Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

УТВЕРЖДЕН

приказом от 29.10.2018 № 8

Регламент системы

КриптоСвязь{Защищенный Электронный Документооборот}

Редакция № 2.3

Ижевск 2018

Реферат

Настоящий документ содержит Регламент системы КриптоСвязь{Защищенный Электронный Документооборот} ООО Научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект»).

Регламент создан в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданского кодекса Российской Федерации и Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Содержание

1 Определения

Электронный документ — документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

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.

Сертификат средств электронной подписи — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной подписи установленным требованиям.

Электронная подпись — 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.

Ключ электронной подписи (закрытый ключ) — уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи — уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (проверка электронной подписи).

Сертификат ключа проверки электронной подписи (сертификат) — 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.

Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат) — сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (уполномоченный федеральный орган).

Сертификат в форме документа на бумажном носителе — документ на бумажном носителе, содержащий информацию из сертификата и заверенный собственноручной подписью уполномоченного лица Удостоверяющего центра и печатью Удостоверяющего центра. Стороны признают возможность использования факсимиле подписи (клише с подписи) уполномоченного лица Удостоверяющего центра для подписи сертификата в качестве аналога собственноручной подписи, равнозначного собственноручной подписи.

Список отозванных (аннулированных) сертификатов (СОС) — электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

Владелец сертификата ключа проверки электронной подписи (*владелец сертификата)* — лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Псевдоним владельца сертификата — вымышленное имя владельца сертификата, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре.

Удостоверяющий центр — Удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект», осуществляющий выполнение целевых функций Удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» непосредственно и/или через Регистрационные отделения Удостоверяющего центра.

Аккредитация удостоверяющего центра — признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона «Об электронной подписи».

Средства удостоверяющего центра — программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Реестр Удостоверяющего центра — набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

— реестр заявлений о регистрации в Удостоверяющем центре;

— реестр зарегистрированных пользователей Удостоверяющего центра;

— реестр заявлений об изготовлении сертификата;

— реестр заявлений об аннулировании (отзыве) сертификата;

— реестр заявлений о приостановлении/возобновлении действия сертификата;

— реестр заявлений о подтверждении подлинности электронной подписи в электронном документе;

— реестр заявлений о подтверждении электронной подписи уполномоченного лица Удостоверяющего центра в изданных сертификатах;

— реестр сертификатов;

— реестр изготовленных списков отозванных сертификатов.

Уполномоченное лицо Удостоверяющего центра — физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов и списков отозванных сертификатов.

Регистрационное отделение Удостоверяющего центра (Регистрационное отделение) — подразделение Удостоверяющего центра или юридическое лицо, заключившее с Удостоверяющим центром агентский договор, уполномоченное Удостоверяющим центром осуществлять регистрацию Пользователей УЦ и управление сертификатами ключей подписей Пользователей УЦ, в т.ч.:

— взаимодействие с Пользователем УЦ, информирование и обработка (прием, регистрация, выдача) документов, предусмотренных Регламентом;

— идентификация Пользователей УЦ, проверка атрибутов и полномочий должностных лиц, подготовка и занесение регистрационной информации Пользователя УЦ в Реестр Удостоверяющего центра;

— изготовление ключевых документов по заявлениям Пользователей УЦ.

Инфраструктура открытых ключей (ИОК) / Public Key Infrastructure (PKI) — технологическая инфраструктура и сервисы, гарантирующие безопасность информационных и коммуникационных систем, использующих криптографические алгоритмы с открытыми ключами.

Регламент Удостоверяющего центра (Регламент)/ Certification Practice Statement (CPS) — документ, устанавливающий общий порядок и условия предоставления Удостоверяющим центром услуг по изготовлению и выдаче сертификатов и дополнительных услуг, связанных с управлением сертификатами.

Правила применения сертификатов (ППС)/ Certificate policy (CP) — установленный набор правил, характеризующих возможность применения сертификата определенным сообществом и/или для класса приложений с определенными требованиями безопасности. Правила применения сертификатов позволяет доверяющей стороне оценить надежность использования сертификата для определенного приложения.

