также дополнительными договорами, заключаемыми между *Участниками,* и правилами *Организаторов сервисов*. Требования дополнительных договоров, заключаемых между *Участниками*, а также правила *Организаторов сервисов* не должны противоречить принципам, установленным в настоящих Правилах.

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

3.3. Настоящие Правила не регулируют вопросы обмена *ЭС*, не являющимися *ЭД/Простыми ЭД* в соответствии с настоящими Правилами.

4. Порядок присоединения к Системе Участников, вступления в действие настоящих Правил, а также внесения в них изменений

4.1. Настоящие Правила, включая все Приложения к ним, утверждаются *Оператором*. Изменения в настоящие Правила вносятся *Оператором* в одностороннем порядке.

4.2. Настоящие Правила вступают в силу в отношении *Клиента* с момента заключения им с *Организатором сервиса/*Уполномоченным лицом *Организатора сервиса* Соглашения о присоединении в соответствии с типовой формой, содержащейся в Приложении №1 к настоящим Правилам (либо в ином виде, определяемом *Организатором Сервиса*, не противоречащем настоящим Правилам), либо на основании Заявления на выдачу *Сертификата,* поданного *Клиентом Агенту, УЦ* (Формы Заявлений изложены в «Правилах работы Удостоверяющего центра «AUTHORITY»», которые размещены в сети Интернет по адресу www.authority.ru, либо в «Правилах работы Центра Цифровых Сертификатов «BeSafe.ru», размещенных в сети Интернет по адресу www.besafe.ru), либо с момента *Регистрации Клиента* в *Сервисе*, при условии успешной проверки данных *Клиента*. Правила распространяются на *Клиента*, *Организатора сервиса*, иных *Участников* только в рамках данного *Сервиса.*

4.3. Настоящие Правила вступают в силу в отношении *УЦ* с момента заключения договора между *УЦ* и *Оператором*.

4.4. Настоящие Правила вступают в силу в отношении *Агента УЦ* с момента заключения им договора с *УЦ,* соглашения о присоединении к настоящим Правилам. Правила действуют в отношении *Агента УЦ* в течение всего срока действия договора с *УЦ*.

4.5. Настоящие Правила вступают в силу в отношении *Организатора сервиса* с момента заключения им с *Оператором* или уполномоченным лицом *Оператора* договора о присоединении к *Системе* в качестве *Организатора сервиса*, либо договора, согласно которому *Организатор сервиса* присоединяется к настоящим Правилам. Правила действуют в отношении *Организатора сервиса* в течение всего срока действия договора о присоединении к *Системе* в качестве *Организатора сервиса*.

4.6. Присоединяясь к настоящим Правилам, *Участник* принимает их условия целиком в порядке, предусмотренном ст.428 ГК РФ и обязуется их выполнять, а также признаёт, что получение *ЭД/Простого ЭД*, заверенного в соответствии с настоящими Правилами *ЭП/Простой ЭП или АСП Участника*, *УЦ,* юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями *Участника*/уполномоченных лиц *Участника*, *УЦ* и оттиском печати *(только для ЭП и АСП) Участника*, *УЦ*. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что *Ключ ЭП*, *ЭП, Простая ЭП, АСП* и *Сертификат Участника, УЦ* созданы с использованием технологии *Системы*.

5. Порядок уведомления о внесении изменений в настоящие Правила

5.1. Текст изменений настоящих Правил и Приложений к ним доводится *Оператором* до сведения *Участников* посредством уведомления не позднее, чем за 14 (Четырнадцать) календарных дней до даты вступления в силу таких изменений. Уведомление осуществляется путем размещения соответствующей информации в информационной части *Системы* в сети Интернет по адресу www.besafe.ru.

5.2. Настоящие Правила располагаются в информационной части *Системы* в сети Интернет по адресу www.besafe.ru.

5.3. Тексты настоящих Правил и всех изменений и дополнений к ним на бумажном носителе должны храниться *Оператором* в течение 5 (Пяти) лет после прекращения их действия.

5.4. Участник имеет право запрашивать копии текстов настоящих Правил и всех изменений и дополнений к ним на бумажном носителе. Указанные в настоящем пункте документы должны быть направлены *Участнику* в течение 15 (Пятнадцати) рабочих дней после получения соответствующего запроса *Участника* и оплаты всех накладных расходов *Оператора*, связанных с изготовлением и отправкой копий Правил.

6. Регулирование электронного документооборота

6.1. *ЭДО* в *Системе* и в рамках *Сервисов* регулируется следующими документами:

– настоящими Правилами;

– соглашениями о присоединении;

– правилами *Организаторов сервисов* и приложениями к ним;

– дополнительными договорами, заключаемыми между *Участниками*.

6.2. Порядок осуществления *ЭДО* в рамках *Сервиса* разрабатывается и принимается *Организатором сервиса* самостоятельно в соответствии с принципами, установленными настоящими Правилами. В случае если порядок, разработанный *Организатором сервиса*, не соответствует настоящим Правилам, *Организатор сервиса* обязан устранить имеющиеся несоответствия в течение 3(Трех) месяцев.

6.3. Правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Участниками*, могут определяться:

– порядок регистрации *Сертификата* в *Сервисе*;

– порядок *Регистрации Клиента* в *Сервисе*;

– дополнительные условия присоединения к *Правилам*;

– перечень и форматы передаваемых *ЭД, Простых ЭД*, регламент информационного взаимодействия, порядок учета *ЭД, Простых ЭД*, порядок формирования подтверждений о получении *ЭД, Простых ЭД*, порядок хранения *ЭД, Простых ЭД* и другие особенности документооборота, связанные с обслуживанием *Участников*;

– порядок и особенности организации технического доступа к *Сервисам*;

– иные условия по усмотрению *Организатора сервиса*.

7. Порядок и условия допуска Организаторов сервисов и Клиентов к осуществлению документооборота в Системе

7.1. *Организатор сервиса* допускается к осуществлению документооборота средствами *Системы* в рамках *Сервиса* после выполнения им всей совокупности следующих действий и условий:

– заключения договора о присоединении в качестве *Организатора сервиса*;

– установки необходимых аппаратных средств, программного обеспечения;

– получения *Ключа ЭП* и *Ключа проверки ЭП Организатора сервиса;*

– создания *Сертификата Организатора сервиса Удостоверяющим центром*;

– обеспечения совместимости *СКЗИ*, используемых *Организатором сервиса* с *СКЗИ*, используемыми *Оператором* в случае необходимости осуществления *ЭДО* с *Оператором*;

– утверждения *Оператором* правил работы *Сервиса*, оформленных в виде отдельного документа или части договора, заключаемого между *Участниками*.

7.2. *Клиент* допускается к осуществлению документооборота средствами *Системы*, а также в рамках *Сервиса* после выполнения им всей совокупности следующих действий и условий:

– присоединения к *Системе «BeSafe»* и Правилам в соответствии с порядком, установленном Правилами (Статья 4 Правил);

– установки необходимых аппаратных средств, программного и информационного обеспечения;

– а также либо:

– получения *Ключа ЭП* и *Ключа проверки ЭП;*

– создания *Сертификата Удостоверяющим центром*;

– регистрации *Сертификата Организатором сервиса* (для каждого *Сервиса*), включая регистрацию *Идентификатора владельца сертификата*, а также (при необходимости) получения необходимых идентификаторов и паролей для доступа к *Сервису*;

– обеспечения совместимости используемых *Клиентом СКЗИ*, с *СКЗИ*, используемыми другими *Участниками*, с которыми *Клиент* осуществляет документооборот в *Системе* и в рамках *Сервиса*.

