



СДК «Гарант»

УТВЕРЖДЕНО
единственным Участником
ООО «СДК «Гарант»
ЗАО «Холдинговая компания Гарант»
Решение №1/97 от 25 марта 2011 года

**ПРАВИЛА
ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
ООО «СДК «ГАРАНТ»**



Специализированная депозитарная
компания «Гарант»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила электронного документооборота ООО «СДК «Гарант» (далее именуются *Правила*), а также приложения к ним определяют общий порядок и принципы осуществления электронного документооборота между ООО «СДК «Гарант» (далее именуется *Организатор СЭД, Компания, Общество*) и лицами, присоединившимися к системе электронного документооборота ООО «СДК «Гарант» (далее именуются *Участники ЭДО*), при осуществлении профессиональной деятельности с использованием документов в электронно-цифровой форме.

1.2. Настоящие Правила разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 10 января 2002 года N 1-ФЗ «Об электронной цифровой подписи» и иных нормативных правовых актов Российской Федерации.

1.3. Настоящие Правила вступают в силу для Участника ЭДО после заключения между Участником ЭДО и Организатором СЭД **Договора о присоединении к Правилам ЭДО ООО «СДК «Гарант»** (далее именуется *Договор*) ([Приложение №1 к настоящим Правилам](#)).

1.4. Структура документов в электронно-цифровой форме, обмен которыми осуществляется в системе электронного документооборота ООО «СДК «Гарант», должна строго соответствовать форматам электронных документов, принятых и утвержденных Организатором СЭД. **Форматы электронных документов, используемые в системе электронного документооборота ООО «СДК «Гарант»** ([Приложение №2 к настоящим Правилам](#)).

1.5. Для обеспечения авторства, целостности и конфиденциальности электронных документов Организатор СЭД и Участники ЭДО используют средства криптографической защиты (далее именуются *СКЗИ*), ключи и сертификаты ключей, предоставляемые Организатором СЭД в порядке, установленном настоящими Правилами.

1.6. Система электронного документооборота ООО «СДК «Гарант» состоит из следующих функциональных блоков:

- Система электронного документооборота Депозитария (далее именуется *СЭД Депозитария*);
- Система электронного документооборота Специализированного депозитария (далее именуется *СЭД Специализированного депозитария*);
- Система электронного документооборота Специализированного регистратора (далее именуется *СЭД Специализированного регистратора*);
- Система электронного документооборота Негосударственный пенсионный фонд – Управляющая компания (дополнительный функционал).

1.7. СЭД ООО «СДК «Гарант» обеспечивает обмен электронными документами между Организатором СЭД и Участником ЭДО.

1.8. Настоящие Правила, включая все Приложения, утверждаются Организатором СЭД. Изменения и дополнения в настоящие Правила и Приложения к ним вносятся в одностороннем порядке по решению Организатора СЭД. Организатор СЭД вправе определять сроки и порядок вступления в силу изменений и дополнений в настоящие Правила и Приложения к ним.

1.9. Настоящие Правила, включая все Приложения, изменения и дополнения к ним, публикуются в сети Internet на официальной странице ООО «СДК «Гарант» - www.sdkgarant.ru.

1.10. Изменения и дополнения в настоящие Правила и Приложения к ним, а также решения о сроках и порядке вступления их в силу, доводятся Организатором СЭД до сведения Участников ЭДО путем направления электронного сообщения с уведомлением о данном факте не позднее, чем за 5 (пять) рабочих дней до вступления в силу изменений в

Правила и Приложения к ним, а также путем опубликования этой информации в сети Internet на официальной странице ООО «СДК «Гарант» - www.sdkgarant.ru. Отправка такого электронного сообщения осуществляется по электронному адресу, указанному Участником ЭДО в сети Internet на официальной странице Участника ЭДО.

1.11. Участник ЭДО имеет право запрашивать у Организатора СЭД копии настоящих Правил и всех изменений и дополнений к ним.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Авторство электронного документа – принадлежность электронного документа конкретному Участнику ЭДО. Авторство электронного документа определяется принадлежностью электронно-цифровой подписи конкретному Участнику ЭДО.

Администратор безопасности СЭД – должностное лицо Организатора СЭД, уполномоченное на управление ключами и сертификатами ключей, регистрацию Участников ЭДО, обеспечение безопасности ЭДО в целом, разработку и направление указаний и рекомендаций по организации системы защиты и повышению ее надежности.

Владелец сертификата ключа электронно-цифровой подписи (Владелец сертификата ключа подписи) – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Дистрибутив ПО SeMa - это комплект программного обеспечения, содержащий вспомогательные инструменты для автоматической или автоматизированной начальной настройки программного обеспечения, программа-инсталлятор.

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

Закрытый (секретный) ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств криптографической защиты информации.

Закрытый (секретный) ключ шифрования – уникальная последовательность данных, используемая для дешифрования электронного документа его получателем и для зашифрования электронного документа его отправителем.

Ключевой носитель - электронный носитель ключевой информации, содержащий криптографические ключи (дискета Smart Card, Touch Memo и т.п.).

Компрометация ключа – констатация лицом, владеющим закрытым (секретным) ключом электронно-цифровой подписи и/или шифрования, обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- утрата ключевых носителей;

- утрата ключевых носителей с последующим обнаружением;

- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей;
- утрата ключей от сейфов в момент нахождения в них ключевых носителей с последующим обнаружением;
- доступ посторонних лиц к ключевой информации
- передача ключевой информации по линии связи в открытом виде;
- нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
- несанкционированное копирование ключевых дискет;
- случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе случаи, когда магнитный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Конфиденциальная информация – документированная информация, имеющая действительную или потенциальную коммерческую или иную ценность в силу неизвестности ее третьим лицам, при отсутствии к ней свободного доступа на законном основании и если обладатель информации принимает меры к ее охране.

Криптографические ключи (Ключи) – общее название открытых и закрытых (секретных) ключей электронно-цифровой подписи и/или шифрования.

Организатор системы электронного документооборота (Организатор СЭД) – Общество с ограниченной ответственностью «Специализированная депозитарная компания «Гарант» (ООО «СДК «Гарант»), имеющее соответствующие лицензии ФСБ России на осуществление деятельности по распространению шифровальных (криптографических) средств, техническому обслуживанию шифровальных (криптографических) средств, предназначенных для криптографической защиты информации при ее обработке, хранении и передаче по каналам связи в конкретной корпоративной информационной системе, и осуществляющее эксплуатацию этой системы.

Организация - Организатор СЭД и Участник ЭДО.

Открытый ключ шифрования – уникальная последовательность данных, соответствующая закрытому (секретному) ключу шифрования, доступная Организатору СЭД и любому Участнику ЭДО, которая используется для зашифрования электронного документа его отправителем.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная Организатору СЭД и любому Участнику ЭДО и предназначенная для подтверждения с

использованием средств криптографической защиты информации подлинности электронной цифровой подписи в электронном документе.

Отправитель электронного документа (Отправитель) – лицо, которое, или от имени которого, направляется электронный документ.

Плановая смена ключей – смена ключей с установленной в СЭД ООО «СДК «Гарант» периодичностью, не вызванная компрометацией ключей.

Подтверждение подлинности электронно-цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Получатель электронного документа (Получатель) – лицо, которому предназначен электронный документ, отправленный самим отправителем или от имени и по поручению отправителя.

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Система электронного документооборота ООО «СДК «Гарант» (СЭД ООО «СДК «Гарант») – совокупность правил, организационных мер и программно-технических средств (включая СКЗИ), реализованная в рамках взаимодействия Организатора СЭД с Участниками ЭДО в целях осуществления электронного документооборота и являющаяся корпоративной информационной системой.

СЭД Депозитария – отдельный функциональный блок СЭД ООО «СДК «Гарант», предназначенный для обеспечения обмена электронными документами между Отделом депозитарного обслуживания Депонентов ООО «СДК «Гарант» и Клиентами Компании в процессе осуществления депозитарной деятельности.