Информационно-телекоммуникационная система (Система) — корпоративная информационная система, устроителем которой является Организатор Системы, основанная на технологии Инфраструктуры открытых ключей (ИОК, PKI), в которой используются сертификаты, изготовленные Удостоверяющим центром, и предназначенная для оказания услуг в области использования электронной подписи/шифрования данных и телематических услуг связи пользователям Системы.

Организатор / Оператор / Владелец Системы — устроитель корпоративной информационной системы с применением электронной подписи, организующий и обеспечивающий предоставление услуг пользователям Системы.

Сторона, присоединившаяся к Регламенту/ Абонент / Участник Системы — юридическое или физическое лицо, участник информационного обмена электронными документами, зарегистрированный в *Системе*, и при необходимости имеющий с *Организатором Системы* договорные отношения о присоединении к *Системе*, соблюдающий требования и условия пользования *Системой* (в том числе применения электронной подписи), и признающий настоящий Регламент.

Пользователь Удостоверяющего центра (Пользователь УЦ) — физическое лицо, зарегистрированное в Удостоверяющем центре и являющееся уполномоченным представителем *Участника Системы*.

Участники электронного взаимодействия — осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

Корпоративная информационная система — информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Информационная система общего пользования — информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Рабочий день Удостоверяющего центра (рабочий день) — промежуток времени с 10:00 до 17:00 по Ижевскому/Московскому времени (UTC+4) каждого дня недели за исключением выходных и праздничных дней.

Рассмотрение заявления об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата — принятие ответственным лицом Удостоверяющего центра решения об осуществлении обработки заявления на основе предоставленных Пользователей УЦ документов.

Обработка заявления об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата — совокупность действий по занесению сведений об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата в реестр Удостоверяющего

центра и уведомлению пользователя об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата.

Оператор Службы актуальных статусов сертификатов — ответственный сотрудник *Удостоверяющего центра*, являющийся владельцем сертификата и соответствующего закрытого ключа, с использованием которого подписываются электронной подписью электронные ответы Службы актуальных статусов сертификатов.

Оператор Службы штампов времени — ответственный сотрудник *Удостоверяющего центра*, являющийся владельцем сертификата, с использованием которого подписываются электронной подписью штампы времени.

Штамп времени электронного документа (штамп времени) — электронный документ, подписанный электронной подписью и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

Cryptographic Message Syntax (CMS) — стандарт, определяющий формат и синтаксис криптографических сообщений (RFC 5652).

CMS Advanced Electronic Signatures (CAdES) — формат усовершенствованной электронной подписи типа CAdES-X Long Type 1 в соответствии ETSI TS 101 733 «Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)» с учётом использования российских криптографических алгоритмов и RFC 5126.

Internet Protocol Security (IPsec) & Internet Key Exchange (IKE) — группа протоколов криптографической защиты на сетевом уровне (RFC 6071).

Online Certificate Status Protocol (OCSP) — протокол установления статуса сертификата открытого ключа (RFC 6960).

Public Key Cryptography Standards (PKCS) — стандарты криптографии с открытым ключом, разработанные компанией RSA Data Security. Удостоверяющий центр осуществляют свою работу в соответствии со следующими стандартами PKCS:

— *PKCS#7* — стандарт, определяющий формат и синтаксис криптографических сообщений.

— *PKCS#10* — стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа.

Secure/Multipurpose Internet Mail Extensions (S/MIME) — формат сообщений защищенной электронной почты (RFC 5751).

Time-Stamp Protocol (TSP) — протокол получения штампа времени (RFC 3161)».

The Transport Layer Security (TLS) Protocol — протокол криптографической защиты на транспортном уровне (RFC 5246).

