Приложение № 1
к Приказу № ОД-28
от 29.11.2019 г.

РЕГЛАМЕНТ
защищенного обмена информацией в электронной форме
в АО «НПФ Газпромбанк-фонд»

Оглавление

1. Общие положения

Настоящий Регламент определяет порядок организации защищенного обмена информацией в электронной форме между АО «НПФ Газпромбанк-фонд» (далее – Фонд) и участниками защищенного обмена информацией в электронной форме.

Настоящий Регламент разработан в соответствии с законодательством Российской Федерации, в том числе Гражданским Кодексом Российской Федерации, Федеральным Законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным Законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005), утверждённым Приказом ФСБ РФ от 09.02.2005 №66.

Защищенный обмен информацией в электронной форме между Фондом и участниками защищенного обмена информацией в электронной форме осуществляется в целях исполнения обязательств по договорам, заключенным между Фондом и соответствующими участниками защищенного обмена информацией в электронной форме, либо которые будут заключены между ними в будущем.

2. Основные понятия

В настоящем Регламенте используются следующие основные понятия и определения:

(1) ***Аккредитация удостоверяющего центра*** – признание федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

(2) ***Владелец сертификата ключа проверки электронной подписи*** – лицо, которому в установленном законодательством Российской Федерации порядке выдан сертификат ключа проверки электронной подписи.

(3) ***Защищенный обмен информацией в электронной форме (Защищенный обмен ИЭ)*** – процесс предоставления по каналам связи информации, защищенной с использованием средств криптографической защиты информации и средств электронной подписи.

(4) ***Информация в электронной форме (ИЭ)*** — для целей настоящего Регламента информация, в том числе документированная информация, представленная в электронной форме, пригодной для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-коммуникационным сетям или обработки в информационных системах.

(5) ***Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат)*** – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

(6) ***Ключевой носитель*** – носитель информации (eToken, ruToken, защищенные носители ключевой информации/криптографических ключей и др.), на котором хранятся криптографические ключи.

(7) ***Ключ проверки электронной подписи*** – уникальная последовательность символов, однозначно связанная с ключом электронной подписи, предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

(8) ***Ключ электронной подписи*** – уникальная последовательность символов, предназначенная для создания электронной подписи.

(9) ***Криптографические ключи*** – ключ электронной подписи и ключ проверки электронной подписи, связанные между собой особым математическим соотношением с помощью криптографических преобразований информации.

(10) ***Пользователь*** – лицо, являющееся владельцем сертификата ключа проверки электронной подписи и имеющее полномочия на ведение защищенного обмена информацией в электронной форме.

(11) ***Предоставление информации*** – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

(12) ***Сертификат ключа проверки электронной подписи*** — электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

(13) ***Средства криптографической защиты информации (СКЗИ)*** — аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

(14) ***Средства электронной подписи*** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

(15) ***Удостоверяющий центр*** – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством Российской Федерации.

(16) ***Участник защищенного обмена ИЭ*** – лицо, присоединившееся к настоящему Регламенту и осуществляющее защищенный обмен информацией в электронной форме в порядке, установленном настоящим Регламентом. К Участникам защищенного обмена ИЭ относятся: ПАО «Газпром», его дочерние общества и организации; иные физические и юридические лица.

(17) ***Шифрование информации*** – обратимое криптографическое преобразование информации с помощью средств криптографической защиты информации и криптографических ключей, обеспечивающее защиту информации от несанкционированного доступа.

(18) ***Электронная подпись (ЭП)*** — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

В случае противоречия в толковании отдельных понятий и определений, изложенных в настоящем Регламенте, нормативным актам действующего законодательства Российской Федерации, следует использовать понятия и определения соответствующих нормативных актов Российской Федерации.