СЭД Специализированного депозитария - отдельный функциональный блок СЭД ООО «СДК «Гарант», предназначенный для обеспечения обмена электронными документами между Департаментом спецдепозитарных услуг и Клиентами Компании в процессе осуществления деятельности специализированного депозитария.

СЭД Специализированного регистратора - отдельный функциональный блок СЭД ООО «СДК «Гарант», предназначенный для обеспечения обмена электронными документами между Отделом ведения реестров владельцев инвестиционных паев ПИФ и Клиентами Компании в процессе осуществления деятельности специализированного регистратора.

СЭД Негосударственный пенсионный фонд – Управляющая компания (дополнительный функционал) - отдельный функциональный блок СЭД ООО «СДК «Гарант», предназначенный для обеспечения обмена электронными документами между Негосударственным пенсионным фондом и Управляющей компанией, являющимися Клиентами ООО «СДК «Гарант».

Средства криптографической защиты информации (СКЗИ) – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи и/или шифрования, зашифрование/дешифрование электронных документов.

Уполномоченный представитель (уполномоченное лицо) – представитель Участника ЭДО, действующий в соответствии с Уставом или имеющий соответствующую доверенность.

Управление ключами и сертификатами ключей – создание (генерация) ключей и сертификатов ключей, их хранение, распространение, удаление (уничтожение), учет (ведение реестра), а также действия, необходимые для выполнения функций удостоверяющего центра в соответствии со статьей 9 Федерального закона от 10 января 2002 года №1-ФЗ «Об электронно-цифровой подписи».

Участник электронного документооборота (Участник ЭДО) – лицо, участвующее в электронном документообороте в качестве отправителя и/или получателя электронных документов и заключившее договор о присоединении к Правилам электронного документооборота ООО «СДК «Гарант».

Форматы электронных документов – Форматы электронных документов, используемых в СЭД ООО «СДК «Гарант», утвержденные Организатором СЭД.

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

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Электронно-цифровая подпись (ЭЦП) – неотъемлемая часть электронного документа, предназначенная для защиты данного электронного документа от подделки и являющаяся аналогом собственноручной подписи должностного лица или уполномоченного представителя юридического лица, представленная в электронно-цифровой форме, как результат криптографического преобразования информации с использованием закрытого (секретного) ключа электронно-цифровой подписи, который позволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронный документ (документ) – документ, в котором информация представлена в электронно-цифровой форме, а также:

- структура документа соответствует Форматам, утвержденным в СЭД ООО «СДК «Гарант»;
- документ подписан электронно-цифровой подписью;
- документ подготовлен и передан с помощью программного обеспечения Организатора СЭД/Участника ЭДО в соответствии со всеми процедурами защиты информации.

Электронный документооборот (ЭДО) – обмен электронными документами, в соответствии с настоящими Правилами, по каналам электросвязи или с помощью иных способов передачи документов в электронно-цифровой форме в процессе осуществления Организатором СЭД и Участниками ЭДО своей профессиональной деятельности.

3. ПОРЯДОК ДОПУСКА УЧАСТНИКА ЭДО К ОСУЩЕСТВЛЕНИЮ ДОКУМЕНТООБОРОТА В СЭД

3.1. Участник ЭДО и Организатор СЭД должны выполнить поэтапно следующие действия, необходимые для получения допуска к осуществлению ЭДО в СЭД:

- заключение договора с Организатором СЭД о присоединении к настоящим Правилам;
- установка Участником ЭДО выданного Организатором СЭД удаленного рабочего места, которое может состоять из аппаратных средств, клиентского программного и информационного обеспечения, а также СКЗИ на свои программно-технические средства;
- выполнение Администратором безопасности СЭД процедуры генерации криптографических ключей Участника ЭДО;
- изготовление Администратором безопасности СЭД сертификата ключа электронно-цифровой подписи для уполномоченного лица Участника ЭДО. Сертификат ключа выдается в форме документа на бумажном носителе, формируется в 2 (двух) экземплярах, которые заверяются собственноручными подписями уполномоченного лица Участника ЭДО и Администратора безопасности СЭД, а также печатью Организатора СЭД и печатью Участника ЭДО.

3.2. Перед началом обмена электронными документами в СЭД Организатор СЭД и Участник ЭДО обмениваются **Анкетами** (*Приложения №4,5 к настоящим Правилам*). В дальнейшем, в случае каких-либо изменений (изменение адресов электронной почты, замена или ввод в действие дополнительных ключей ЭЦП, изменение списка ответственных лиц, определенного Анкетами) одна Сторона предоставляет другой Стороне новую Анкету. При этом предыдущая Анкета теряет силу.

Перед началом осуществления электронного документооборота, а также в случае каких-либо изменений в отношении единоличного исполнительного органа или иного ответственного лица Участника ЭДО, Участник ЭДО обязан предоставить Организатору СЭД **Анкету представителя** (*Приложение № 5 к Условиям осуществления депозитарной деятельности ООО «СДК «Гарант» (Клиентский регламент)*).

Не предоставление информации об указанных выше ответственных лицах Участника ЭДО по вине последнего, исключает ответственность Организатора СЭД в случае возникновения конфликтных ситуаций.

3.3. Участник ЭДО из числа своих сотрудников назначает ответственных лиц, имеющих право работать с СКЗИ, с указанием их полномочий и срока действия этих полномочий. На каждое уполномоченное лицо Участник ЭДО предоставляет Организатору СЭД **Доверенность** (*Приложение №6 к настоящим Правилам*). В обязанности уполномоченного лица должны входить шифрование, постановка ЭЦП, передача документов (сообщений), прием документов (сообщений), расшифровка, проверка ЭЦП, хранение криптографических ключей.

3.4. Организатор СЭД и Участник ЭДО признают, что началом обмена электронными документами является дата подписания **Акта ввода в эксплуатацию электронного документооборота** (*Приложение №3 к настоящим Правилам*).

4. ОСОБЕННОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТА

4.1. Требования к электронному документу и порядок использования электронного документа

4.1.1. Электронный документ, сформированный в СЭД ООО «СДК «Гарант», имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в случае его надлежащего оформления в соответствии с настоящими Правилами.

4.1.2. Электронное сообщение приобретает статус электронного документа при его соответствии настоящим Правилам.

4.1.3. Электронный документ должен быть сформирован в одном из форматов, определенных в настоящих Правилах.

4.1.4. Все действия с электронными документами, оформленными, переданными и/или полученными в соответствии с настоящими Правилами признаются Участниками ЭДО действиями, совершенными в письменной форме и не могут быть оспорены только на том основании, что они совершены в электронном виде.

4.2. Порядок использования электронно-цифровой подписи и шифрования

4.2.1. Электронный документ должен быть подписан закрытым (секретным) ключом электронно-цифровой подписи, идентификатор которого указан в действующем сертификате и использование которого допускается в системе электронного документооборота Организатора СЭД.

4.2.2. Замена закрытых ключей электронно-цифровой подписи не влияет на юридическую силу электронного документа, если он был подписан действующим на момент подписания закрытым (секретным) ключом электронно-цифровой подписи в соответствии с настоящими Правилами.

4.2.3. Каждый Участник ЭДО должен иметь свой индивидуальный закрытый ключ электронно-цифровой подписи для подписания исходящих от него электронных документов.

4.2.4. Любой электронный документ, содержащий конфиденциальную информацию и пересылаемый по открытым каналам связи, должен быть зашифрован, при этом конфиденциальность электронного документа должна определяться его отправителем.

4.2.5. Полученный зашифрованный электронный документ должен быть расшифрован, после чего проводится проверка электронно-цифровой подписи.

4.2.6. Электронный документ принимается к дальнейшей обработке и исполнению только после положительного результата проверки электронно-цифровой подписи.

4.2.7. Участниками ЭДО используются СКЗИ, а также открытые и закрытые ключи и соответствующие сертификаты ключей, полученные от Организатора СЭД в установленном настоящими Правилами порядке.

4.3. Порядок признания подлинника электронного документа

4.3.1. Все экземпляры электронного документа, зафиксированные у Организатора СЭД и Участников ЭДО, являются подлинниками данного электронного документа.