2 Обозначения и сокращения

CAdES	CMS Advanced Electronic Signatures (Формат усовершенствованной электронной подписи)
CDP	CRL Distribution Point (Точка распространения СОС)
CMS	Cryptographic Message Syntax (Синтаксис криптографических сообщений)
CP	Certificate Policy (Правила применения сертификатов)
CPS	Certification Practice Statement (Регламент Удостоверяющего центра)
CRL	Certificate Revocation List (Список отозванных сертификатов)
DN	Distinguished Name (Отличительное имя)
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security (Протокол криптографической защиты на сетевом уровне)
OID	Object IDentifier (Объектный идентификатор)
OCSP	Online Certificate Status Protocol (Протокол установления актуального статуса сертификата)
PDS	PKI Disclosure Statement (Справочник по ИОК УЦ)
PKI	Public Key Infrastructure (Инфраструктура Открытых Ключей)
RFC	Request For Comments
S/MIME	Secure/Multipurpose Internet Mail Extensions (Формат сообщений защищенной электронной почты)
TLS	Transport Layer Security Protocol (Протокол криптографической защиты на транспортном уровне)
TSP	Time-Stamp Protocol (Протокол получения штампа времени)
URI	Uniform Resource Identifier (Единый идентификатор ресурса)
URL	Uniform Resource Locator (Единый локатор ресурса)
UTC/GMT	Universal Time Coordinated/Greenwich Mean Time (Универсальное координированное время/Всемирное время «по Гринвичу»)
ИОК	Инфраструктура Открытых Ключей (Public Key Infrastructure)

КСКПЭП	Квалифицированный сертификат ключа проверки электронной подписи (Квалифицированный сертификат)
КС	Квалифицированный сертификат (Квалифицированный сертификат ключа проверки электронной подписи)
КЭП	Квалифицированная электронная подпись
НСД	Несанкционированный доступ
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКПЭП	Сертификат ключа проверки электронной подписи
СОС	Список отозванных сертификатов (Certificate Revocation List)
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

3 Введение

Работа с документами в электронной форме позволяет оперативно и удобно хранить, обрабатывать и передавать документы в информационной системе. При этом информационные системы могут быть потенциально подвержены следующим атакам:

— нарушение конфиденциальности передаваемых документов;

— несанкционированное искажение электронных документов;

— отправка ложного электронного документа от имени легального пользователя системы.

Подобные уязвимости могут быть устранены за счет использования электронной подписи (обеспечение целостности и подлинности) и шифрования (обеспечение конфиденциальности) электронных документов в информационной системе.

Кроме этого, условием использования электронных документов является обеспечение способности электронного документа быть надежным аргументом, и под юридической значимостью, прежде всего, следует понимать возможность использования его в судах в качестве доказательств. Для этого в электронном документе обязательного должны присутствовать определенные реквизиты (дата, номер, подпись, печать и прочее), соблюдения правомочности субъекта и его полномочий (права должностного лица подписывать такие документы).

3.1 Сведения о Системе

НПП «Ижинформпроект» предлагает комплексный вариант создания автоматизированных рабочих мест для обеспечения обмена конфиденциальными электронными юридически значимыми документами в системе обмена конфиденциальными электронными юридически значимыми электронными документами КриптоСвязь{Защищенный Электронный Документооборот} (далее — *Система*) ООО Научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект») (далее — *Оператор*).

В *Системе* допускается (при обязательном использовании шифрования) обмениваться электронными документами, содержащими конфиденциальную информацию (персональные данные, служебная, банковская, коммерческая тайна и т.п.).

Участники Системы при необходимости устанавливают особые (дополнительные) условия взаимодействия. При этом дополнительные условия в целях обеспечения защищенности электронного документооборота (конфиденциальность, целостность, аутентичность, неотказуемость и юридическая значимость) рекомендуется согласовывать с *Оператором*.

Регламент не устанавливает требований к форматам электронных документов, периодичности обмена, внутреннего учета и обеспечения защиты документов у *Участников Системы*.

Защищенный электронный документооборот в *Системе* реализуется с использованием базовых приложений Инфраструктуры открытых ключей (ИОК) / Public Key Infrastructure (PKI) — технологическая инфраструктура и сервисы, гарантирующие безопасность информационных и коммуникационных систем, использующих криптографические алгоритмы с открытыми ключами.

При построении защищенного электронного документооборота применяются электронная подпись (а также шифрование) электронных документов, представленных в виде файлов, передаваемых между *Участниками Системы*, и электронная подпись и шифрование почтовых сообщений Internet.