– либо:

– *Регистрации.*

В ходе *Регистрации Участник*, уполномоченный на проведение *Регистрации,* производит проверку документов и полномочий *Клиента* и/или должностных лиц *Клиента* в объеме, установленном правилами *Сервиса*; заключает с *Клиентом* договоры и соглашения, позволяющие *Клиенту* использовать *Сервис* для осуществления обмена *Простыми электронными документами*; обеспечивает получение *Клиентом Средств простой электронной подписи/Аналога собственноручной подписи* для обмена

Простыми электронными документами с использованием *Простой электронной подписи/Аналога собственноручной подписи*, регистрирует *Клиента*, и/или должностных лиц *Клиента*, а также информацию, полученную в ходе *Регистрации*, в *Сервисе*.

7.3. *Организатор сервиса* вправе устанавливать дополнительные требования для возможности участия в документообороте в рамках *Сервиса*.

8. Порядок и условия распространения ПО Оператором для осуществления документооборота в Системе

8.1. Порядок предоставления *Оператором Участнику ПО Сервиса* с элементами *СКЗИ*:

8.1.1. В целях осуществления *Участником ЭДО* в рамках *Сервиса Оператор* безвозмездно предоставляет *Участнику*, а также привлекаемым им третьим лицам на период действия отношений с *Организатором Сервиса* или с *Участником Сервиса* в рамках Правил *Сервиса* право использования *ПО Сервиса* с элементами *СКЗИ*, на условиях простой (неисключительной) лицензии, перечень которых содержится в Приложении № 3 к настоящим Правилам.

8.1.2. *Оператор* гарантирует, что располагает надлежащими правами для передачи программного обеспечения *Участникам* в соответствии с настоящими Правилами и обладает соответствующими лицензиями на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

8.1.3. *Оператор* имеет право размещать и изымать *ПО Сервиса* с элементами *СКЗИ* в сети Интернет по адресам, указанным в Приложении №3 к настоящим Правилам.

8.1.4. *Оператор* обязуется по мере необходимости обновлять *ПО Сервиса* с элементами *СКЗИ* и предоставлять *Участникам* доступ к его актуальной версии. Обновления *ПО Сервиса* с элементами *СКЗИ* размещаются *Оператором* на ресурсах, указанных в Приложения №3 к настоящим Правилам.

8.1.5. *Оператор* имеет право по своему усмотрению и без дополнительного согласования с *Участниками* привлекать к выполнению работ (оказанию услуг, не связанных с элементами *СКЗИ*), по адаптации, модификации *ПО Сервиса* с элементами *СКЗИ*, необходимого для осуществления *ЭДО* в рамках *Сервиса*, Закрытое акционерное общество «ЦЕНТР ФИНАНСОВЫХ ТЕХНОЛОГИЙ» (ИНН 5407125059).

8.1.6. В случае прекращения участия в *Сервисе* и/или в *Системе* по любому основанию, а также в случае прекращения отношений с *Организатором Сервиса* и/или *Оператором, Участник* обязан незамедлительно прекратить использование *ПО Сервиса* с элементами *СКЗИ,* и немедленно уничтожить предоставленное *ПО Сервиса* с элементами *СКЗИ* и копии *ПО Сервиса* с элементами *СКЗИ*, в том числе удалить из устройств для хранения информации.

8.1.7. *Организатор Сервиса* обязуется предоставлять *Оператору* список всех *Участников* и привлекаемых им третьих лиц, которые используют *ПО Сервиса* с элементами *СКЗИ* в целях осуществления *ЭДО* в *Сервисе*.

8.1.8. *Участник* приобретает ограниченные права использовать *ПО Сервиса* с элементами *СКЗИ,* предоставляемое *Оператором* на условиях простой (неисключительной) лицензии фактом скачивания и установки *ПО Сервиса* с элементами *СКЗИ*, признает его соответствие назначению и не имеет к *Оператору* никаких претензий, связанных с передачей *ПО Сервиса* с элементами *СКЗИ*.

8.1.9. *Участник* признает, что *ПО Сервиса* с элементами *СКЗИ*, включая документацию и любые спецификации к нему, содержат информацию, характеризуемую высокой степенью конфиденциальности, являющуюся уникальной, секретной и ценной информацией *Оператора*, и обязуется не разглашать указанную информацию без письменного согласия *Оператора*.

8.1.10. *Участник* без письменного согласия *Оператора* обязуется не осуществлять копирование *ПО Сервиса* с элементами *СКЗИ* или его частей с целью распространения.

8.1.11. *Участник* обязуется не подвергать код *ПО Сервиса* с элементами *СКЗИ* техническому анализу с целью декомпиляции и/или дизассемблирования.

8.1.12. *Участник* обязуется не продавать, не передавать, не публиковать, не раскрывать, не делать каким-либо другим образом доступным для третьих лиц *ПО Сервиса* с элементами *СКЗИ* и любые относящиеся к нему или составляющие его часть материалы.

8.1.13. Участник обязуется не использовать *ПО Сервиса* с элементами *СКЗИ* в целях, не связанных с осуществлением *ЭДО* в *Сервисе*.

8.1.14. *Участник* самостоятельно принимает решение об использовании *ПО Сервиса* с элементами *СКЗИ* в своей деятельности и принимает на себя риски, связанные с использованием *ПО Сервиса* с элементами *СКЗИ* (в том числе риски, связанные с сопряжением (интеграцией) *ПО Сервиса* с элементами *СКЗИ* с программным обеспечением *Участника* и третьих лиц). *Оператор* не несет ответственности перед *Участником* и третьими лицами за убытки, претензии или потери, включая претензии об упущенной выгоде, потерянных накоплениях или другом специфическом, случайном или косвенном ущербе, возникающем в результате использования *ПО Сервиса* с элементами *СКЗИ*.

8.1.15. *Участник* обязан самостоятельно отслеживать появление обновлений программного обеспечения и самостоятельно своевременно устанавливать обновления на свои программно-аппаратные комплексы.

8.1.16. Все обязательства *Участника* в части конфиденциальности, неразглашения, уничтожения, принимаемые им на себя в отношении *ПО Сервиса* с элементами *СКЗИ*, остаются в силе после прекращения участия *Участника* в *Сервисе* и/или *Системе*.

ЭЛЕКТРОННЫЙ ДОКУМЕНТ/ПРОСТОЙ ЭЛЕКТРОННЫЙ ДОКУМЕНТ

9. Требования, предъявляемые к Электронному документу/Простому электронному документу

9.1. *ЭД/Простой ЭД*, сформированный в *Системе*, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в соответствии с настоящими Правилами и действующим законодательством Российской Федерации, а также договорными отношениями между *Участниками*.

9.2. *ЭД/Простой ЭД,* используемый в *Системе*, считается надлежащим образом оформленным при условии его соответствия законодательству Российской Федерации, настоящим Правилам, правилам *Организаторов сервисов*, а также дополнительным договорам, заключаемым между *Участниками*, при наличии таковых.

9.3. *ЭД/Простой ЭД* должен быть сформирован в формате, предусмотренном текущей технологией *Системы*, на момент формирования *ЭД/Простого ЭД*.

9.4. *ЭД* должен быть подписан *ЭП Владельца сертификата*, *Сертификат* которого зарегистрирован согласно настоящими Правилам. *Простой ЭД* должен быть подписан *Простой ЭП* или *АСП,* при этом *Клиент* должен пройти процедуру *Регистрации* в *Сервисе* согласно правилам *Сервиса*.

9.5. Предусмотренные для данного *ЭД/Простого ЭД* правовые последствия могут наступить, только если получен положительный результат проверки *ЭП/Простой ЭП* или *АСП* этого *ЭД/Простого ЭД.*

9.6. *ЭД/Простой ЭД* без *ЭП/Простой ЭП* или *АСП* или имеющий формат, не отвечающий установленным правилам, в качестве *ЭД/Простого ЭД* в рамках *Системы* в соответствии с настоящими Правилами не рассматривается.

10. Использование Электронной подписи, Простой электронной подписи/Аналога собственноручной подписи и шифрования в Электронном документообороте

10.1. Для обмена *ЭД* между *Участниками* допускается использование *Участниками* только совместимых *СКЗИ*. Перечень *СКЗИ*, сертифицированных (разрешённых к использованию) *Оператором* в *Системе* указан в Приложении №2 к настоящим Правилам.