4.3.2. Подлинником электронного документа считается документ с воспроизведенным содержанием и электронно-цифровой подписью.

4.3.3. Подлинник электронного документа не существует, если нет ни одного учтенного Организатором СЭД или Участником ЭДО экземпляра данного электронного документа.

4.3.4. Подлинник электронного документа не существует, если получение или восстановление экземпляра данного электронного документа невозможно.

4.3.5. Подлинник электронного документа не существует, если нет способа установить подлинность электронно-цифровой подписи.

4.3.6. Электронный документ не может иметь копий в электронном виде.

4.3.7. Электронный документ может иметь неограниченное количество экземпляров.

4.4. Порядок формирования копии электронного документа на бумажном носителе

4.4.1. Копии электронного документа на бумажном носителе должны быть заверены собственноручной подписью уполномоченного лица Участника ЭДО или Организатора СЭД.

4.4.2. Копии электронного документа на бумажном носителе должны содержать обязательную отметку, свидетельствующую о том, что это копия.

Отметкой, свидетельствующей о бумажной копии электронного документа, является, в том числе и графическое отображение электронной подписи.

4.4.3. Информация, содержащаяся в копии электронного документа на бумажном носителе, должна быть идентична информации, содержащейся в самом электронном документе.

5. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

5.1. Этапы электронного документооборота

5.1.1. Электронный документооборот включает в себя следующие этапы:

- формирование электронного документа;
- регистрация исходящего электронного документа;
- отправка электронного документа;
- доставка электронного документа;
- проверка целостности, подлинности и формата электронного документа;
- подтверждение получения электронного документа;
- отзыв электронного документа;
- регистрация входящего электронного документа;
- ведение архива электронных документов;
- создание дополнительных экземпляров электронного документа;
- создание бумажных копий электронного документа.

5.2. Порядок формирования электронного документа и его регистрации

5.2.1. Электронный документ формируется в установленном Организатором СЭД для данного электронного документа формате.

5.2.2. Сформированный электронный документ зашифровывается и подписывается электронно-цифровой подписью отправителя (Участника/Организатора СЭД).

5.2.3. В СЭД регистрируются все электронные документы, принятые сервером СЭД. При регистрации электронного документа происходит присвоение этому документу уникального номера (входящего или исходящего, в зависимости от типа электронного документа), а также сохраняются дата и время поступления этого документа на сервер СЭД.

5.3. Порядок отправки и доставки электронного документа

5.3.1. Электронный документ отправляется отправителем или лицом, уполномоченным на это отправителем.

5.3.2. Отправитель должен присвоить отправляемому электронному документу уникальный исходящий номер. При отсутствии исходящего номера документа, он может быть сформирован приложениями СЭД автоматически.

5.3.3. Электронный документ не считается отправленным/полученным, если получатель знал или должен был знать, что электронный документ не исходит от отправителя (уполномоченного им лица).

5.3.4. Электронный документ не считается отправленным/полученным, если получатель знал или должен был знать, что им получен искаженный электронный документ.

5.3.5. Порядок отправки и доставки электронного документа Участником ЭДО Организатору СЭД

5.3.5.1. Участник ЭДО посредством специального приложения из состава клиентского рабочего места СЭД вносит электронные документы, предназначенные для отправки Организатору СЭД, в базу данных клиентского рабочего места СЭД. Клиентское рабочее место СЭД с базой данных размещается на стороне Участника ЭДО. Далее посредством коммуникационного приложения из состава клиентского рабочего места СЭД Участник ЭДО отправляет эти электронные документы на сервер Организатора СЭД.

5.3.5.2. Участник ЭДО должен присвоить отправляемому Организатору СЭД электронному документу уникальный исходящий номер.

5.3.5.3. Отправка электронного документа осуществляется коммуникационным приложением из состава клиентского рабочего места с использованием транспортного протокола HTTP.

5.3.5.4. Участник ЭДО посредством коммуникационного приложения из состава клиентского рабочего места самостоятельно контролирует доставку отправленного электронного документа Организатору СЭД.

5.3.5.5. После отправки электронного документа Участник ЭДО обязан удостовериться в отсутствии сбоев при доставке. В случае сбоя при доставке электронного документа, например, в случае нарушения связи или возникновения проблем с расшифровкой электронного документа на стороне Организатора СЭД, в коммуникационном приложении из состава клиентского рабочего места выдаются сообщения о сбоях доставки. В этом случае электронный документ не считается отправленным и не попадает в базу данных Организатора СЭД, а Участник ЭДО должен повторить процедуру подготовки и/или отправки электронного документа.

5.3.5.6. Каждому электронному документу, отправленному Участником ЭДО и принятому Организатором СЭД, Организатор СЭД присваивает уникальный входящий номер, фиксирует дату и время его получения, которые передаются Участнику ЭДО и сохраняются в базе данных клиентского рабочего места Участника ЭДО. При этом такой электронный документ в базе данных клиентского рабочего места Участника ЭДО получает статус «отправлен».

5.3.5.7 Моментом получения электронного документа Организатором СЭД считается фиксация даты и времени получения Участником ЭДО служебного информационного документа с подтверждением о поступлении электронного документа Организатору СЭД в базе данных клиентского рабочего места Участника ЭДО, в Журнале учета исходящих документов, в поле «дата/время исходящее».

Электронный документ считается полученным или представленным с момента получения Участником ЭДО служебного информационного документа с подтверждением о поступлении электронного документа Организатору СЭД.

5.3.5.8. В случае невозможности использования СЭД по причине отказа компьютерного оборудования и (или) программного обеспечения, повреждений линий связи, ведущих к технической невозможности использования электронных документов, Участник ЭДО передает документы Организатору СЭД в бумажном виде, до устранения технической невозможности использования электронных документов. При возникновении технической невозможности использования СЭД Участник ЭДО обязан уведомить об этом Организатора ЭДО.

5.3.6. Порядок отправки и доставки электронного документа Организатором СЭД Участнику ЭДО

5.3.6.1. Электронные документы, предназначенные для получения Участником ЭДО, находятся на сервере Организатора СЭД.

5.3.6.2. Участник ЭДО посредством коммуникационного приложения из состава клиентского рабочего места самостоятельно проверяет наличие на сервере Организатора СЭД, предназначенных для него документов. При их наличии в коммуникационном приложении будет отображен список этих документов.

При наличии документов, предназначенных для получения Участником ЭДО, Участник ЭДО самостоятельно посредством коммуникационного приложения из состава клиентского рабочего места переносит электронные документы в базу данных своего клиентского рабочего места.

5.3.6.3. У Участника ЭДО полученные документы расшифровываются, проверяется их электронно-цифровая подпись. После завершения расшифровки и проверки электронно-цифровой подписи принятые документы разбираются и сохраняются в базе данных клиентского рабочего места на стороне Участника ЭДО.

5.3.6.4. Участник ЭДО посредством коммуникационного приложения самостоятельно контролирует процесс получения электронных документов от Организатора СЭД. Никаких документарных подтверждений от Организатора СЭД не требуется.

5.3.6.5. После получения электронного документа Участник ЭДО должен удостовериться в отсутствии сбоев при его получении. В случае успешного получения Участником ЭДО электронного документа, этот документ удаляется из списка документов, готовых к получению Участником ЭДО.

5.3.6.6. Моментом получения электронного документа Участником ЭДО считается фиксация даты и времени получения Организатором СЭД служебного информационного сообщения с подтверждением о поступлении электронного документа Участнику ЭДО. что подтверждает соответствующая запись в Журнале учета исходящих электронных документов СЭД, в поле «дата/время входящее». При отсутствии такой записи считается, что документ в СЭД не поступал.

Электронный документ считается полученным или представленным с момента получения Организатором СЭД служебного информационного документа с подтверждением о поступлении электронного документа Участнику ЭДО.