Электронная почта с электронной подписью позволяет получателю убедиться в подлинности и целостности электронного документа/сообщения. Шифрование электронных документов/сообщений электронной почты препятствует его прочтению другими людьми в процессе доставки.

Если защищенный электронный документ/сообщение с ошибками (например, сообщение подделано или истек срок действия сертификата отправителя), перед тем, как можно будет просмотреть содержимое объекта, будет отображаться предупреждение, в котором излагается подробное описание неполадки. На основе

содержащихся в предупреждении сведений пользователь может принять решение относительно уровня доверия к нему.

Для возможности работы в *Системе* пользователь должен получить квалифицированный сертификат ключа проверки электронной подписи в Удостоверяющем центре InfoTrust ООО НПП «Ижинформпроект» в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Сертификат должен содержать сведения о возможности использования в *Системе* в соответствии с разделом Обеспечение юридической значимости электронных документов настоящего *Регламента*.

После обмена *Участниками Системы* их сертификатами (сертификат направляется вместе с сообщением) и помещением этих сертификатов в адресную книгу почтового клиента можно направлять электронные документы/сообщения в защищенном виде.

Если проверка отзыва сертификатов ключей подписи включена, статус сертификатов проверяется при открытии сообщения, если установлено подключение через Интернет к серверу Удостоверяющего центра.

3.2 Сведения об Операторе

Общество с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект»), предоставляющее услуги *Оператора* в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданского кодекса Российской Федерации и Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», именуемое в дельнейшем *Оператор*, зарегистрировано на территории Российской Федерации в городе Ижевске.

Оператор осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

1 лицензия Управления ФСБ России по Удмуртской Республике на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) от 11.10.2016 № 110Н;

2 лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание услуг связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации, от 18.08.2018 № 163770;

3 лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание телематических услуг связи от 18.08.2018 № 163771.

Реквизиты ООО НПП «Ижинформпроект»:

ИНН 1831014533 КПП 183101001

Юридический адрес: ул. Бородина, 21, офис 207, г. Ижевск, Удмуртская Республика, 426057

Банковские реквизиты:

Удмуртском отделении № 8618 ПАО СБЕРБАНК г. Ижевск

р/с 40702810768170101530

к/с 30101810400000000601

БИК 049401601

Контактная информация

телефон/факс: +7 (3412) 918-100,

e-mail: pki@infotrust.ru, info@infotrust.ru

WWW: www.infotrust.ru

3.3 Идентификация документа

Наименование документа — Регламент системы КриптоСвязь{Защищенный Электронный Документооборот}.

Редакция: 2.3.

Дата: 29.10.2018.

Количество страниц в документе: 60.

3.4 Статус документа

Регламент системы КриптоСвязь{Защищенный Электронный Документооборот} (далее — *Регламент*) устанавливает общий порядок взаимодействия *Участников Системы* защищенного электронного документооборота, требования к инфраструктуре обеспечения применения электронной подписи, порядок использования доверенных служб и требования обеспечения безопасности электронных документов.

Любое заинтересованное лицо может ознакомиться с *Регламентом* в офисе *Оператора*, и по запросу получить его копию за плату, не превышающую расходов на ее изготовление.

Регламент вступает в силу со дня его публикации.

3.5 Изменения (дополнения) документа

Внесение изменений (дополнений) в *Регламент*, в том числе в приложения к ним, производится *Оператором* в одностороннем порядке.

Уведомление *Участника Системы* о внесении изменений (дополнений) в *Регламент* осуществляется *Оператором* путем размещения указанных изменений (дополнений) на сайте *Оператора* по адресу http://www.infotrust.ru.

4 Условия взаимодействия участников

Участниками Системы являются *Пользователи УЦ*, имеющие сертификаты, соответствующие требованиям системы КриптоСвязь{Защищенный Электронный Документооборот}.

Присоединение к *Регламенту Системы* осуществляется в момент присоединения к Регламенту Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект», т.е. при получении сертификата Пользователя УЦ.

Участники при организации взаимодействия руководствуются *Регламентом* системы КриптоСвязь{Защищенный Электронный Документооборот}.