3. Присоединение к Регламенту

Для присоединения к Регламенту защищенного обмена информацией в электронной форме в АО «НПФ Газпромбанк-фонд» (далее – Регламент) необходимо:

(1) заключить Соглашение об участии в защищенном обмене информацией в электронной форме, по форме в соответствии с Приложением № 1 к настоящему Регламенту;

(2) определить список Пользователей защищенного обмена ИЭ. Списки Пользователей, уполномоченных вести защищенный обмен ИЭ, определяются Фондом и Участниками защищенного обмена ИЭ в соответствии с Соглашением об участии в защищенном обмене информацией в электронной форме;

(3) на компьютере каждого Пользователя установить и настроить СКЗИ и средства электронной подписи в соответствии с требованиями, определенными гл. 5.3 настоящего Регламента;

(4) обеспечить каждого Пользователя криптографическими ключами и сертификатом ключа проверки электронной подписи в соответствии с требованиями, определенными гл. 5.3 настоящего Регламента.

4. Правила ведения защищенного обмена информацией в электронной форме

4.1 Формирование информации в электронной форме

Источниками для формирования ИЭ могут быть любые сведения, независимо от формы их представления, а также документированная информация, закрепленная на материальном носителе с реквизитами, позволяющими определить такую информацию.

При формировании ИЭ применяются средства вычислительной техники, в том числе средства преобразования документов на бумажном материальном носителе в электронную форму.

Передаваемая ИЭ при ведении защищенного обмена ИЭ представляется в виде файлов. В целях обеспечения корректного распознавания и последующего использования ИЭ Пользователем получающей стороны к файлам, содержащим ИЭ, предъявляются следующие требования:

- размер файла не должен превышать 5 Мб;
- не допускается использование исполняемых типов файлов (например: EXE, COM, PIF, SCR, JS).

В случае, если размер файла, содержащего ИЭ, превышает 5 Мб, необходимо использовать сжатие такого файла или его разделение на отдельные части с помощью средств архивирования.

4.2 Подготовка к обмену информацией в электронной форме

Для передачи файлов, содержащих ИЭ, при ведении защищенного обмена ИЭ Пользователь передающей стороны выполняет следующие действия:

(1) определяет Пользователя получающей стороны в соответствии со списком Пользователей;

(2) обменивается с Пользователем получающей стороны сертификатами ключа проверки электронной подписи любым доступным способом (если это не было сделано ранее);

(3) подписывает электронной подписью файл, сформированный в соответствии с гл. 4.1 Регламента, с помощью своего ключа электронной подписи;

(4) подписанный файл зашифровывает с помощью ключа проверки

электронной подписи Пользователя получающей стороны. В случае необходимости отправки подписанного файла нескольким Пользователям для шифрования должны использоваться ключи проверки электронной подписи всех указанных Пользователей.

Файл, содержащий ИЭ, подписанный электронной подписью, должен иметь расширение «P7S», зашифрованный файл должен иметь расширение «P7M». Подписанный и зашифрованный файл должен иметь двойное расширение «P7S.P7M». Изменение расширения файла выполняется автоматически при использовании средств электронной подписи и СКЗИ в порядке, определенном в гл.5 Регламента.

При подготовке ИЭ Пользователю передающей стороны следует убедиться в действительности собственного сертификата ключа проверки электронной подписи и сертификата ключа проверки электронной подписи Пользователя получающей стороны в порядке, определенном в гл.5.2 настоящего Регламента.

4.3 Обмен информацией в электронной форме

Защищенный обмен ИЭ осуществляется с помощью средств электронной почты. Фонд и Участники защищенного обмена ИЭ обеспечивают доставку сообщений электронной почты и обязуются незамедлительно при поступлении сообщений знакомиться с их содержанием.

Для отправки ИЭ Пользователь передающей стороны выполняет следующие действия:

(1) создает сообщение в электронной почте и добавляет в него в качестве вложения файл, сформированный в соответствии с гл.4.2 настоящего Регламента;

(2) сформированное сообщение направляет на адрес электронной почты Пользователя получающей стороны.