5.3.6.7. В случае невозможности использования СЭД по причине отказа компьютерного оборудования и (или) программного обеспечения, повреждений линий связи, ведущих к технической невозможности использования электронных документов, Организатор СЭД передает документы Участнику ЭДО в бумажном виде, до устранения технической невозможности использования электронных документов. При возникновении технической невозможности использования СЭД Организатор СЭД обязан уведомить об этом Участника ЭДО.

5.3.7. Порядок отправки и доставки электронного документа между Участниками ЭДО.

5.3.7.1. Участники ЭДО могут обмениваться между собой электронными документами. Отправитель электронного документа формирует электронный документ, предназначенный для отправки Получателю электронного документа. Подготовленный к отправке электронный документ сохраняется на рабочем месте Отправителя в виде файла.

5.3.7.2. Отправка электронного документа осуществляется путем направления Получателю электронного сообщения с вложением – файлом, содержащим электронный документ, и с использованием системы защищенной электронной почты «Курьер».

5.3.7.3. При открытии электронного сообщения Получателем, успешной расшифровки и проверки электронно-цифровой подписи система защищенной электронной почты «Курьер» автоматически отправляет в адрес Отправителя защищенное информационное сообщение, подтверждающее получение электронного сообщения, содержащего файл с электронным документом. Получение Отправителем защищенного информационного сообщения является подтверждением получения Получателем отправленного электронного сообщения, содержащего файл с электронным документом.

5.3.7.4. Участник ЭДО – Отправитель самостоятельно контролирует доставку электронного сообщения Получателю. Во время и после отправки электронного сообщения, содержащего файл с электронным документом, Участник ЭДО - Отправитель обязан удостовериться в отсутствии сбоев при отправке электронного сообщения.

5.3.7.5. Участник ЭДО должен хранить все полученные и отправленные электронные сообщения с файлом, содержащим электронный документ, а также все полученные и отправленные защищенные информационные сообщения, подтверждающие доставку документа. Участник ЭДО должен принять меры по ежедневному резервному копированию и архивному хранению полученных и отправленных электронных сообщений с файлом, содержащим электронный документ, а также полученных и отправленных защищенных квитанций.

5.3.7.6. Моментом получения электронного документа считается получение Отправителем подтверждения о поступлении электронного документа Получателю, которое является защищенным информационным сообщением.

5.4. Порядок проверки электронного документа на целостность, подлинность и соответствие установленным форматам

5.4.1. Полученный электронный документ проверяется на целостность, т.е. его доставку в неискаженном (по отношению к первоначальному) виде, путем расшифрования и обязательной проверки электронно-цифровой подписи.

5.4.2. Полученный электронный документ проверяется на соответствие установленному для него формату.

5.4.3. Получатель производит расшифровку полученных электронных документов и проверку их электронно-цифровой подписи. После завершения расшифровки и проверки электронно-цифровой подписи принятые электронные документы разбираются и сохраняются в базе данных Получателя.

5.4.4. Электронный документ подлежит дальнейшей обработке и исполнению только в случае положительного результата проверки целостности электронного документа и его соответствия установленному формату и подлинности электронно-цифровой подписи.

5.4.5. В случае невозможности расшифрования электронного документа, а также при отрицательном результате проверки целостности электронного документа и подлинности электронно-цифровой подписи электронный документ считается не полученным и не подлежит дальнейшей обработке и исполнению. В этом случае при использовании СЭД между Организатором СЭД и Участником ЭДО Отправителю в коммуникационном приложении из состава клиентского рабочего места Участника ЭДО выдается сообщение об ошибке при доставке. В случае использования СЭД для обмена электронными документами между Участниками ЭДО Отправителю будет доставлено

информационное сообщение, содержащее отрицательный результат расшифрования и/или проверки электронно-цифровой подписи.

5.5. Порядок подтверждения получения электронного документа при взаимодействии Участников ЭДО

5.5.1. Подтверждением получения электронного документа Участником ЭДО, считается наличие у Отправителя защищенного информационного сообщения о доставке отправленного электронного сообщения Получателю, содержащего файл с электронным документом.

5.5.2. Электронный документ считается не полученным Участником ЭДО, если у Отправителя отсутствуют защищенное информационное сообщение о доставке отправленного электронного сообщения, содержащего файл с электронным документом Получателю.

5.6. Порядок отзыва электронного документа при взаимодействии Организатора СЭД и Участника ЭДО

5.6.1. Отправитель имеет право отозвать отправленный электронный документ путем отправки получателю электронного документа «Отзыв операции», при его обработке в системе происходит проверка этапа, на котором находится операция.

5.6.2. Если в соответствии с логикой работы «Отзыв операции» возможен, то на стороне контрагента прекращается обработка отзываемого электронного документа и генерируется документ «Подтверждение отзыва», который затем отправляется получателю.

5.6.3. Если в соответствии с логикой работы «Отзыв операции» не возможен, то создается документ «Отказ на отзыв», оповещающий сторону, приславшую «Отзыв операции», о том, что операция уже не может быть отозвана.

5.7. Порядок учета электронных документов при взаимодействии Организатора СЭД и Участника ЭДО

5.7.1. Организатор СЭД осуществляет учет электронных документов путем ведения Журнала учета входящих электронных документов и Журнала учета исходящих электронных документов. Ведение учетных журналов осуществляется с использованием электронной базы данных с возможностью их формирования на бумажных носителях. Программные средства ведения журналов учета являются составной частью программного обеспечения Организатора СЭД.

5.7.2. Запись в Журнале учета входящих электронных документов должна содержать:

- уникальный входящий номер электронного документа;
- дата и время получения электронного документа сервером СЭД;
- наименование документа;
- исходящий номер полученного электронного документа;
- идентификатор отправителя электронного документа;
- входящий номер уведомления об отзыве (в случае отзыва).

5.7.3. Запись в Журнале учета исходящих электронных документов должна содержать:

- уникальный исходящий номер электронного документа;
- наименование документа;
- идентификатор отправителя электронного документа;
- идентификатор получателя электронного документа;

- дата и время получения электронного документа сервером СЭД;
- исходящий номер уведомления об отзыве (в случае отзыва).

5.7.4. Организатор СЭД и Участники ЭДО обеспечивают защиту от несанкционированного доступа и непреднамеренного уничтожения учетных данных, содержащихся в журналах учета электронных документов.

5.8. Порядок учета электронных документов при взаимодействии Участников ЭДО

5.8.1. Участники ЭДО осуществляют учет электронных документов путем ведения архива электронных документов и информационных сообщений.

5.8.2. Участники ЭДО обеспечивают защиту от несанкционированного доступа и непреднамеренного уничтожения учетных данных, содержащихся в архивах электронных документов и информационных сообщений.

5.9. Порядок ведения архива электронных документов

5.9.1. Все электронные документы, сформированные, отправленные и полученные Участниками ЭДО, хранятся в течение сроков, установленных действующим законодательством для соответствующих документов в бумажном виде. Электронные документы, для которых законодательством не установлены сроки их хранения, хранятся в течение 3 (трёх) лет.

5.9.2. Электронные документы должны храниться в формате, в котором они были получены.

5.9.3. Хранение электронных документов сопровождается хранением сертификатов ключей электронно-цифровой подписи.

5.9.4. Закрытые ключи шифрования хранятся у их владельцев в соответствующем электронном архиве в случае хранения электронных документов в зашифрованном виде.

5.9.5. При ведении архива электронных документов реализуются принципы ежедневного резервного копирования и восстановления электронных документов.

5.9.6. Ведение соответствующих архивов электронных документов осуществляется Участниками ЭДО и Организатором СЭД.

5.9.7. Организатор СЭД и Участники ЭДО должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения архивных данных.

6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В СЭД ООО «СДК «Гарант»

6.1. Общие положения

6.1.1. В СЭД ООО «СДК «Гарант» используются только сертифицированные ФСБ средства криптографической защиты информации (СКЗИ).

6.1.2. После подписания Участником ЭДО договора о присоединении к настоящим Правилам Организатор СЭД передает ему с правом использования только в СЭД ООО «СДК «Гарант» программное обеспечение СКЗИ, а также обеспечивает ключевой информацией, необходимой для работы.