Участники признают электронный документ в *Системе*, подписанный электронной подписью, равнозначным документу на бумажном носителе, подписанному собственноручной подписью *Участника Системы*, а также заверенному печатью, с учетом требований, определенных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и настоящим *Регламентом*.

Заказчик признает надежность используемых в *Системе* сертифицированных в установленном порядке СКЗИ достаточной для подтверждения подлинности участников взаимодействия и обеспечения конфиденциальности передаваемой информации, доступ к которой ограничен федеральными законами (информация ограниченного доступа/конфиденциальная информация).

Участники Системы самостоятельно обеспечивают соответствие своих автоматизированных рабочих мест защищенного электронного документооборота (АРМ-ЗЭД) установленным требованиям по аппаратному и программному обеспечению, каналам связи, средствам защиты информации и т.д. Перечень требований отражен в разделе Технические условия подключения автоматизированного рабочего места участника *Системы* КриптоСвязь {Защищенный Электронный Документооборот}.

Участник Системы самостоятельно обеспечивает выполнение требований Положения о порядке использования средств криптографической защиты

информации и ключевой информации к ним, Требований по обеспечению безопасности автоматизированного рабочего места, в т.ч.

— безопасное размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним;

— оборудование средства вычислительной техники, на котором осуществляется штатное функционирование СКЗИ, средствами контроля их вскрытия (опечатывание, опломбирование);

— назначение пользователей СКЗИ и ответственных за обеспечение безопасности хранения, обработки и передачи информации по каналам связи с использованием СКЗИ (администратор безопасности);

— наличие обученного персонала для пользования СКЗИ;

— ведение поэкземплярного учета используемых СКЗИ;

— периодический контроль за соблюдением условий использования СКЗИ, указанных в правилах пользования на них.

Участник Системы самостоятельно обеспечивает выполнение требований по эксплуатации СКЗИ в соответствии с технической и эксплуатационной документацией:

— безопасный порядок изготовления, санкционированного копирования, выбор отчуждаемых защищенных носителей криптографических ключей и защищенных мест их хранения;

— обеспечение защиты компьютера от несанкционированного доступа путем настройки политики безопасности, установки дополнительных сертифицированных средств защиты от несанкционированного доступа, установки лицензионного программного обеспечения, полученного из надежных источников и не содержащего средств разработки и отладки программ, своевременной установки обновлений безопасности для него, удаление/отключение средств удаленного доступа и администрирования (Удаленный помощник, Radmin, TeamViewer, Ammyy Admin и т.п.);

— соблюдение правил безопасной работы в сети Интернет и обеспечение непрерывной комплексной защиты компьютера от вирусов, атак, спама, шпионского программного обеспечения и других вредоносных программ при подключении к сетям передачи данных путем установки антивирусных программ, средства обнаружения вторжений и персонального межсетевого экрана с периодическим обновлением их баз данных решающих правил;

— установка надежных (не менее 6 символов, использование букв, цифр и спецсимволов) паролей к ключевым носителям, системе конфигурирования компьютера (BIOS/UEFI), учетной записи и экранной заставке операционной системы, обеспечение их регулярной смены.

Участник Системы самостоятельно обеспечивает допуск к конфиденциальной информации только уполномоченных должностных лиц и создает все необходимые условия для обеспечения неразглашения конфиденциальной информации, сведений о реквизитах доступа, паролях и PIN-кодах доступа к криптографическим ключам и ключевым носителям.

Участник Системы самостоятельно обеспечивает доступ к определенным почтовым ящикам электронной почты Интернет (другим используемым узлам/сервисам сети Интернет) и оплачивает доступ в сеть общего пользования Интернет с автоматизированного рабочего места защищенного электронного документооборота (АРМ-ЗЭД) пользователя.

При необходимости согласования между *Участниками Системы* формы и типа передаваемых электронных документов и порядок их обработки, то рекомендуется составить соглашение на основании Типового Соглашения об информационном взаимодействии (Приложение А).

5 Средства криптографической защиты информации

Для защиты электронных документов/сообщений в *Системе* используются сертифицированные средства криптографической защиты информации (СКЗИ) «КриптоПро CSP» и «КриптоАРМ», а также совместимые с ними.