При получении сообщения электронной почты, направленного при ведении защищенного обмена ИЭ, Пользователь получающей стороны выполняет следующие действия:

(1) извлекает из сообщения электронной почты вложенный файл, содержащий ИЭ;

(2) расшифровывает файл, полученный в результате выполнения п.1 с помощью своего ключа электронной подписи (файл с расширением «P7S.P7M»);

(3) выполняет проверку ЭП, которой подписан файл, полученный в результате выполнения п.2 (файл с расширением «P7S»), в соответствии с гл.5.2 настоящего Регламента;

(4) после успешной проверки ЭП извлекает ИЭ из полученного файла.

4.4 Обмен уведомлениями

В целях информирования Пользователей Фонда и Участников защищенного обмена ИЭ о состоянии защищенного обмена ИЭ применяются следующие виды уведомлений:

(1) уведомление об отрицательных результатах проверки ЭП;

(2) уведомление о невозможности расшифровать файл, содержащий ИЭ;

(3) уведомление о невозможности ведения защищенного обмена ИЭ в случае:

– сбоя в работе средств электронной почты, СКЗИ, средств электронной подписи или иных средств;

– истечения срока действия сертификата ключа проверки электронной подписи;

– внесения изменений в список Пользователей, уполномоченных вести защищенный обмен ИЭ;

– компрометации ключа электронной подписи Пользователя, замены криптографических ключей и сертификата ключа проверки электронной подписи (плановая/внеплановая);

– ограничений при использовании сертификатов ключа проверки электронной подписи.

Срок отправки указанных уведомлений не должен превышать 1 (один) рабочий день со дня наступления обстоятельств соответствующего уведомления.

Уведомление должно включать следующую информацию:

– наименование стороны, отправляющей и получающей уведомление;

– дата и время отправки уведомления;

– вид уведомления;

– описание обстоятельств уведомления (если требуется).

Правила формирования, подготовки и обмена уведомлениями соответствуют правилам, установленным при защищенном обмене ИЭ, согласно гл. 4.1, 4.2 настоящего Регламента, без применения шифрования. При этом обеспечивается подписание уведомления ЭП.

При получении уведомления, согласно п.п.2-3 гл.4.4 настоящего Регламента, Фонд и Участники защищенного обмена ИЭ обязаны незамедлительно приостановить ведение защищенного обмена ИЭ и предпринять необходимые действия для выяснения обстоятельств соответствующего уведомления.

5. Обеспечение безопасности при ведении защищенного обмена информацией в электронной форме

Безопасность ИЭ при ведении защищенного обмена ИЭ, обеспечивается соблюдением следующих правил:

(1) Фонд и Участники защищенного обмена ИЭ применяют СКЗИ в соответствии с настоящим Регламентом и признают их достаточность для обеспечения защиты передаваемой ИЭ;

(2) Фонд и Участники защищенного обмена ИЭ применяют средства электронной подписи в порядке, установленном настоящим Регламентом, и признают, что:

– получение файлов, содержащих ИЭ, подписанных ЭП, является подтверждением того, что эти файлы отправлены Пользователем, их подписавшим;

– наличие положительного результата проверки ЭП на полученном файле является подтверждением целостности содержащейся в нем ИЭ (отсутствие модификации файла после его подписания);

(3) Фонд и Участники защищенного обмена ИЭ обязуются заблаговременно обновлять сертификаты ключей проверки электронной подписи;

(4) Фонд и Участники защищенного обмена ИЭ обязуются своевременно направлять друг другу уведомления и осуществлять необходимые действия при их получении в соответствии с требованиями гл.4.4 настоящего Регламента.

5.1 Допустимость использования криптографических ключей

Допустимость использования криптографических ключей при ведении защищенного обмена ИЭ определяется следующими условиями:

(1) сертификат ключа проверки электронной подписи может быть создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата (если иное не указано в гл.5.3 настоящего Регламента);

(2) имеется положительный результат проверки ЭП, которой подписан файл, содержащий ИЭ, на момент проведения указанной проверки Пользователем получающей стороны;

(3) в случае защищенного обмена ИЭ между Фондом и иными физическими и юридическими лицами необходимо использовать квалифицированные сертификаты, выданные аккредитованным удостоверяющим центром;

Пользователям в повседневной работе рекомендуется применять меры по обеспечению безопасности криптографических ключей, определенные в регламенте удостоверяющего центра, в котором был изготовлен их сертификат ключа проверки

электронной подписи, а также в Руководстве по использованию ключа электронной подписи, приведенном в Приложении № 2 к настоящему Регламенту.