6.1.3. Для обеспечения криптографической защиты информации в СЭД используются СКЗИ с открытым распределением ключей. При этом каждый Участник ЭДО имеет свои закрытые ключи шифрования и электронно-цифровой подписи, а также соответствующие им открытые ключи шифрования и электронно-цифровой подписи, которые не являются секретными и передаются другим участникам информационного обмена. При формировании закрытого ключа (как шифрования, так и электронно-цифровой подписи) с помощью специализированного программного обеспечения

одновременно формируются соответствующие им открытые ключи, и, кроме того, производится распечатка сертификата ключа электронной подписи. Подписанный руководителем и заверенный печатью Участника ЭДО сертификат является документом, который подтверждает принадлежность ключа электронно-цифровой подписи или шифрования Участнику ЭДО. Один экземпляр сертификата хранится у Администратора безопасности СЭД.

6.1.4. Для шифрования информации Отправителю необходим его собственный закрытый ключ и открытый ключ Получателя информации. Для цифровой подписи документа необходим только собственный закрытый ключ подписи. Для расшифрования информации Получателем используется открытый ключ Отправителя и собственный закрытый ключ Получателя. Для проверки подписи документа необходим только открытый ключ Отправителя.

6.1.5. Реализованные в СКЗИ алгоритмы шифрования и подписи гарантируют невозможность восстановления закрытых ключей шифрования и подписи Отправителя по его открытым ключам, что обеспечивает целостность, подлинность и конфиденциальность переданной Отправителем информации.

6.1.6. Закрытые ключи шифрования и подписи Участника ЭДО находятся только на носителях ключевой информации, передаваемых Участнику ЭДО.

6.1.7. При работе в СЭД каждый Участник ЭДО использует необходимое количество действующих комплектов криптографических ключей. В состав каждого комплекта входят открытый и закрытый ключи шифрования, открытый и закрытый ключи электронно-цифровой подписи.

6.1.8. Порядок работы с ключевыми носителями лиц, непосредственно работающих с СКЗИ, определяется самим Участником ЭДО.

6.1.9. Непосредственная генерация ключей и запись их на носители производится Администратором безопасности СЭД на АРМ Администратора безопасности СЭД. Программное обеспечение СКЗИ АРМ Администратора безопасности СЭД имеет сертификат ФСБ и обеспечивает невозможность несанкционированного получения Администратором безопасности СЭД копии формируемых закрытых ключей.

6.1.10. Участник ЭДО обязуется не делать копий с программного обеспечения СКЗИ;

6.1.11. По окончании срока действия договора о присоединении к настоящим Правилам или в случае его расторжения Участник ЭДО обязуется провести деинсталляцию установленного программного обеспечения СКЗИ.

6.2. Порядок предоставления СКЗИ

6.2.1. Для получения СКЗИ и криптографических ключей Участнику ЭДО необходимо:

- оформить и представить Организатору СЭД **Заявку на предоставление СКЗИ и формирование криптографических ключей** (*Приложение №7 к настоящим Правилам*). В Заявке указывается количество комплектов СКЗИ, необходимое количество комплектов криптографических ключей и USB-ключей для защиты программного продукта SeMa от нелегального использования и несанкционированного распространения, а также дистрибутива ПО SeMa;

- оформить **Доверенность на получении средств электронного документооборота** (*Приложение №13 к настоящим Правилам*).

6.2.2. Уполномоченный представитель Участника ЭДО в офисе Организатора СЭД на основании соответствующей доверенности получает программное обеспечение СКЗИ и носители с ключевой информацией.

6.2.3. Программное обеспечение СКЗИ передается уполномоченному представителю Участника ЭДО по **Акту передачи средств электронного документооборота** (*Приложение №8 к настоящим Правилам*).

6.2.4. Генерация криптографических ключей и запись на ключевые носители производятся Администратором безопасности СЭД.

6.2.5. Администратор безопасности СЭД регистрирует информацию о генерации ключей в Журнале учета и движения ключевых документов. Составляется **Акт формирования и передачи криптографических ключей** (*Приложение №9 к настоящим Правилам*).

6.2.6. Сертификация открытых ключей шифрования и подписи Участника ЭДО производится путем заверения **Сертификата ключа электронной подписи** личной подписью руководителя и печатью Участника ЭДО.

6.2.7. Участнику ЭДО передаются:

- комплект (рабочий и резервная копия) открытых и секретных криптографических ключей Участника ЭДО;
- сертификат ключа электронной подписи Участника ЭДО, подписанный Администратором безопасности СЭД;
- носители информации с дистрибутивами программного обеспечения СКЗИ;
- необходимая документация (в электронной форме);
- дистрибутив ПО SeMa;
- USB-ключ для защиты программного продукта SeMa от нелегального использования и несанкционированного распространения

6.2.8. Ключевые носители передаются уполномоченному представителю Участника ЭДО в опечатанных конвертах.

6.2.9. Со дня передачи СКЗИ Участник ЭДО обязан:

- осуществить инсталляцию и проверку работоспособности СКЗИ на предоставленных ему ключевых носителях;
- произвести сверку параметров выданных ключей с данными, указанными в сертификатах ключей, подписать сертификаты ключей и заверить их печатью Участника ЭДО.
- подписать Акт передачи СКЗИ;
- представить Организатору СЭД один экземпляр заверенных сертификатов и один экземпляр Акта передачи СКЗИ.

6.3. Плановая смена ключей в СЭД

6.3.1. Плановая смена криптографических ключей в СЭД производится один раз в год, поэтому срок действия для ключей шифрования и подписи при генерации устанавливается равным одному году. Срок действия криптографических ключей Участника ЭДО при первой генерации определяется Организатором СЭД и может составлять менее или более одного года до даты плановой смены криптографических ключей, определенной Организатором СЭД.

6.3.2. О дате проведения плановой смены криптографических ключей Организатор СЭД уведомляет Участников ЭДО путем направления электронного сообщения не позднее, чем за 10 (десять) рабочих дней, а также путем опубликования этой информации в сети Internet на официальной странице ООО «СДК «Гарант» - www.sdkgarant.ru. Отправка такого электронного сообщения осуществляется по электронному адресу, указанному Участником ЭДО в Анкете Участника ЭДО.

6.3.3. Старые ключевые носители и файлы с ранее действовавшими открытыми ключами должны сохраняться Участником ЭДО для обеспечения возможности доступа к локальным архивам и проведения процедуры разбора конфликтных ситуаций.

6.3.4. Формирование и выдача Участнику ЭДО новых комплектов криптографических ключей осуществляется Организатором СЭД в следующем порядке:

- Участник ЭДО должен направить Организатору СЭД **Заявку на предоставление СКЗИ и формирование криптографических ключей** (*Приложение №7 к настоящим Правилам*);
- после получения Заявки Организатор СЭД согласовывает с Участником ЭДО дату и время получения нового комплекта ключей. После этого уполномоченный представитель Участника ЭДО прибывает в офис Организатора СЭД, предъявляет доверенность на получение ключей, и Организатор СЭД производит выдачу нового комплекта ключей;
- порядок получения Участником ЭДО ключевых носителей аналогичен порядку, изложенному в пп.6.2.4.-6.2.8. настоящего документа, за следующими исключениями:

Участнику ЭДО передаются:

- новый комплект (рабочий и резервная копия) открытых и секретных криптографических ключей Участника ЭДО;
- сертификат ключа электронной подписи Участника ЭДО, подписанный Администратором безопасности СЭД;

6.3.5. Со дня получения ключевых носителей и открытых ключей Участник ЭДО обязан:

- включить новые ключи в свои справочники открытых ключей;
- произвести сверку параметров новых ключей с данными, указанными в сертификатах ключей;
- подписать сертификаты ключей, заверить их печатью и вернуть один экземпляр Организатору СЭД.

6.4. Порядок расчетов при оказании услуг по обеспечению криптографической защиты информации

6.4.1. Стоимость услуг, предоставляемых Организатором СЭД, определяется в соответствии с тарифами, указанными в *Приложении №10 к настоящим Правилам*.