Применение сертифицированных СКЗИ обеспечивает использование российских криптографических алгоритмов:

— Алгоритм зашифрования/расшифрования данных и вычисление имитовставки в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая»;

— Алгоритм формирования и проверки цифровой подписи в соответствии с ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

— Алгоритм формирования и проверки цифровой подписи в соответствии с ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

— Алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

— Алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

Класс криптографической защиты информации определяется требованиями руководящих документов и моделями угроз *Участников Системы*. Для обеспечения классов криптографической защиты информации КС2 и КС3 необходимо использовать сертифицированное ФСБ России средство защиты от несанкционированного доступа типа «электронный замок».

Использование средств защиты информации производится в соответствии с технической и эксплуатационной документацией на них.

В связи с применением СКЗИ в составе стандартного программного обеспечения Microsoft и UNIX (Word, Excel, InfoPath, Outlook из состава Microsoft Office, Почта Windows Mail, Live Mail, Microsoft Outlook Express и TLS-клиент из состава Internet Explorer, TLS-сервер из состава Internet Information Services и Trusted TLS, КриптоПро OCSP и TSP, КриптоАРМ, CryptCP) (без встраивания в прикладное программное обеспечение) проводить оценку влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований не требуется.

6 Доверенная третья сторона

6.1 Удостоверяющий центр

В *Системе* используются квалифицированные сертификаты, изготовленные аккредитованным Минкомсвязью России Удостоверяющим центром InfoTrust ООО НПП «Ижинформпроект», осуществляющим выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» непосредственно и/или через Регистрационные отделения Удостоверяющего центра.

Пользователи обязаны устанавливать корневые сертификаты Удостоверяющего центра InfoTrust, полученные из надежных источников.

Сертификаты уполномоченного лица Удостоверяющего центра InfoTrust можно загрузить из официальных точек публикации удостоверяющего центра, а также из реестра Уполномоченного федерального органа в области электронной цифровой подписи (Минкомсвязь России).

Рекомендуется проверить подлинность устанавливаемых сертификатов удостоверяющего центра в соответствии с документацией Удостоверяющего центра InfoTrust, опубликованной на официальном сайте www.infotrust.ru.

6.2 Служба актуального статуса сертификатов

Оператор оказывает услуги по предоставлению актуальной информации о статусе сертификатов посредством Сервиса службы актуальных статусов сертификатов.

Доступ к использованию сервисов Службы актуальных статусов сертификатов *Удостоверяющего центра* обеспечивается Владельцам сертификатов, имеющих в сертификате расширение области применения Использование усовершенствованной электронной подписи (1.2.643.3.34.2.7).

Служба актуальных статусов сертификатов по запросам формирует и предоставляет OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата. OCSP-ответы представляются в форме электронного

документа, подписанного электронной подписью с использованием сертификата Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов).

OCSP-ответ признается действительным при одновременном выполнении следующих условий:

— Подтверждена подлинность подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) в OCSP-ответе;

— Сертификат Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент подтверждения подлинности подписи OCSP-ответа действителен;

— Закрытый ключ подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;

— Сертификат Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении Extended Key Usage область применения — Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);

— Сертификат участника, статус которого установлен с использованием данного OCSP-ответа, издан Удостоверяющим центром и содержит в расширении Extended Key Usage или Certificate Policies область применения — Использование усовершенствованной электронной подписи (1.2.643.3.34.2.7).

Адрес обращения к Службе актуальных статусов сертификатов *Удостоверяющего центра* — http://z.infotrust.ru/ocsp###/ocsp.srf. Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых *Удостоверяющим центром* сертификатов, предназначенных для работы со Службой актуальных статусов сертификатов *Удостоверяющего центра*.

6.3 Служба штампов времени

Оператор оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени.

Доступ к использованию сервисов Службы штампов времени *Удостоверяющего центра* обеспечивается Владельцам сертификатов, имеющих в сертификате расширение области применения Использование усовершенствованной электронной подписи (1.2.643.3.34.2.7).