5.2 Проверка электронной подписи

Проверка ЭП, которой подписан файл, содержащий ИЭ, передаваемый при ведении защищенного обмена ИЭ, включает:

(1) определение действительности сертификата ключа проверки электронной подписи;

(2) определение принадлежности ЭП, которой подписан файл, содержащий ИЭ, владельцу сертификата ключа проверки электронной подписи (проверка подлинности ЭП).

Проверка действительности и подлинности ЭП осуществляется автоматизировано с помощью средств электронной подписи. Для проверки необходимо руководствоваться эксплуатационной документацией соответствующего применяемого средства.

5.3 Требования к средствам криптографической защиты информации и электронной подписи

При ведении защищенного обмена ИЭ допускается передача файлов, содержащих ИЭ, подписанных электронной подписью и/или зашифрованных в формате PKCS#7 с применением штампа времени.

В качестве СКЗИ рекомендуется средство «КриптоПро CSP» (версии 4.0 или выше).

Порядок установки, настройки и эксплуатации СКЗИ «КриптоПро CSP» определяется производителем данного средства в сопроводительной документации к ним (http://www.cryptopro.ru/).

Порядок создания и применения криптографических ключей и сертификатов ключа проверки электронной подписи определяется удостоверяющими центрами в утвержденных ими регламентах.

Перечень аккредитованных удостоверяющих центров размещен на Интернет-ресурсе http://minsvyaz.ru/ru/activity/govservices/2/.

6. Конфиденциальность

При ведении защищенного обмена ИЭ Фонд и Участники защищенного обмена ИЭ могут передавать сведения, к которым законодательством Российской Федерации или обладателем таких сведений предъявляются требования по обеспечению их конфиденциальности (конфиденциальная информация).

Обязательства по обеспечению конфиденциальности ИЭ, передаваемой при ведении защищенного обмена ИЭ, определяются Фондом и Участниками защищенного обмена ИЭ в заключенных между ними Договорах, Соглашениях о

конфиденциальности, либо в Соглашении об участии в защищенном обмене информацией в электронной форме, форма которого приведена в Приложении № 1 к настоящему Регламенту.

Порядок обработки и хранения ИЭ, полученной при ведении защищенного обмена ИЭ, определяется законодательством Российской Федерации и локальными нормативными актами получающей стороны.

7. Порядок внесения изменений

Фонд имеет право в одностороннем порядке вносить изменения/дополнения в настоящий Регламент и приложения к нему. Для вступления в силу внесенных изменений/дополнений, Фонд соблюдает обязательную процедуру по предварительному раскрытию информации.

Предварительное раскрытие информации осуществляется Фондом не позднее, чем за 10 (десять) календарных дней до вступления изменений в силу путем рассылки сведений о внесенных изменениях Участникам защищенного обмена ИЭ.

О своем несогласии с изменениями и/или дополнениями, вносимыми в настоящий Регламент, Участники защищенного обмена ИЭ уведомляют Фонд и прекращают вести защищенный обмен ИЭ в соответствии с условиями заключенного Соглашения об участии в защищенном обмене информацией в электронной форме.

Приложение № 1
к Регламенту защищенного обмена
информацией в электронной форме
АО «НПФ Газпромбанк-фонд»

Соглашение об участии в защищенном обмене информацией в электронной форме

Акционерное общество «Негосударственный пенсионный фонд Газпромбанк-фонд», именуемый в дальнейшем «Фонд», в лице _____, действующего на основании _____, и _____, именуемое в дальнейшем «Участник защищенного обмена ИЭ», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1. Основные понятия

Основные понятия, применяемые в настоящем Соглашении, определены в Регламенте защищенного обмена информацией в электронной форме в АО «НПФ Газпромбанк-фонд» (далее – Регламент), прилагаемом к настоящему Соглашению и являющемся его неотъемлемой частью.