10.2. *ЭД* считается подписанным *Участником*, если он заверен *ЭП, Сертификат* которой зарегистрирован за ним. *Простой ЭД* считается подписанным *Участником,* если он заверен *Простой ЭП* или *АСП*, принадлежащей *Участнику*.

10.3. *ЭП* в *ЭД, Сертификат* которой зарегистрирован за юридическим лицом, признается равнозначной собственноручной подписи уполномоченного лица такого юридического лица в документе на бумажном носителе, заверенном печатью. *АСП* в *Простом ЭД*, принадлежащая уполномоченному лицу юридического лица, удостоверяет факт составления и подписания *Простого ЭД* от имени этого юридического лица, а также подлинность платежного документа, включая все его обязательные реквизиты. *Простая ЭП*, принадлежащая физическому лицу, признается равнозначной собственноручной подписи физического лица в документе на бумажном носителе. При проверке документов для регистрации *Сертификата* за юридическим лицом, физическим лицом или для *Регистрации* юридического лица, физического лица *Оператор, Организатор сервиса* или другой уполномоченный *Участник* обязан в полном объеме проверить документы такого юридического лица, физического лица, проверить полномочия уполномоченного лица на право осуществления действий (заключения сделок, распоряжение банковским счетом и т.д.) от имени юридического лица в рамках *Системы, Сервиса*.

10.4. *ЭД,* содержащий конфиденциальную информацию, может быть зашифрован. Конфиденциальность *ЭД* определяется *Отправителем ЭД*.

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

11. Использование Электронного документа/Простого электронного документа

11.1. Информация в электронной форме, оформляемая *Участником* в виде ЭД в соответствии с настоящими Правилами, а также договорными отношениями между *Участниками*, признаётся электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью и имеющему оттиск печати (при ее наличии), при одновременном выполнении следующих условий:

– подтверждена подлинность *ЭП* в *ЭД* с использованием соответствующих *СКЗИ*, разрешённых к использованию *Оператором* в *Системе ЭДО*, которые перечислены в Приложении № 2 к настоящим Правилам;

– *Сертификат*, относящийся к этой *ЭП,* не утратил силу (действует) на момент подписания *ЭД;*

– *ЭД* учтён *Оператором* или *Организатором сервиса*, согласно правилам учета *ЭД* (Статья 25 настоящих Правил);

– *ЭП* используется в отношениях, регламентируемых настоящими Правилами, правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Оператором*, *Организаторами сервисов*, *Участниками*.

11.2. Информация в электронной форме, оформляемая *Участником* в виде Простого ЭД в соответствии с настоящими Правилами, а также договорными отношениями между *Участниками*, признаётся электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, при одновременном выполнении следующих условий:

– подтверждена подлинность *Простой ЭП* в *Простом ЭД* с использованием *Технологии*, определенной *Организатором сервиса*;

– *Клиент Зарегистрирован* в *Сервисе* на момент подписания *Простого ЭД;*

– *Простой ЭД* учтён *Оператором* или *Организатором сервиса*, согласно правилам учета *Простых ЭД* (Статья 25 настоящих правил);

– *Простая ЭП/АСП* используется в отношениях, регламентируемых настоящими Правилами, правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Оператором*, *Организаторами сервисов, Участниками*.

11.3. В случае если правилами *Организатора сервиса* предусмотрена необходимость подписания *ЭД* или *Простого ЭД ЭП* или *Простой ЭП/АСП* нескольких лиц, то *ЭД* или *Простой ЭД* признается таковым только при условии наличия всех необходимых подписей.

11.4. Факт признания получения *ЭД* или *Простого ЭД Получателем ЭД* или *Простого ЭД* определяется правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Оператором*, *Организаторами сервисов*, *Участниками*. Если категория документа не определена правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Оператором*, *Организаторами сервисов, Участниками*, то *ЭД* или *Простой ЭД* признается полученным с момента подписания *ЭД* или *Простого ЭД*.

12. Подлинник Электронного документа/Простого электронного документа

12.1. *ЭД/Простой ЭД* может иметь неограниченное количество экземпляров, в том числе выполненных на машиночитаемых носителях различного типа. Для создания дополнительного экземпляра существующего *ЭД/Простого ЭД* осуществляется воспроизводство содержания документа вместе с *ЭП/Простой ЭП/АСП*.

12.2. Все экземпляры *ЭД/Простого ЭД* являются подлинниками данного *ЭД/Простого ЭД*.

12.3. *ЭД/Простой ЭД* не может иметь копий в электронном виде.

12.4. Подлинник *ЭД/Простого ЭД* считается не существующим в случаях если:

– не существует ни одного учтенного *Оператором* или *Организатором сервиса* экземпляра данного *ЭД/Простого ЭД* и восстановление таковых невозможно;

– не существует способа установить подлинность *ЭП/Простой ЭП/АСП*, которой подписан данный документ.

13. Копии Электронного документа/Простого электронного документа на бумажном носителе

13.1. Копии *ЭД/Простого ЭД* могут быть изготовлены (распечатаны) на бумажном носителе и должны быть заверены собственноручной подписью уполномоченного лица *Оператора* или *Организатора сервиса* или *Участника*, являющегося *Отправителем ЭД/Простого ЭД* или *Получателем ЭД/Простого ЭД*.

13.2. Копии *ЭД/Простого ЭД* на бумажном носителе должны соответствовать требованиям действующего законодательства, а также содержать обязательную отметку «*Копия Электронного Документа*».

13.3. Информация, содержащаяся в копии на бумажном носителе, должна соответствовать содержанию *ЭД/Простого ЭД*.

КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ И СЕРТИФИКАТЫ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

14. Создание Криптографических ключей

14.1. *Участники* создают собственные *Криптографические ключи* самостоятельно.

14.2. В случаях, предусмотренных правилами *Организаторов сервисов*, *Криптографические ключи Клиента* могут создаваться *Клиентом* с использованием программно-технических средств *Оператора.*.

15. Сертификаты

15.1. *Владелец сертификата* может быть обладателем любого количества *Сертификатов*. Одному *Идентификатору владельца сертификата* может соответствовать более чем один *Сертификат*.

15.2. Для *Участников*, являющихся юридическими лицами, один *Сертификат* может быть зарегистрирован в конкретном *Сервисе* за несколькими разными *Участниками*. Ответственность за надлежащее оформление передачи полномочий *Владельцем* такого *Сертификата* лежит на *Участнике,* осуществившем регистрацию *Сертификата* в *Сервисе*.

15.3. Для *Участников,* являющихся физическими лицами и (или) индивидуальными предпринимателями, *Сертификат* может быть зарегистрирован за единственным *Участником*, являющимся *Владельцем сертификата.*

15.4. *Сертификат* содержит следующие данные:

– *Идентификатор владельца сертификата* (ФИО или псевдоним *Владельца сертификата*, дополнительные сведения);

– *Ключ проверки ЭП*;

– *Идентификатор владельца Сертификата УЦ*, создавшего *Сертификат*;

– Уникальный регистрационный номер *Сертификата*, присвоенный *Удостоверяющим центром*;

– Дату начала и окончания срока действия *Сертификата*;

– Подпись *Удостоверяющим центром* данных *Сертификата*.

15.5. *Сертификат* может содержать дополнительные данные.

15.6. До начала работы *Клиента* в рамках *Системы Идентификаторы владельцев сертификатов* должны быть зарегистрированы *Организатором сервиса* или *Оператором*.