Штамп времени, относящийся к подписанному электронному документу, признается действительным при одновременном выполнении следующих условий:

— Подтверждена подлинность подписи Службы штампов времени (Оператора Службы штампов времени) в штампе времени;

— Сертификат Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности подписи штампа времени действителен;

— Закрытый ключ подписи Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;

— Сертификат Службы штампов времени (Оператора Службы штампов времени) содержит в расширении Extended Key Usage область использования — Установка штампа времени (1.3.6.1.5.5.7.3.8);

— Сертификат участника, на котором сформирована подпись электронного документа и к которому относится данный штамп времени, издан Удостоверяющим центром и содержит в расширении Extended Key Usage или Certificate Policies область использования — Использование усовершенствованной электронной подписи (1.2.643.3.34.2.7).

Адрес обращения к Службе штампов времени *Удостоверяющего центра* — http://z.infotrust.ru/tsp###/tsp.srf.

Сведения о параметрах политики выдачи штампов времени указываются в штампе времени.

7 Обеспечение юридической значимости электронных документов

В соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» информация в электронной форме, подписанная квалифицированной электронной подписью, созданной с помощью квалифицированного сертификата ключа проверки электронной подписи, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

Квалифицированная электронная подпись, признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с

помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств электронной подписи, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом, и с использованием квалифицированного сертификата лица, подписавшего электронный документ;

4) квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены).

Поля Key Usage, Extended Key Usage, а также Certificate Policies, сертификата содержат, наряду со стандартными/технологическими объектными идентификаторами (OID) (по RFC 5280 и др.), определяющими технологии/ приложения PKI (аутентификация, защищенная электронная почта и т.д.), сведения об отношениях, разрешенных *Пользователю УЦ*, а также в установленных случаях об ограничениях, в системах и приложениях построенных на основе технологии Инфраструктуры открытых ключей, и при которых электронный документ будет иметь юридическое значение. Данные сведения представляют собой набор объектных идентификаторов, зарегистрированных в установленном порядке.

Поля Extended Key Usage квалифицированного сертификата *Участника Системы* должны содержать, наряду со стандартными/технологическими объектными идентификаторами (OID), определяющими технологии/приложения PKI (аутентификация, защищенная электронная почта и т.д.), дополнительные сведения о возможности использования в *Системе*. Данные сведения представляют собой набор OID, зарегистрированных в установленном порядке:

1.	1.3.6.1.4.1.23133	ООО НПП «Ижинформпроект»
2.	1.2.643.1.10.1	Защищенная информационно-телекоммуникационная система «КриптоСвязь»
3.	1.2.643.3.34.2.1	Подпись документов (соглашений, договоров, актов, писем и т.п.)
4.	1.2.643.3.34.2.4	Межведомственный/межкорпоративный защищенный электронный документооборот

8 Форматы электронных документов

8.1 Обрабатываемые данные

Формат электронного документа — структура содержательной части электронного документа. Через *Систему* можно обмениваться документами любых форматов: формализованные — со строгой печатной формой или описанием XML-структуры, атрибуты которых подлежат автоматической обработке, и неформализованные — свободная форма в общеупотребительных форматах.

Рекомендуется использовать следующие наиболее распространенные форматы содержательной части электронного документа:

Текстовые документы	Microsoft Word 97-2010 (.doc) Office Open XML (.docx) Rich Text Format (.rtf) Текстовый файл (.txt)
Табличные документы	Microsoft Excel 97-2010 (.xls) Office Open XML (.xlsx)
Графические документы	Portable Document Format (.pdf) Joint Photographic Experts Group (.jpeg, .jpe, .jpg) Tagged Image File Format (.tif, .tiff)

Для обеспечения гарантированной доставки электронных сообщений рекомендуется ограничивать максимально допустимый размер файлов, содержащих электронные документы, в объеме 5 Мб.

Не рекомендуется подписывать архивные файлы (.zip, .rar), содержащие несколько отдельных электронных документов.