2. Предмет Соглашения

2.1. Настоящее Соглашение регулирует отношения Сторон при ведении защищенного обмена информацией в электронной форме, в соответствии с Регламентом.

Ведение защищенного обмена информацией в электронной форме осуществляется Сторонами в соответствии с законодательством Российской Федерации, в том числе Гражданским Кодексом Российской Федерации, Федеральным Законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным Законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (ПКЗ-2005), утверждённым Приказом ФСБ РФ от 09.02.2005 № 66.

2.2. Стороны обязаны документально подтвердить полномочия каждого Пользователя на ведение защищенного обмена информацией в электронной форме от имени соответствующей Стороны путем предоставления друг другу соответствующего документа.

2.3. Стороны используют усиленную квалифицированную/ неквалифицированную [*оставить нужное*] электронную подпись.

2.4. Стороны обеспечивают получение Пользователями сертификата ключа проверки электронной подписи в удостоверяющем центре СУЦ Группы Газпром/ [*указать название аккредитованного УЦ*] [*оставить нужное*].

2.5. Стороны признают обязательность выполнения правил и требований Регламента.

2.6. Стороны признают, что передаваемые электронные документы (документированная информация) при ведении защищенного обмена информацией в электронной форме, подписанные электронной подписью в порядке, установленном Регламентом, равнозначны документам, подписанным собственноручной подписью.

3. Список Пользователей

3.1. Списки лиц, определенных в Регламенте, как Пользователи, которые уполномочены вести защищенный обмен информацией в электронной форме, формируются каждой Стороной в рабочем порядке и, при необходимости, если Стороной является юридическое лицо, фиксируются в локальных нормативных актах данной Стороны. Списки Пользователей должны включать фамилию, имя, отчество, адрес электронной почты и номер контактного телефона Пользователей.

3.2. Стороны обязуются обменяться списками Пользователей до начала осуществления ими защищенного обмена информацией в электронной форме и поддерживать их в актуальном состоянии посредством направления уведомлений, определенных Регламентом.

3.3. Сторона, являющаяся физическим лицом, обязана документально подтвердить другой Стороне полномочия Пользователей, выступающих от её имени при ведении защищенного обмена информацией в электронной форме, путем предоставления соответствующего документа (нотариально удостоверенной доверенности).

4. Ответственность и обязанности Сторон

4.1. Ответственность за соответствие электронного документа (документированной информации), направляемого при ведении защищенного обмена информацией в электронной форме, подлиннику такого документа возлагается на Сторону, направившую соответствующий электронный документ.

4.2. Стороны принимают на себя обязательство своевременно уведомлять друг друга о внесении изменений в список Пользователей защищенного обмена информацией в электронной форме, замене сертификатов ключа проверки электронной подписи и в других случаях, предусмотренных Регламентом.

5. Конфиденциальность

5.1. При ведении защищенного обмена информацией в электронной форме Стороны могут передавать сведения, к которым законодательством Российской Федерации или обладателем таких сведений предъявляются требования по обеспечению их конфиденциальности (конфиденциальная информация).

5.2. В целях настоящего Соглашения Стороны признают конфиденциальной информацией информацию, не содержащую сведений, составляющие государственную тайну, доступ к которой ограничивается её обладателем в соответствии с законодательством Российской Федерации или локальными нормативными документами обладателя, в частности, к конфиденциальной информации относятся:

– информация, составляющая коммерческую тайну - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

– информация, составляющая персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

– иная информация, к которой её обладатель на законных основаниях предъявляет требования по обеспечению конфиденциальности.

– Стороны принимают на себя обязательство по обеспечению режима конфиденциальности в отношении конфиденциальной информации, доступ к которой был получен в результате защищенного обмена информацией в электронной форме. Конфиденциальная информация, полученная Сторонами в рамках настоящего Соглашения, не подлежит разглашению в течение 5 (Пять) лет со дня прекращения настоящего Соглашения.

– Обязательства, предусмотренные п.5.3 настоящего Соглашения, не применимы к информации, которая одобрена для обнародования путем письменного согласия раскрывающей Стороны.