15.7. В *Системе* действуют *Сертификаты* четырех *Классов*:

– *Класс 2* и *Класс* 3 - при создании *Сертификата* произведена проверка с предъявлением соответствующих документов, аналогичная проверке при открытии банковского счета, а также проверка на уникальность *Идентификатора владельца сертификата* таким образом, чтобы *Идентификаторы владельцев сертификатов* данного *Класса*, принадлежащие разным *Владельцам сертификатов*, были уникальны в рамках *УЦ*;

– *Класс* 4 и *Класс 6* - при создании *Сертификата* осуществляется проверка документов и прочей информации в соответствии с порядком, определяемом *Удостоверяющим центром* в каждом конкретном случае.

16. Порядок действий при Компрометации ключа электронной подписи/Средств Простой ЭП/АСП

16.1. В случае *Компрометации ключа ЭП, Средств простой ЭП/АСП Владелец сертификата* скомпрометированного *Ключа ЭП, Средств простой ЭП/АСП* обязан незамедлительно уведомить *Администраторов безопасности* всех *Сервисов*, услугами которых он пользуется, о *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП.*

16.2. Форма уведомления о *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП* определяется правилами *Организатора сервиса*. Уведомление о *Компрометации ключа ЭП* должно содержать *Идентификатор владельца сертификата* соответствующего скомпрометированного *Ключа ЭП*. Уведомление о *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП* может содержать другие данные, определённые правилами *Организатора сервиса*.

16.3. Датой и временем *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП* в рамках данного *Сервиса* считаются дата и время получения *Администратором безопасности Сервиса* уведомления о *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП* с добавлением времени реагирования на уведомление о *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП*, определённого правилами *Организатора сервиса*. Время реагирования на уведомление о *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП* не может превышать одного рабочего дня. Если правилами *Организатора сервиса* время реагирования на уведомление о *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП* не определено, оно считается равным одному рабочему дню.

16.4. Дата и время *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП* не могут быть ранее даты и времени получения уведомления о *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП*.

16.5. Скомпрометированными считаются все *Ключи ЭП*, которым соответствует содержащийся в уведомлении *Идентификатор владельца сертификата*.

16.6. *Организатор сервиса* должен аннулировать права и полномочия доступа к данным и совершения операций *Владельца сертификатов* скомпрометированных *Ключей ЭП, владельца Средств простой ЭП/АСП* и прекратить обработку документов, подписанных или зашифрованных с использованием скомпрометированных *Ключей ЭП, Средств простой ЭП/АСП* не позднее наступления даты и времени *Компрометации ключа ЭП, Компрометации средств простой ЭП/АСП*.

16.7. *ЭД*, *Простой ЭД* подписанный при помощи скомпрометированного *Ключа ЭП*, скомпрометированных *Средств простой ЭП/АСП* признается ненадлежащим и не порождает никаких последствий для *Отправителя ЭД/Простого ЭД*, *Получателя ЭД/Простого ЭД*.

УДОСТОВЕРЯЮЩИЙ ЦЕНТР

17. Правовой статус Удостоверяющего центра

17.1. Правовой статус *УЦ* определяется настоящими Правилами и договорами, заключаемыми *Удостоверяющим центром* с *Оператором*, *Агентами*, действующим законодательством Российской Федерации.

18. Деятельность и обязательства Удостоверяющего центра по отношению к Владельцам сертификатов ключей проверки электронной подписи.

18.1. *УЦ* создает *Сертификаты* в соответствии с Правилами работы *УЦ* только для *Участников*, для которых настоящие Правила вступили в силу в соответствии со Статьей 4, при условии соблюдения ими настоящих Правил и условий договора между *Удостоверяющим центром* и соответствующим *Участником.* Процедура проверки сведений, предоставленных *Участником* при создании *Сертификата*, определяется *Классом*.

18.2. Проверка документов и содержащихся в документах сведений, предоставленных *Клиентом*, осуществляется *Удостоверяющим центром* либо его *Агентом*.

18.3. *УЦ* гарантирует уникальность *Идентификаторов владельцев сертификатов* одного *Класса*, принадлежащих разным владельцам, в рамках *УЦ* при условии, что *Владелец сертификата* не допустил *Компрометации* собственных *Ключей ЭП*. Программно-аппаратные средства *УЦ* исключают возможность создания двух *Сертификатов* с совпадающими *Идентификаторами владельцев*

сертификатов, принадлежащих разным *Владельцам сертификатов*, при условии, что *Ключи ЭП* не были скомпрометированы.

18.4. *УЦ* ведёт реестр *Сертификатов* и предоставляет возможность доступа к нему *Участников*.

18.5. *УЦ* хранит выданные *Сертификаты* в электронном виде в течение всего срока деятельности *УЦ*.

18.6. *УЦ* не несёт ответственности перед *Владельцами сертификатов* и лицами, использующими *Сертификаты* для проверки подписи и шифрования сообщений, третьими лицами за любые убытки, потери, иной ущерб, связанный с использованием *Сертификатов*, независимо от суммы заключенных с использованием *Сертификатов* сделок и совершения ими иных действий в рамках и вне *Системы*, за исключением случаев нарушения *Удостоверяющим центром* обязательств, предусмотренных Правилами и/или действующим законодательством Российской федерации.

18.7. *УЦ* осуществляет иную деятельность, предусмотренную действующим законодательством Российской федерации, настоящими Правилами, соглашениями и договорами, заключенными между *УЦ* и *Участниками*.

19. Обязательства Владельцев сертификатов ключей проверки электронной подписи

19.1. *Владелец сертификата* несёт ответственность за достоверность сведений, которые были предоставлены им *Оператору, УЦ, Агенту* или *Организатору сервиса* при создании *Сертификата* и регистрации *Сертификата*.

19.2. *Владелец сертификата* обязан использовать *Ключи ЭП*, а также *Сертификаты* в рамках *Системы* в соответствии с настоящими Правилами и правилами *Организаторов сервисов*.

19.3. *Владелец сертификата* обязан хранить собственные *Ключи ЭП* в тайне и принять все необходимые меры для предотвращения *Компрометации ключа ЭП* в процессе хранения и использования.

19.4. В случае *Компрометации ключа ЭП Владелец сертификата* соответствующего *Ключа ЭП* обязан предпринять действия, предусмотренные статьёй 15 настоящих Правил.

19.5. *Владелец сертификата* обязан самостоятельно хранить выданный ему *Сертификат* в электронном виде, в том числе и по истечении срока действия *Сертификата*.

ОРГАНИЗАЦИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

20. Электронный документооборот

20.1. *ЭДО* может включать:

- формирование *ЭД/Простых ЭД;*
- отправку и доставку *ЭД/Простых ЭД*;
- проверку *ЭД/Простых ЭД*;
- подтверждение получения *ЭД/Простых ЭД*;
- отзыв *ЭД/Простых ЭД*;
- учет *ЭД/Простых ЭД* (регистрацию входящих и исходящих *ЭД/Простых ЭД*);
- хранение *ЭД/Простых ЭД* (ведение архивов *ЭД/Простых ЭД*);
- создание дополнительных экземпляров *ЭД/Простых ЭД*;
- создание бумажных копий *ЭД/Простых ЭД*.

21. Формирование Электронного документа/Простого электронного документа

21.1. Формирование *ЭД/Простого ЭД* осуществляется в следующем порядке:

- формирование *ЭС* в формате, установленном для данного *ЭД/Простого ЭД;*
- подписание сформированного *ЭС ЭП/Простой ЭП или АСП*.

22. Отправка и доставка Электронного документа/Простого ЭД

22.1. *ЭД/Простой ЭД* считается исходящим от *Отправителя ЭД/Простого ЭД*, если *ЭД/Простой ЭД* отправлен:

- самим отправителем;

– от имени *Отправителя ЭД/Простого ЭД* автоматическим процессом, который представляет собой часть технологических средств *Клиента*, *Организатора сервиса* или *Оператора* и действует в соответствии с правилами *Сервиса*.