6.4.2. Оплата услуг производится путем перечисления предоплаты в размере 100 (ста) процентов стоимости услуг на расчетный счет Организатора СЭД.

6.4.3. Организатор СЭД на основании Заявки на предоставление СКЗИ и формирование криптографических ключей выставляет Участнику ЭДО счет на оплату услуг.

6.4.4. Участник ЭДО оплачивает счет не позднее 5 (пяти) рабочих дней со дня его получения.

6.4.5. Тарифы на услуги Организатора СЭД подлежат пересмотру при изменении цен и тарифов на материальные ресурсы. Об изменении тарифов Организатор СЭД уведомляет Участников ЭДО путем направления электронного сообщения не позднее, чем за 5 (пять) рабочих дней, а также путем опубликования этой информации в сети Internet на официальной странице ООО «СДК «Гарант» - www.sdkgarant.ru. Отправка такого электронного сообщения осуществляется по электронному адресу, указанному Участником ЭДО в Анкете Участника ЭДО.

6.4.6. Все взаиморасчеты производятся в рублях.

7. ПОРЯДОК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОБЩИЕ ТРЕБОВАНИЯ К РЕЖИМУ ЭКСПЛУАТАЦИИ СКЗИ

7.1. Система обеспечения информационной безопасности при взаимодействии Организатора СЭД и Участника ЭДО

7.1.1. С целью защиты информации Организатор СЭД и Участники ЭДО принимают к использованию для осуществления электронной передачи документов в СЭД ООО «СДК «Гарант» СКЗИ «Верба-OW» («Верба-О»), сертифицированное ФСБ. Для выполнения процедуры постановки/снятия/проверки электронно-цифровой подписи и шифрования/дешифрования электронных документов используется система защиты HTTP-протокола «Корвет-В» производства ООО «Валидата» (далее именуется система «Корвет-В».)

7.1.2. Система Корвет-В предназначена для создания защищенных корпоративных прикладных систем, базирующихся на Web-технологиях, и обеспечивает конфиденциальность и целостность информации, передаваемой между браузером и Web-сервером по открытым IP-сетям, а также аутентификацию взаимодействующих сторон и защиту от несанкционированных повторов ранее переданной в канале информации.

В основе системы Корвет-В лежит технология Клиент – Сервер.

7.1.3. В системе Корвет-В клиент взаимодействует с сервером по специальному защищенному протоколу - HTTP-secure tunnel, который в момент установления соединения клиента с сервером осуществляет двустороннюю криптографическую аутентификацию и вырабатывает сеансовый ключ шифрования. Протокол HTTP-secure tunnel инкапсулирует в себя протокол HTTP, шифруя при этом весь трафик. Кроме того, целостность данных, передаваемых с помощью протокола HTTP-secure tunnel, защищена имитовставкой.

Встроенный в систему механизм двусторонней криптографической аутентификации служит для установления подлинности как клиента, так и для того, чтобы клиент мог удостовериться в подлинности сервера в момент установления соединения.

7.1.4. Организатор СЭД и Участники ЭДО осуществляют защиту информации, содержащей персональные данные и конфиденциальную информацию в СЭД.

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

- целостность и криптографическую защиту информации;
- защиту информации от несанкционированного доступа.

7.1.7. Система обеспечения информационной безопасности реализуется посредством применения аппаратно-программных средств и организационных мер.

7.1.7. К аппаратно-программным средствам относятся:

- программные средства, специально разработанные для осуществления электронного документооборота;
- средства аутентификации и разграничения доступа;
- СКЗИ;
- средства обеспечения безотказной работы, включая антивирусные средства.

7.1.8. К организационным мерам относятся:

- размещение аппаратно-программных средств в помещении с контролируемым доступом;
- административные ограничения доступа к этим средствам;
- допуск только специально обученных и уполномоченных лиц;
- защита от повреждающих внешних воздействий (пожар и т.п.).

7.1.9. С целью защиты информации, при взаимодействии между Отделом ведения реестров владельцев инвестиционных паев ПИФ и номинальным держателем в процессе осуществления деятельности Специализированного регистратора, используется программное обеспечение, описанное в пункте 7.2.

7. 2. Система обеспечения информационной безопасности при взаимодействии Участников ЭДО

7.2.1. С целью защиты информации Участники ЭДО принимают к использованию для осуществления электронной передачи документов в СЭД ООО «СДК «Гарант» СКЗИ «Верба-OW» («Верба-О»), сертифицированное ФСБ. Для выполнения процедуры постановки/снятия/проверки электронно-цифровой подписи и шифрования/дешифрования электронных документов при взаимодействии используется система защиты электронной почты «Курьер» производства ООО «Валидата» (далее именуется система «Курьер»).

7.2.2. Система «Курьер» предназначена для создания конфиденциальной и авторизованной переписки между абонентами и основывается на применении программ электронной почты компании Microsoft (Outlook)/ IBM(Lotus Notes).

7.2.3. Система «Курьер» позволяет отправлять подписанные электронно-цифровой подписью подтверждения о доставке электронного сообщения.

7.2.4. Система «Курьер» позволяет накладывать электронно-цифровую подпись на создаваемые в почтовых клиентах Microsoft Outlook и Lotus Notes электронные сообщения и шифровать их. Вложенные файлы также подписываются электронно-цифровой подписью и шифруются вместе с электронным сообщением.

7.2.5. Участники ЭДО осуществляют защиту информации, содержащей персональные данные и конфиденциальную информацию в СЭД.

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

- целостность и криптографическую защиту информации;
- защиту информации от несанкционированного доступа.

7.2.7. Система обеспечения информационной безопасности реализуется посредством применения аппаратно-программных средств и организационных мер.

7.2.8. К аппаратно-программным средствам относятся:

- программные средства, специально разработанные для осуществления электронного документооборота;
- средства аутентификации и разграничения доступа;
- СКЗИ;
- средства обеспечения безотказной работы, включая антивирусные средства.

7.2.9. К организационным мерам относятся:

- размещение аппаратно-программных средств в помещении с контролируемым доступом;
- административные ограничения доступа к этим средствам;
- допуск только специально обученных и уполномоченных лиц;
- защита от повреждающих внешних воздействий (пожар и т.п.).

7.3. Общие требования к режиму эксплуатации СКЗИ

7.3.1. Требования по организационному обеспечению безопасности СКЗИ:

- руководством организации должны быть выделены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ;
- вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утвержденных руководством организации с учетом эксплуатационной документации на СКЗИ;
- в организациях должны быть созданы условия, обеспечивающие сохранность конфиденциальной информации, обрабатываемой с помощью СКЗИ, а также ключевой информации.

7.3.2. Требования по размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены СКЗИ:

- размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее именуются помещения), должны обеспечивать безопасность информации, СКЗИ и криптографических ключей, сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами;
- порядок допуска в помещения должен определяться внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации;
- при расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь прочные входные двери, на которые устанавливаются надежные замки;
- криптографические ключи, инсталляционные дискеты СКЗИ и эксплуатационная документация должна храниться в металлических шкафах (хранилищах, сейфах), оборудованных внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством организации;
- устанавливаемый руководством организации порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны;
- размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ;
- системные блоки ПЭВМ с СКЗИ должны быть оборудованы средствами контроля их вскрытия.