6. Порядок заключения и расторжения Соглашения, прочие условия

6.1. Настоящее Соглашение заключено на неопределенный срок и вступает в силу с даты его подписания Сторонами.

6.2. Соглашение может быть расторгнуто по соглашению Сторон либо любой из Сторон в одностороннем порядке.

6.3. В случае прекращения любой из Сторон ведения защищенного обмена информацией в электронной форме, такая Сторона обязана уведомить другую Сторону не менее чем за 30 (тридцать) календарных дней до предполагаемой даты прекращения ведения защищенного обмена информацией в электронной форме.

6.4. Любые изменения и дополнения в настоящее Соглашение действительны, если совершены в письменной форме и подписаны уполномоченными представителями Сторон.

6.5. Все споры и разногласия, которые могут возникнуть между Сторонами в связи с настоящим Соглашением, будут по возможности решаться путем переговоров между Сторонами. При невозможности урегулирования споров путем переговоров в разумные сроки, такие споры по требованию любой из Сторон передаются для окончательного разрешения в Арбитражный суд г. Москвы.

6.6. Настоящее Соглашение толкуется и регулируется в соответствии с законодательством Российской Федерации.

6.7. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

7. Приложение:

1) Регламент защищенного обмена информацией в электронной форме в АО «НПФ Газпромбанк-фонд».

8. Подписи и реквизиты Сторон:

___ «___ _____ _____»	АО «НПФ Газпромбанк-фонд»
Местонахождения:	Местонахождения : Симферопольский бульвар, д. 13, г. Москва, 117556
Почтовый адрес:	Почтовый адрес: Симферопольский бульвар, д. 13, г. Москва, 117556
_____	_____
_____ _____	_____ _____
(подпись)	(подпись)

Приложение № 2
к Регламенту защищенного обмена
информацией в электронной форме
АО «НПФ Газпромбанк-фонд»

Руководство по использованию ключа электронной подписи

Владельцам сертификата ключа проверки электронной подписи, наделенным правом постановки на электронную информацию электронной подписи при ведении защищенного обмена информацией в электронной форме, необходимо соблюдать ряд правил использования электронной подписи и ключевых носителей.

(1) Правила использования ключевых носителей:

- ключевой носитель, содержащий ключ (ключи) электронной подписи, используется владельцем сертификата ключа проверки электронной подписи персонально;
- ключевой носитель хранится в порядке, исключающем компрометацию ключей электронной подписи.

(2) Обязанности владельца сертификата ключа проверки электронной подписи:

- обеспечить хранение ключевого носителя в порядке, исключающем компрометацию содержащихся на нем ключей электронной подписи;
- не применять ключ электронной подписи при наличии факта его компрометации или подозрений на его компрометацию.
- применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа электронной подписи), если такие ограничения были установлены.
- немедленно обратиться в Удостоверяющий центр, в котором осуществлялось получение сертификата ключа проверки электронной подписи, с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае компрометации или подозрения на компрометацию ключа электронной подписи.
- не использовать ключ электронной подписи и связанный с ним сертификат ключа проверки электронной подписи, после подачи в Удостоверяющий центр заявления на прекращение (приостановление) действия сертификата ключа проверки электронной подписи, в течение времени, исчисляемого с момента подачи соответствующего заявления до момента официального уведомления о прекращении (приостановлении) действия сертификата, либо об отказе в

прекращении (приостановлении) действия сертификата.

- не использовать ключ электронной подписи и связанный с ним сертификат ключа проверки электронной подписи, если сертификат ключа проверки электронной подписи аннулирован, его действие прекращено или приостановлено.
- использовать для создания и проверки электронной подписи и создания криптографических ключей только сертифицированные в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации и средства электронной подписи.

(3) Порядок применения средств криптографической защиты информации и электронной подписи

Средства криптографической защиты информации и средства электронной подписи должны применяться владельцем сертификата ключа проверки электронной подписи в соответствии с эксплуатационной документацией на соответствующее применяемое средство.