22.2. *ЭД/Простой ЭД* не считается исходящим от *Отправителя ЭД/Простого ЭД*, если:

– *Получатель ЭД/Простого ЭД* знал или должен был знать, в том числе в результате выполнения проверки *ЭП/Простой ЭП или АСП,* о том, что *ЭД/Простой ЭД* не исходит от *Отправителя ЭД/Простого ЭД*;

– *Получатель ЭД/Простого ЭД* знал или должен был знать, в том числе в результате выполнения проверки *ЭП/Простой ЭП или АСП*, о том, что получен искаженный *ЭД/Простой ЭД*.

22.3. Особенности отправки, доставки и получения *ЭД/Простого ЭД* могут устанавливаться настоящими Правилами, правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Участниками*.

23. Проверка подлинности доставленного Электронного документа/Простого электронного документа

23.1. Проверка *ЭД/Простого ЭД* включает:

– проверку *ЭД/Простого ЭД* на соответствие установленному для него формату;

– проверку подлинности всех *ЭП/Простых ЭП или АСП, ЭД/Простых ЭД*.

23.2. В случае положительного результата проверки *ЭД/Простого ЭД*, данный *ЭД/Простой ЭД* признается надлежащим. В противном случае данный *ЭД/Простой ЭД* считается не полученным, о чем *Получатель ЭД/Простого ЭД* может послать уведомление *Отправителю ЭД/Простого ЭД*.

23.3. При получении зашифрованного *ЭД*, для проведения проверки подлинности *ЭД* сначала выполняется расшифровывание *ЭД*. В случае невозможности расшифровывания *ЭД Получатель ЭД* может послать уведомление *Отправителю ЭД*.

24. Подтверждение получения ЭД/Простого ЭД

24.1. Подтверждение получения *ЭД/Простого ЭД* определяется правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Оператором*, *Организаторами сервисов*, *Участниками*. Если алгоритм подтверждения документа не определен правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Оператором*, *Организаторами сервисов, Участниками*, то *ЭД/Простой ЭД* считается не полученным *Получателем ЭД/Простого ЭД* до тех пор, пока *Отправитель ЭД/Простого ЭД* не получил соответствующего подтверждения.

24.2. Если подтверждение не получено *Отправителем ЭД/Простого ЭД* в течение установленного срока, то *Отправитель ЭД/Простого ЭД* может уведомить *Получателя ЭД/Простого ЭД* о неполучении подтверждения и указать срок, в течение которого подтверждение должно быть получено.

24.3. Если подтверждение не получено в течение указанного *Отправителем ЭД/Простого ЭД* срока, он вправе считать *ЭД/Простой ЭД* не отправленным. Правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Участниками*, в случае неполучения подтверждения в течение установленного срока может предусматриваться обязанность такого *Отправителя ЭД/Простого ЭД* передать адресату информацию, содержавшуюся в *ЭД/Простом ЭД*, при помощи иных средств связи.

25. Отзыв Электронного документа/Простого электронного документа

25.1. *Отправитель ЭД/Простого ЭД* вправе отозвать *ЭД/Простой ЭД* путем отправки *Получателю ЭД/Простого ЭД ЭД/Простого ЭД* «Уведомление об отзыве», если это предусмотрено правилами *Организатора сервиса.*

25.2. В «Уведомлении об отзыве» должно указываться основание отзыва *ЭД/Простого ЭД.*

25.3. Порядок, сроки, условия отзыва *ЭД/Простого ЭД* и формат *ЭД/Простого ЭД*, уведомляющего об отзыве *ЭД/Простого ЭД*, определяются правилами *Организаторов сервиса*.

26. Учет Электронных документов/Простых электронных документов

26.1. Учет *ЭД/Простых ЭД* осуществляется путем ведения электронных журналов учета или традиционных бумажных журналов учета. Технология ведения электронных журналов учета должна включать 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 *ЭДО*.

26.2. Для выполнения текущих работ по ведению учета *ЭД/Простых ЭД* в рамках *Сервиса Организатор сервиса* назначает ответственных лиц.

26.3. Особенности учета *ЭД/Простых ЭД* в *Сервисе* определяются правилами *Организаторов сервисов*, а также дополнительными договорами, заключаемыми между *Оператором, Организаторами сервисов, Участниками.*

26.4. *Оператор* и *Организаторы сервисов* должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в принадлежащих им электронных журналах учета *ЭД/Простых ЭД*. Срок хранения учетных данных не может быть менее 5 (Пяти) лет.

27. Хранение Электронных документов/Простых электронных документов

27.1. Все учтенные *ЭД/Простые ЭД* должны храниться в течение сроков, предусмотренных настоящими Правилами или правилами *Организатора сервиса*. *ЭД/Простые ЭД* должны храниться либо в электронных архивах, либо в виде копий *ЭД/Простых ЭД* на бумажных носителях, заверенных ответственным лицом *Участника*.

27.2. Если правилами *Организатора сервиса*, а также дополнительными договорами, заключаемыми между *Участниками*, не предусмотрено иное, *ЭД/Простые ЭД* должны храниться в том же формате, в котором они были сформированы, отправлены или получены. Срок хранения *ЭД/Простых ЭД* не может быть менее 3 (Трех) лет.

27.3. Хранение *ЭД/Простых ЭД* должно сопровождаться хранением соответствующих электронных журналов учета, *Сертификатов* и программного обеспечения, обеспечивающего возможность работы с электронными журналами и проверки *ЭП/Простых ЭП или АСП* хранимых *ЭД/Простых ЭД*.

27.4. Обязанности хранения *ЭД/Простых ЭД* возлагаются на *Участников*.

27.5. Для выполнения текущих работ по ведению электронных архивов в подсистемах обработки данных *Системы Участники* назначают ответственных лиц.

27.6. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного или преднамеренного уничтожения и/или искажения.

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

28. Средства обеспечения информационной безопасности

28.1. Информация, содержащая персональные данные, и конфиденциальная информация в *Системе* подлежит защите от разглашения.

28.2. Соблюдение требований информационной безопасности при организации *ЭДО* обеспечивает:

– конфиденциальность информации (расшифровать информацию могут только уполномоченные лица);

– целостность передаваемой информации (гарантирование, что данные передаются без искажений, и исключается возможность подмены информации);

– аутентичность информации (отправителем информации является именно тот, от чьего имени она отправлена).

28.3. Требования по информационной безопасности при организации *ЭДО* реализуются посредством применения программно-технических средств и организационных мер.

28.4. К программно-техническим средствам относятся:

– программные средства, специально разработанные для осуществления *ЭДО;*

– система паролей и идентификаторов для ограничения доступа пользователей и операторов к техническим и программным средствам системы *ЭДО*;

– средства формирования и проверки *ЭП*;

– *Средства простой ЭП/АСП;*

– *Технология простой ЭП/АСП;*

– *СКЗИ*;

– программно-аппаратные средства защиты от несанкционированного доступа;

– средства защиты от программных вирусов;

– средства защиты от иных угроз информационной безопасности.

28.5. 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 ЭДО 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.);

– иные организационные меры, направленные на обеспечение информационной безопасности.

28.6. Порядок использования *СКЗИ*, применяемых в *Системе*, определяются настоящими Правилами. Особенности использования *СКЗИ*, применяемых в *Системе*, могут также дополнительно определяться правилами *Организаторов сервисов*, дополнительными договорами, заключаемыми между *Оператором* и *Участниками*, а также законодательством РФ.

28.7. Порядок использования *Средств простой ЭП/АСП*, применяемых в *Сервисе*, определяются правилами *Сервиса*.

ЧРЕЗВЫЧАЙНЫЕ СИТУАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

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

29.1. 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 *Оператора*, *Организатора сервиса*, временно или на неопределенный срок сделали, делают или могут сделать невозможным или значительно затруднить осуществление *ЭДО*. К таким событиям/обстоятельствам, в том числе, могут быть отнесены:

– пожары, наводнения, иные стихийные бедствия или техногенные катастрофы, иные обстоятельства непреодолимой силы;

– разрушения или значительные повреждения занимаемых помещений;

– нестабильность или отключение электроэнергии, которое не может быть нейтрализовано имеющимися в распоряжении техническими средствами;

– неработоспособность программного обеспечения, вычислительной техники, оргтехники, средств связи, включая средства телекоммуникаций;

– массовые беспорядки, вооруженные столкновения, демонстрации;

– террористические акты или диверсии;

– воздействие на программные комплексы *Системы* вредоносных программ.