7.3.3. Требования по обеспечению безопасности криптографических ключей:

- учет и хранение носителей криптографических ключей и инсталляционных дискет, непосредственная работа с ними поручается руководством организации специально выделенному работнику. Этот работник несет персональную ответственность за сохранность криптографических ключей;
- все поступающие для использования криптографические ключи и инсталляционные дискеты должны браться в организации на поэкземплярный учет в выделенных для этих целей журналах;
- в организации должен вестись учет криптографических ключей, регистрация их выдачи сотрудникам для работы, возврата и уничтожения;
- хранение криптографических ключей, инсталляционных дискет допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение. Наряду с этим должна быть предусмотрена возможность безопасного отдельного хранения рабочих и резервных криптографических ключей;
- при доставке криптографических ключей в организацию должны быть обеспечены условия транспортировки, исключающие возможность физических повреждений и внешнего воздействия на записанную ключевую информацию;
- в случае отсутствия у сотрудника, работающего с СКЗИ, индивидуального хранилища криптографические ключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение;

- уполномоченными лицами периодически должен проводиться контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов;
- закрытые ключи владельцев сертификатов ключей записываются при их генерации на отчуждаемые носители ключевой информации;
- в качестве отчуждаемых носителей ключевой информации используются только носители, указанные в документации на СКЗИ;
- после использования СКЗИ ключевой материал не должен присутствовать в ПЭВМ;
- вне процесса работы ключевые носители информации находятся в специально оборудованных металлических шкафах или сейфах;
- хранение ключевых носителей допускается в одном хранилище с другими документами в условиях, исключающих их непреднамеренное уничтожение.

7.3.4. Требования к сотрудникам, осуществляющим эксплуатацию и установку (инсталляцию) СКЗИ:

- к работе с СКЗИ допускаются решением руководства организации только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ;
- руководитель организации или уполномоченное им лицо должен иметь представление о возможных угрозах при обработке, передаче и хранении информации, методах и средствах защиты информации.

7.4. Порядок действий при компрометации криптографических ключей

7.4.1. Порядок действий Сторон при компрометации ключей Участника ЭДО

7.4.1.1. При компрометации криптографических ключей Участник ЭДО, являющийся владельцем сертификатов ключей, прекращает обмен электронными документами с использованием скомпрометированных ключей. При получении достоверной информации о смене единоличного исполнительного органа Участника ЭДО, Организатор СЭД вправе при не предоставлении Участником ЭДО необходимого комплекта документов осуществить блокировку криптографического ключа, выданного ранее Администратором безопасности СЭД единоличному исполнительному органу Участника ЭДО, в течение дня, следующего за днем получения информации.

7.4.1.2. В случае возникновения компрометации криптографических ключей Участник ЭДО обязан незамедлительно уведомить об этом Администратора безопасности СЭД, чтобы он осуществил блокировку скомпрометированных ключей. Для этого уполномоченное лицо Участника ЭДО, указанное в Анкете Участника ЭДО, должно связаться с Администратором безопасности СЭД (в случае его отсутствия - с лицом, замещающим Администратора безопасности СЭД) по телефонам, приведенным в **Карточке оповещения (Приложение №11 к настоящим Правилам)**, назвать себя, назвать полное наименование организации Участника ЭДО, сообщить пароль и сообщить о факте компрометации ключей. После этого Участник ЭДО обязан в течение одного рабочего дня предоставить Организатору СЭД письменное **Уведомление о факте компрометации криптографических ключей (Приложение №12 к настоящим Правилам)**.

7.4.1.3. Датой и временем компрометации криптографических ключей считается дата и время получения Организатором СЭД Уведомления о факте компрометации криптографических ключей.

7.4.1.4. При получении электронного документа, подписанного скомпрометированным ключом электронно-цифровой подписи данный электронный документ считается неполученным.

7.4.1.5. Получив сообщение о факте компрометации криптографических ключей Участника ЭДО, Администратор безопасности СЭД должен убедиться в его достоверности в соответствии с пунктом 7.4.1.2. и незамедлительно заблокировать ключи Участника ЭДО в СЭД (пометить их как скомпрометированные).

7.4.1.6. Организатор СЭД предоставляет Участнику ЭДО новый комплект криптографических ключей (шифрования и электронно-цифровой подписи) в течение 2 (двух) рабочих дней, следующих за днем получения письменного уведомления от Участника ЭДО о факте компрометации ключей. Участник ЭДО обязан оплатить стоимость нового комплекта ключей в соответствии с действующими на этот момент тарифами Организатора СЭД.

7.4.2. Порядок действий Сторон при компрометации ключей Организатора СЭД

7.4.2.1. В случае компрометации криптографических ключей Организатора СЭД работа СЭД приостанавливается на срок, необходимый для формирования новых криптографических ключей Организатора СЭД и выдачи Участникам ЭДО новых комплектов криптографических ключей.

7.4.2.2. Оповещение Участников ЭДО производится путем опубликования информации в сети Internet на официальной странице ООО «СДК «Гарант» - www.sdkgarant.ru либо путем уведомления уполномоченных лиц Участников ЭДО, указанных в Анкетах, по телефону. При оповещении Участников ЭДО по телефону Администратор безопасности СЭД должен назвать свой пароль, а Участник ЭДО должен сверить его с паролем Администратора безопасности СЭД, записанным в Карточке оповещения.

7.4.2.3. В случае компрометации ключей Организатора СЭД новые комплекты криптографических ключей (шифрования и электронно-цифровой подписи) предоставляются Участникам ЭДО на безвозмездной основе.

8. СИСТЕМА МЕР УПРАВЛЕНИЯ РИСКАМИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

8.1. Виды рисков, связанных с осуществлением ЭДО в рамках СЭД ООО «СДК «Гарант»

8.1.1. Правовые риски – риски возникновения конфликтных ситуаций, вызванных правовой неурегулированностью вопросов применения электронно-цифровой подписи и отношений Участников ЭДО.

8.1.2. Организационные риски – риски необеспечения (ненадлежащего обеспечения) ЭДО вследствие неэффективности СЭД.

8.1.3. Технологические риски – риски необеспечения (ненадлежащего обеспечения) порядка осуществления ЭДО вследствие неэффективности и/или неадекватности технологий, порядка и способов осуществления ЭДО.

8.1.4. Операционные риски – риски возникновения нарушений при осуществлении ЭДО вследствие ненадлежащих действий сотрудников, ненадлежащего функционирования используемых СКЗИ и иного аппаратно-программного обеспечения.

8.1.5. Криминальные риски – риски совершения сотрудниками Участников ЭДО, иными лицами, умышленных действий в целях неправомерного получения и

использования конфиденциальной информации, связанной с осуществлением ЭДО, а также нарушения деятельности Участников ЭДО.

8.1.6. Форс-мажорные риски – риски нарушения деятельности Участников ЭДО, целостности системы электронного документооборота, вследствие возникновения непредотвратимых (форс-мажорных) чрезвычайных ситуаций техногенного, природного и социального характера.

8.2. Меры снижения правовых рисков ЭДО, применяемые в СЭД (с указанием ответственной стороны)

8.2.1. Обеспечение соответствия СКЗИ, используемых при осуществлении ЭДО, требованиям законодательства Российской Федерации (Организатором СЭД).

8.2.2. Обеспечение признания Участниками ЭДО равнозначности электронной и письменной формы документов (Организатором СЭД).

8.2.3. Установление признаков подлинности и целостности электронного документа (Организатором СЭД).

8.2.4. Установление порядка разрешения конфликтов, связанных с использованием ЭДО (Организатором СЭД).

8.3. Меры снижения организационных рисков ЭДО, применяемые в СЭД (с указанием ответственной стороны)

8.3.1. Установление прав и обязанностей Участников ЭДО, связанных с осуществлением ЭДО (Организатором СЭД).

8.3.2. Установление функциональных обязанностей подразделений Организатора СЭД, принимающих участие в осуществлении ЭДО (Организатором СЭД).

8.4. Меры снижения технологических рисков ЭДО, применяемые в СЭД (с указанием ответственной стороны)

8.4.1. Установление требований к назначению и составу СКЗИ, используемых при осуществлении ЭДО (Организатором СЭД).

8.4.2. Обеспечение использования Участниками ЭДО СКЗИ при осуществлении ЭДО (Организатором СЭД).

8.4.3. Обеспечение однозначной идентификации владельца сертификата ключа, уникальности регистрационной информации о владельце сертификата ключа (Организатором СЭД).

8.4.4. Обеспечение Участниками ЭДО и Организатором СЭД целостности системы электронного документооборота, регистрации отправленных и полученных электронных документов, хранению сформированных, отправленных и полученных электронных документов.