– неспособность *Организатора сервиса* выполнять свои функции *Организатора сервиса,* в том числе и в случае расторжения или приостановления действия договора на участие в *Системе*;

– любые другие подобные события или обстоятельства, которые могут существенным образом затруднить или сделать невозможным осуществление *ЭДО*.

29.2. 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 *ЭДО* в том виде, форме и порядке, в которых он осуществлялся до принятия данных актов.

30. Порядок уведомления о наступлении обстоятельств, могущих послужить причиной возникновения чрезвычайных ситуаций

30.1. В случае наступления хотя бы одного из обстоятельств, соответствующих перечисленным в статье 28 настоящих Правил:

– *Участник* обязан незамедлительно с учетом сложившейся ситуации и способом, доступным в сложившихся обстоятельствах, известить *Организатора сервиса* о возникших обстоятельствах;

– *Организатор сервиса* обязан незамедлительно известить *Участников* о возникших обстоятельствах размещением информации на сервере *Организатора сервиса*, если это является возможным;

– *Оператор* обязан незамедлительно известить *Участников* о возникших обстоятельствах путем размещения соответствующей информации в информационной части *Системы* по адресу www.BeSafe.ru, если это является возможным.

Впоследствии *Участник* обязан письменным сообщением *Организатору сервиса* подтвердить уведомление о возникших обстоятельствах, способных послужить причиной возникновения чрезвычайных ситуаций.

30.2. Для квалификации ситуации, связанной с наличием хотя бы одного из обстоятельств, соответствующих перечисленным в статье 28 настоящих Правил, в качестве чрезвычайной ситуации, в том числе технического сбоя, достаточно решения *Оператора*, *Организатора сервиса*.

30.3. Решение *Оператора*, *Организатора сервиса* о квалификации обстоятельств, из числа перечисленных в статье 29 настоящих Правил в качестве чрезвычайной ситуации (квалифицирующее решение *Оператора*, *Организатора сервиса*) оформляется документом, составленным в письменной форме. По требованию заинтересованных *Участников* такое решение может быть представлено в виде *ЭД/Простого ЭД* или на бумажном носителе.

31. Последствия принятия квалифицирующего решения Оператором, Организатором сервиса

31.1. В случае признания *Оператором/Организатором сервиса* ситуации, связанной с наличием хотя бы одного из обстоятельств, соответствующих перечисленным в статье 28 настоящих Правил, в качестве чрезвычайной ситуации, *ЭДО* в рамках *Системы/Сервиса* может быть прекращен по решению *Оператора/Организатора сервиса*.

31.2. Одновременно с признанием ситуации чрезвычайной *Оператор/Организатор сервиса* приступает к разработке мер по урегулированию сложившейся чрезвычайной ситуации в *Системе/Сервисе*.

31.3. Возобновление *ЭДО* осуществляется по решению *Оператора/Организатора сервиса*.

32. Меры по урегулированию чрезвычайных ситуаций

32.1. В качестве мер по урегулированию сложившейся чрезвычайной ситуации *Оператор/Организатор сервиса* вправе:

– прекратить или ограничить обращение всех или части *ЭД/Простых ЭД* в *Системе/Сервисе*;

– совместно с *Участником* 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 *Участников* безвозмездного и незамедлительного с учетом сложившихся обстоятельств предоставления *Оператору/Организатору сервиса* копий на бумажных носителях всех или части *ЭД/Простых ЭД*, обращавшихся в *Системе/Сервисе* за определенный период времени;

– потребовать от *Участников* за их счет незамедлительного с учетом сложившихся обстоятельств восстановления, в том числе, в виде копий на бумажных носителях обращения всех или части *ЭД/Простых ЭД* в *Системе/Сервисе*;

– потребовать от *Участников* безвозмездного и незамедлительного с учетом сложившихся обстоятельств предоставления копий, в том числе и, в случае необходимости, нотариально заверенных копий журналов *ЭД/Простых ЭД*, сформированных и обращавшихся в *Системе/Сервисе* за определенный период;

– предусмотреть иные меры, направленные на преодоление чрезвычайной ситуации.

32.2. При принятии решений по урегулированию чрезвычайных ситуаций *Оператор/Организатор сервиса* вправе:

– устанавливать сроки и форму уведомления *Участников* о своих решениях;

– устанавливать сроки и порядок исполнения своих решений;

– обуславливать порядок вступления в силу своих решений определенными обстоятельствами.

32.3. Решения *Оператора/Организатора сервиса* по урегулированию чрезвычайной ситуации в *Системе/Сервисе* являются обязательными для исполнения *Участниками*.

32.4. О решениях *Оператора/Организатора сервиса* и мерах по урегулированию чрезвычайной ситуации *Участники* уведомляются не позднее принятия данных мер в соответствии с данным решением.

ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ, ВОЗНИКШИХ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СИСТЕМЕ

33. Возникновение конфликтных ситуаций в связи с осуществлением Электронного документооборота в Системе

33.1. В связи с осуществлением *ЭДО* возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения *ЭД/Простых ЭД*, а также использованием в данных документах *ЭП/Простой ЭП/АСП*. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

– неподтверждение подлинности *ЭД/Простого ЭД* средствами проверки *ЭП/Простой ЭП/АСП* принимающей *Стороны*;

– оспаривание факта формирования *ЭД/Простого ЭД*;

– оспаривание факта идентификации *Владельца сертификата*, подписавшего документ;

– оспаривание факта *Регистрации Клиента,* подписавшего *Простой ЭД*;

– заявление *Участника* об искажении *ЭД/Простого ЭД*;

– оспаривание факта отправления и/или доставки *ЭД/Простого ЭД*;

– оспаривание времени отправления и/или доставки *ЭД/Простого ЭД*;

оспаривание соответствия экземпляров *ЭД/Простого ЭД* и/или подлинника и копии *ЭД/Простого ЭД* на бумажном носителе; иные случаи возникновения конфликтных ситуаций, связанных с функционированием *Системы и/или Сервисов*.

33.2. Конфликтная ситуация возникает также в случае, если *Участник*:

– высказывает недоверие к составу и формату *ЭД/Простых ЭД*, хранящихся в локальном архиве рабочего места *Участника*;

– высказывает недоверие к программному обеспечению, функционирующему на данном рабочем месте.

34. Уведомление о конфликтной ситуации

34.1. В случае возникновения конфликтной ситуации *Организатор сервиса* или *Клиент*, считающие, что их права были нарушены действиями *Участников* и (или) *УЦ*, должен не позднее чем в течение 3 (Трех) рабочих дней или в иной более короткий срок, указанный в правилах *Организаторов сервисов*, а также договорах, заключаемых между *Оператором* и *Организаторами сервисов*, со дня, когда соответственно *Организатору сервиса* или *Клиенту* стало известно или должно было стать известно о нарушении его права, направить уведомление о конфликтной ситуации *Оператору*, а в случае возникновения конфликтной ситуации в рамках *Сервиса – Организатору данного сервиса.*

34.2. 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 *ЭД/Простой ЭД*), оно должно содержать реквизиты *ЭД/Простого ЭД*, а также фамилию, имя, отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации. В случае если конфликтная ситуация затрагивает интересы нескольких *Участников*, то уведомитель также приводит в уведомлении контактные данные всех *Участников* (либо уполномоченных лиц – представителей *Участников*), чьи интересы были затронуты в данной конфликтной ситуации.

34.3. Уведомление о наличии конфликтной ситуации оформляется и отправляется в виде *ЭД/Простого ЭД*, а в случае, если это невозможно или не предусмотрено правилами *Организатора сервиса*, то составляется в письменной форме и направляется с нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату, а также дублируется факсимильным сообщением либо сообщением электронной почты. Сторона, которой направлено уведомление, обязана незамедлительно, однако не позднее чем в течение следующего рабочего дня (или в иной, более короткий срок, указанный в правилах *Организаторов сервисов*, а также договорах, заключаемых между *Оператором* и *Организаторами сервисов*), 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.

34.4. При необходимости в случае возникновения спора между *Участниками Организатор сервиса* по письменному запросу *Участника*, состоящего в споре, представляет ему подтверждение участия спорящих *Участников* в *Сервисе*, а также заверенную выписку из журнала *Сервиса*, содержащую регистрацию событий в *Сервисе*, имеющих отношение к предмету спора, если *Участник* представит разумное обоснование ее необходимости для урегулирования спора.

35. Разрешение конфликтной ситуации в рабочем порядке

35.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае если уведомитель удовлетворен информацией, полученной от *Участника*, которому было направлено уведомление.

35.2. В случае если уведомитель не удовлетворен информацией, полученной от *Участника*, которому направлялось уведомление, для рассмотрения конфликтной ситуации формируется техническая комиссия.

36. Формирование технической комиссии, ее состав

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

36.2. Если *Участники*, 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 и представитель *Оператора* и по согласованию сторон представитель *Организатора сервиса*. В случае участия представителя *Оператора* работа технической комиссии осуществляется по месту нахождения *Оператора*.

36.3. В состав технической комиссии, как правило, назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности сторон.

36.4. Право представлять в комиссии соответствующую *Сторону*, а также *Оператора*, *Организатора сервиса*, должно подтверждаться доверенностью, выданной каждому представителю на срок работы комиссии.

36.5. По инициативе любой из сторон к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты без права голоса, обладающие необходимыми знаниями в области защиты информации, работы компьютерных информационных систем. *Сторона*, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

36.6. Работа технической комиссии осуществляется по месту нахождения *Оператора* или *Организатора сервиса.*

37. Компетенция и полномочия технической комиссии

37.1. 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 *ЭД/Простого ЭД*, его подлинности, а также о подписании *ЭД/Простого ЭД* конкретной *ЭП/Простой ЭП/АСП*, идентичности отправленного и полученного *ЭД/Простого ЭД*.

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

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

37.4. Для проведения необходимых проверок и документирования данных, используемых при указанных проверках, применяется специальное программное обеспечение, предоставляемое *Оператором* или *Организатором сервиса*. Для подтверждения подлинности *ЭП/Простой ЭП/АСП* в *ЭД/Простом ЭД* применяется эталонный модуль проверки подписи документа.

38. Протокол работы технической комиссии

38.1. 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.

38.2. 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.

38.3. Протокол составляется в одном подлинном экземпляре на бумажном носителе, который находится на хранении у *Оператора* или *Организатора сервиса*. По требованию любой из сторон в конфликтной ситуации, или любого из членов технической комиссии, им может быть выдана заверенная *Оператором* или *Организатором сервиса* копия Протокола.

39. Акт по итогам работы технической комиссии

39.1. 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;
- выводы, к которым пришла комиссия в результате проведенных мероприятий;
- подписи членов комиссии;
- указание на особое мнение члена (или членов комиссии), в случае наличия такового.

39.2. Акт составляется в таком количестве экземпляров, чтобы каждая из сторон в конфликтной ситуации, а также *Оператор* или *Организатор сервиса* имели по одному подлинному экземпляру составленного акта. По требованию члена комиссии ему может быть выдана заверенная *Оператором* или *Организатором сервиса* копия Акта.

39.3. К Акту может прилагаться особое мнение члена (или членов комиссии), не согласного 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.

39.4. Акт по итогам работы технической комиссии направляется *Оператором* или *Организатором сервиса* сторонам в конфликтной ситуации с нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

40. Претензионный порядок урегулирования конфликтной ситуации

40.1. В случае, если конфликтная ситуация не урегулирована в результате работы технической комиссии, либо в иной ситуации, если *Участник* считает, что его права при осуществлении *ЭДО* в рамках *Системы* или *Сервиса* были нарушены, он обязан направить стороне, которая, по его мнению, нарушила его права, претензию.

40.2. Претензия должна содержать:

– изложение существа требований *Участника*;

– указание суммы претензии и ее расчет (если претензия подлежит денежной оценке);

– изложение обстоятельств, на которых основываются требования, и доказательства, подтверждающие их, со ссылкой на нормы законодательства и/или внутренние нормативные документы;

– сведения о работе технической комиссии и, в случае, если техническая комиссия работала в связи с возникшей конфликтной ситуацией, копии материалов работы технической комиссии, независимо от выводов технической комиссии, согласия или несогласия с этими выводами заявителя претензии;

– иные документы, имеющие значение, по мнению заявителя претензии;

– перечень прилагаемых к претензии документов и других доказательств, а также иные сведения, необходимые для урегулирования разногласий по претензии.

40.3. Претензия и все прилагаемые к ней документы направляются с нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

40.4. Сторона, в адрес которой направлена претензия, обязана не позднее чем в течение 14 (Четырнадцати) рабочих дней удовлетворить претензию или представить мотивированный отказ в удовлетворении заявленной претензии. Непредставление ответа на претензию в течение установленного срока является нарушением установленного настоящими Правилами претензионного порядка и может рассматриваться лицом, направившим претензию, в качестве отказа в удовлетворении претензии.

41. Разрешение споров в Арбитражном суде

41.1. Все споры и разногласия между *Участниками*, возникающие в связи с осуществлением *ЭДО* в соответствии с настоящими Правилами, а также в связи с применением, нарушением, толкованием настоящих Правил, признанием недействительными настоящих Правил или их части, в случае если претензия истца не была удовлетворена в сроки, установленные настоящими Правилами, подлежат разрешению в Арбитражном суде по месту нахождения ответчика, или по месту нахождения *Оператора*, в случае если одной из сторон является *Оператор* или *Организатор сервиса*.

41.2. Решения Арбитражного суда являются обязательными для сторон. Неисполненное в срок решение Арбитражного суда подлежит принудительному исполнению в соответствии с законодательством Российской Федерации, законодательством страны места принудительного исполнения и международными соглашениями.

ИНЫЕ ПОЛОЖЕНИЯ

42. Приложения к настоящим Правилам

42.1. К настоящим Правилам прилагаются и являются их неотъемлемой частью:

Приложение № 1. Соглашение о присоединении к Правилам *Электронного документооборота* корпоративной информационной *Системы «BeSafe»*

Приложение № 2. Перечень *Средств криптографической защиты информации*, сертифицированных (разрешённых к использованию) *Оператором* в *Системе*.

Приложение № 3. Перечень ПО Сервиса с элементами СКЗИ, разрешённых к использованию Оператором в Системе для Участников:

43. Прекращение действия настоящих Правил для всех Участников

43.1. Настоящие Правила прекращают свое действие на основании решения *Оператора*.

43.2. Прекращение действия настоящих Правил и Приложений к ним не влияет на юридическую силу и действительность *ЭД/Простых ЭД*, которыми *Участники* обменивались до прекращения действия настоящих Правил и Приложений к ним.

44. Переходные положения

44.1. Категории подтверждения получения *ЭД/Простых ЭД*, применяемые в предыдущих редакциях Правил, устранены. *ЭД/Простые ЭД*, соответствующие данным категориям, начиная с настоящей редакции Правил признаются полученными *Получателем ЭД/Простых ЭД* с момента подтверждения получения *ЭД/Простых ЭД Получателем*.