8.4.5. Установление требований к порядку осуществления электронного документооборота Участниками ЭДО (Организатором СЭД).

8.4.6. Обеспечение исполнения требований к форматам и реквизитам электронного документа (Организатором СЭД).

8.4.7. Определение порядка действий Участников ЭДО (Организатором СЭД) по формированию, доставке электронного документа, а также его отзыву.

8.4.8. Определение порядка действий Участников ЭДО (Организатором СЭД) по проверке действительности и области действия электронно-цифровой подписи, подлинности, целостности электронного документа и его соответствия установленным форматам.

8.5. Меры снижения операционных рисков ЭДО, применяемые в СЭД

8.5.1. Разделение полномочий и служебных обязанностей сотрудников Участников ЭДО и Организатора СЭД, участвующих в осуществлении ЭДО.

8.5.2. Осуществление контроля за надлежащим исполнением сотрудниками Участников ЭДО и Организатора СЭД своих служебных обязанностей, связанных с осуществлением ЭДО.

8.5.3. Определение порядка выявления ошибок (ошибочных действий), совершенных сотрудниками Участников ЭДО и Организатора СЭД и порядка их устранения.

8.5.4. Установление квалификационных требований к сотрудникам (руководителям подразделений) Участников ЭДО и Организатора СЭД, участвующих в осуществлении ЭДО.

8.5.5. Определение порядка обнаружения и устранения отказов, сбоев, нарушений работы СКЗИ, используемых Участниками ЭДО при осуществлении ЭДО (Организатором СЭД).

8.6. Меры снижения криминальных рисков ЭДО, применяемые в СЭД (с указанием ответственной стороны)

8.6.1. Установление требований (Организатором СЭД) по обеспечению Участниками ЭДО защиты конфиденциальной информации, связанной с осуществлением ЭДО, от несанкционированного доступа.

8.6.2. Установление требований (Участником ЭДО) по обеспечению владельцами сертификатов ключей сохранности в тайне закрытых (секретных) ключей электронно-цифровой подписи.

8.6.3. Определение порядка действий владельцев сертификатов ключей (Организатором СЭД, Участниками ЭДО) в случае компрометации закрытых (секретных) ключей электронно-цифровой подписи.

8.6.4. Определение порядка (Организатором СЭД) расследования случаев неправомерного предоставления и/или использования конфиденциальной информации, неисполнения (ненадлежащего исполнения) своих служебных обязанностей сотрудниками Участников ЭДО и Организатора СЭД.

8.7. Меры снижения форс-мажорных рисков ЭДО, применяемые в СЭД

8.7.1. Обеспечение Участниками ЭДО и Организатором СЭД целостности ЭДО, защиты конфиденциальной информации, связанной с осуществлением ЭДО, в случае возникновения чрезвычайных ситуаций.

8.7.2. Определение порядка действий сотрудников Участников ЭДО и Организатора СЭД в случае возникновения чрезвычайных ситуаций.

8.7.3. Применение Участниками ЭДО и Организатором СЭД резервных источников питания, систем бесперебойного питания, средств безаварийного завершения работы.

8.7.4. Применение Участниками ЭДО и Организатором СЭД средств защиты от поражения компьютерными вирусами и вредоносными программами.

8.8. Компенсационные инструменты, применяемые для покрытия убытков от реализации рисков ЭДО

8.8.1. Собственные средства Участников ЭДО и Организатора СЭД.

8.8.2. Средства гарантийных/компенсационных/страховых фондов, сформированных в целях покрытия убытков от реализации рисков ЭДО, в которых принимают участие Участники ЭДО.*¹

8.8.3. Страхование ответственности Участников ЭДО (в т.ч. путем участия в обществах взаимного страхования Участников ЭДО), Организатора СЭД за причинение убытков третьим лицам при осуществлении ЭДО.

8.9. Управление рисками электронного документооборота

8.9.1. Подразделением, ответственным за управление рисками электронного документооборота, является отдел внутреннего контроля и аудита Организатора СЭД.

8.9.2. Основными функциями отдела внутреннего контроля и аудита в области управления рисками электронного документооборота являются:

- анализ текущей и планируемой деятельности Организатора СЭД с целью выявления новых рисков электронного документооборота, установление источников и причин их реализации, оценка последствий реализации выявленных рисков;
- контроль за практическим применением Организатором СЭД мер, препятствующих реализации рисков электронного документооборота;
- мониторинг событий, способных привести к реализации рисков электронного документооборота, анализ эффективности применяемых Организатором СЭД способов снижения рисков;
- расследование случаев реализации рисков электронного документооборота, установление причин несрабатывания, применяемых Организатором СЭД способов снижения рисков;
- оценка эффективности сформированных Организатором СЭД компенсационных инструментов, применяемых при покрытии убытков, в случае реализации рисков электронного документооборота;
- разработка предложений по повышению эффективности системы мер снижения рисков электронного документооборота.

9. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТОВ

9.1. Возникновение конфликтов

9.1.1. В случае возникновения конфликтов при использовании электронных документов в СЭД ООО «СДК «Гарант», в частности, спора между Участниками ЭДО в отношении авторства, подлинности или целостности электронных документов, подписанных электронно-цифровой подписью, применяется порядок разрешения конфликтов, предусмотренный настоящими Правилами.

9.1.2. При возникновении конфликта Участник ЭДО, оспаривающий авторство, подлинность или целостность электронного документа в СЭД ООО «СДК «Гарант», извещает Администратора безопасности СЭД об этом событии любым способом, позволяющим однозначно установить отправителя.

9.2. Согласительный порядок разрешения конфликтов

9.2.1. Все конфликтные ситуации, которые могут возникнуть в связи с применением, нарушением, толкованием настоящих Правил, признанием недействительными настоящих Правил или их части, Стороны будут стремиться

¹ В случае (и по мере) регламентации формирования таких фондов СРО

разрешить, используя механизмы согласительного урегулирования конфликтных ситуаций.

9.2.2. В случае, если конфликтная ситуация не урегулирована в процессе переговоров и конфликтная ситуация содержит признаки дисциплинарных нарушений, стороны обязаны обратиться в Дисциплинарный Комитет ПАРТАД, для разрешения конфликтной ситуации в соответствии с Кодексом мер дисциплинарного воздействия ПАРТАД.

9.3. Судебный порядок разрешения конфликтов

9.3.1. Все гражданские споры, которые могут возникнуть в связи с применением, нарушением, толкованием настоящих Правил, признанием недействительными настоящих Правил или их части, подлежат разрешению в Арбитражном суде г.Москвы.

10. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ НАСТОЯЩИХ ПРАВИЛ ДЛЯ ВСЕХ УЧАСТНИКОВ ЭДО

10.1. Настоящие Правила прекращают свое действие на основании решения исполнительного органа Организатора СЭД.

10.2. Прекращение действия настоящих Правил и приложений к ним не влияет на юридическую силу и действительность электронных документов, которыми Организатор СЭД и Участники ЭДО обменивались до прекращения действия настоящих Правил и приложений к ним.

11. ПРИЛОЖЕНИЯ

Приложение № 1	Договор о присоединении к Правилам ЭДО ООО «СДК «Гарант»
Приложение № 2	Форматы электронных документов, используемые в системе электронного документооборота ООО «СДК «Гарант»
Приложение № 3	Акт ввода в эксплуатацию электронного документооборота
Приложение № 4	Анкета Организатора СЭД
Приложение № 5	Анкета Участника ЭДО
Приложение № 6	Доверенность
Приложение № 7	Заявка на предоставление СКЗИ и формирование криптографических ключей
Приложение № 8	Акт передачи средств электронного документооборота
Приложение № 9	Акт формирования и передачи криптографических ключей
Приложение № 10	Стоимость подключения функциональных блоков СЭД ООО «СДК «Гарант» и тарифы на услуги по обеспечению криптографической защиты информации
Приложение № 11	Карточка оповещения
Приложение № 12	Уведомление о компрометации криптографических ключей
Приложение № 13	Доверенность на получение средств электронного документооборота