Приложение №1 к «Правилам *Электронного документооборота* корпоративной информационной *Системы «BeSafe»*» - *Соглашение о присоединении между Организатором сервиса/Уполномоченным лицом Организатора сервиса и Участником*

Соглашение о присоединении к Правилам *Электронного документооборота* корпоративной информационной *Системы «BeSafe».*

г. Новосибирск ____ _____20 года

_____, в лице _____, действующего (ей) на основании _____, именуемое в дальнейшем *«Организатор сервиса»/«Уполномоченное лицо Организатора сервиса»*, с одной стороны, и_____(Полное наименование юридического лица, ФИО, должность и документ на основании которого осуществляется деятельность/ ФИО физического лица), именуемое в дальнейшем *«Участник»*, с другой стороны, заключили настоящее Соглашение о следующем:

1.Предметом Соглашения является присоединение Участника к Правилам корпоративной информационной *Системы «BeSafe»,* которые расположены в Интернете по адресу www.besafe.ru, а также правилам *Сервиса* _____, которые расположены в Интернете по адресу www._____.ru. Правила корпоративной информационной *Системы «BeSafe»* и Правила *Сервиса* _____ являются неотъемлемой частью настоящего Соглашения.

2.Правила корпоративной информационной *Системы «BeSafe»* распространяются на *Организатора сервиса, Клиента*, других *Участников* только в рамках их участия в работе *Сервиса* _____.

3.*Организатор сервиса* и *Участник* признают, что:

получение документа, подписанного *Простой электронной подписью Участника,* юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручной подписью *Участника*. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что *Простая электронная подпись Участника* создана с использованием технологии *Системы «BeSafe»*;

получение документа, подписанного *Электронной подписью Участника*, уполномоченного лица *Участника*, *Удостоверяющего центра* юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц *Участника, Удостоверяющего центра* и оттиском печати *Участника, Удостоверяющего центра*. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что *Ключ электронной подписи, Электронная подпись* и *Сертификат ключа проверки электронной подписи Участника*, уполномоченного лица *Участника, Удостоверяющего центра* созданы с использованием технологии *Системы «BeSafe»*;

получение документа, подписанного *Электронной подписью Организатора сервиса*, *Удостоверяющего центра* юридически эквивалентно получению документа на бумажном носителе, заверенного собственноручными подписями уполномоченных лиц *Организатора сервиса*, *Удостоверяющего центра* и оттиском их печати. Обязательства, предусмотренные настоящим пунктом, действительны при условии, что *Ключ электронной подписи, Электронная подпись* и *Сертификат ключа проверки электронной подписи Организатора сервиса*, *Удостоверяющего центра* созданы с использованием технологии *Системы «BeSafe».*

4.Настоящее Соглашение вступает в силу от даты его подписания сторонами и действует до его расторжения по основаниям, предусмотренным настоящими Правилами, договором или действующим законодательством.

5.Каждая из сторон имеет право расторгнуть настоящее Соглашение в одностороннем порядке, предварительно направив уведомление другой стороне не менее чем за три месяца до его расторжения.

РЕКВИЗИТЫ СТОРОН:

Организатор сервиса/Уполномоченное лицо Организатора сервиса:	Участник:
	(Реквизиты Юридического лица или паспортные данные физического лица)
_____ (_____)	_____ (_____)
М.п.	

Приложение №2 к «Правилам *Электронного документооборота* корпоративной информационной *Системы «BeSafe»*»

Перечень *Средств криптографической защиты информации*, сертифицированных (разрешённых к использованию) *Оператором* в *Системе*.

1. Для защиты *ЭД* в *Системе* могут использоваться следующие *СКЗИ*:
    - Microsoft Enhanced CSP
    - Java security provider SUN
    - SUN Java Secure Socket Extension
    - OpenSSL (www.openssl.org)
    - КриптоПро CSP
    - MS_Key K, MS_Key
    - Oberthur ID-One Cosmo
    - eToken ГОСТ
    - eToken Pro (Java)
    - Infotecs VipNet CSP
    - РУТОКЕН ЭЦП

Использование иных *СКЗИ* в *Системе* для защиты *ЭД* до внесения их в приведённый выше список недопустимо.

2. *СКЗИ*:
    - Microsoft Enhanced CSP
    - Java security provider SUN
    - SUN Java Secure Socket Extension
    - OpenSSL (www.openssl.org)
    - Oberthur ID-One Cosmo
    - MS_Key K, MS_Key
    - eToken Pro (Java)

Основаны на криптографических алгоритмах, соответствующих международным стандартам и совместимы между собой. Для обеспечения взаимодействия отправитель и получатель *ЭД* могут использовать любое из перечисленных криптографических средств.

3. *СКЗИ*:
    - КриптоПро CSP
    - MS_Key K, MS_Key
    - eToken ГОСТ
    - Infotecs VipNet CSP
    - РУТОКЕН ЭЦП

Основаны на криптографических алгоритмах, соответствующих ГОСТ и имеет сертификат ФСБ. Для обеспечения взаимодействия и отправитель, и получатель *ЭД* могут использовать любое из перечисленных криптографических средств.

Приложение №3 к «Правилам *Электронного документооборота* корпоративной информационной *Системы «BeSafe»*»

1. Перечень *ПО Сервиса* с элементами *СКЗИ*, разрешённых к использованию *Оператором* в *Системе* для *Участников*:

- Шлюз;
- SMS-шлюз;
- NPD-Crypto-Proxy;
- Мобильное приложение F.Balance для платформы IOS;
- Мобильное приложение F.Balance для платформы Android;
- Мобильное приложение F.Business для платформы IOS;
- Мобильное приложение F.Business для платформы Android;
- Интернет-банк FAKTURA.RU для «1С: Предприятие»;
- АРМ «Обмен реестрами»;
- АРМ «Администратор пользователей»;
- АРМ «Формирования отчетов»;
- Плагин ЕАС ОПС;
- Инсталлятор (библиотеки печати+VPN) для работы с терминальными АРМ-ами;
- МПКТ Android;
- МПКТ Аврора;
- МПКТ Sailfish.

2.Условия размещения *ПО Сервиса*.

2.1. Адреса размещения *ПО Сервиса* с элементами *СКЗИ* в сети Интернет для *Сервиса* «Faktura.ru»:

2.1.1. *ПО Сервиса* с элементами *СКЗИ* Шлюз, SMS-шлюз, NPD-Crypto-Proxy, Интернет-банк FAKTURA.RU для «1С: Предприятие» размещаются по адресу www.besafe.ru.

2.1.2. *ПО Сервиса* с элементами *СКЗИ* Мобильное приложение F.Balance для платформы IOS и Мобильное приложение F.Business для платформы IOS размещаются в магазине приложений iTunes Store по адресу https://www.apple.com/iphone/.

Для размещения *ПО Сервиса* Мобильное приложение F.Balance для платформы IOS и Мобильное приложение F.Business для платформы IOS в магазине приложений iTunes Store по адресу https://www.apple.com/iphone/, включая (при необходимости) повторную загрузку, обновление, перемещение, размещение описания *ПО Сервиса*, *Участник* обязуется предоставить представителям Оператора доступ к учетной записи *Участника* на портале iTunesConnect (https://itunesconnect.apple.com) с ролью «Менеджер приложений» (App Manager).

2.1.3. *ПО Сервиса* с элементами *СКЗИ* Мобильное приложение F.Balance для платформы Android и Мобильное приложение F.Business для платформы Android размещаются в магазине приложений Google Play Store по адресу play.google.com.

2.2. Адреса размещения *ПО Сервиса* с элементами *СКЗИ* в сети Интернет для *Сервиса* «Федеральная система «Город», а также для иных договоров, заключаемых *Организатором Сервиса* «Федеральная система «Город», в рамках которых партнерами *Организатора Сервиса* используется указанное ниже *ПО Сервиса*:

2.2.1. *ПО Сервиса* с элементами *СКЗИ* АРМ «Обмен реестрами»; АРМ «Администратор пользователей»; АРМ «Формирования отчетов»; Плагин ЕАС ОПС; Инсталлятор (библиотеки печати+VPN) для работы с терминальными АРМ-ами, МПКТ Android, МПКТ Аврора, МПКТ Sailfish размещаются по адресу www.besafe.ru