8.2 Формат электронной подписи

Для электронной подписи электронных документов в *Системе* применяются следующие криптографические алгоритмы:

— алгоритм формирования и проверки цифровой подписи в соответствии с ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

— алгоритм формирования и проверки цифровой подписи в соответствии с ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

— алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»;

— алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»,

с учетом требований RFC 4357, RFC 4490 и RFC 4491.

Используемый формат и синтаксис криптографических сообщений — *Cryptographic Message Syntax (CMS)* (RFC 5652) (Public Key Cryptography Standard #7 — PKCS#7).

Для удобства использования подписанной информации всеми участниками обмена рекомендуется использовать формат отсоединённой подписи (detached signature) — электронная подпись помещается в отдельный файл, имеющий формализованное правило именования, при котором к имени исходного файла добавляется постфикс .sig (text.txt → text.doc + text.doc.sig). Примеры наименования файлов представлены в Приложении Б.

По согласованию между участниками допускается применение присоединённой подписи (attached signature) — электронная подпись с исходным файлом объединяется общий файл криптографического сообщения, имеющий формализованное правило именования, при котором к имени исходного файла добавляется постфикс .sig (text.txt → text.doc.sig). А также возможно использование форматов «внутренней» подписи документов XML-DSig и PDF (правила включения CMS в PDF), при этом требуется дополнительно применять программные продукты КриптоПро Office Signature и КриптоПро PDF.

8.3 Формат усовершенствованной электронной подписи

Для повышения уровня надежности и увеличения срока хранения электронных документов с электронной подписью в *Системе* может применяться формат усовершенствованной электронной подписи (CMS Advanced Electronic Signatures (CAdES)) типа CAdES-X Long Type 1 в соответствии ETSI TS 101 733 «Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)» с учётом использования российских криптографических алгоритмов и RFC 5126.

При этом используются Служба актуального статуса сертификатов *Удостоверяющего центра* по протоколу установления статуса сертификата открытого ключа (Online Certificate Status Protocol (OCSP)), определенному RFC 2560, и Служба штампов времени *Удостоверяющего центра* по протоколу получения штампа времени (Time-Stamp Protocol (TSP)) по RFC 3161.

Такая усовершенствованная электронная подпись (CAdES-X Long Type 1) содержит штамп времени на подпись, все сертификаты, доказательства подлинности сертификатов и штамп времени на доказательства подлинности.

Для формирования усовершенствованной подписи требуется дополнительно применять программные продукты КриптоПро TSP Client и КриптоПро OCSP Client.

Сертификат *Пользователя УЦ* должен содержать расширение, позволяющее обращаться к Службе актуального статуса сертификатов Службе штампов времени *Удостоверяющего центра.*

По согласованию между участниками возможно использование форматов «внутренней» усовершенствованной электронной подписи документов XML Advanced Electronic Signatures (XAdES) (XML-Dsig+) по ETSI TS 101 903 и PDF Advanced Electronic Signatures (PAdES) (CAdES & XAdES in PDF) по ETSI TS 102 778 с использованием дополнительных программных средств.

9 Обеспечение конфиденциальности электронных документов

При необходимости обеспечения конфиденциальности электронных документов при их хранении, а также при передаче по каналам связи (в случае отсутствия таких механизмов в используемых для этого протоколах обмена) *Участники Системы* могут использовать шифрование.

Применение сертифицированных СКЗИ обеспечивает использование российских криптографических алгоритмов зашифрования/расшифрования данных и вычисление имитовставки в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая» с учетом требований RFC 4357, RFC 4490 и RFC 4491.

Используемый формат и синтаксис криптографических сообщений — *Cryptographic Message Syntax (CMS)* (RFC 5652) (Public Key Cryptography Standard #7 — PKCS#7). Шифрование и имитозащита могут быть совмещены с процедурой формирования электронной подписи, в т.ч. с усовершенствованной.

Результат криптографического преобразования помещается в файл, имеющий формализованное правило именования, при котором к имени исходного файла добавляется постфикс .enc (text.txt → text.doc.enc). Примеры наименования файлов представлены в Приложении Б.

При зашифровании информации автором криптографического сообщения определяется перечень *Участников Системы*, которые смогут получить доступ к зашифрованной информации. Для этого в процессе криптографического преобразования используются действующие сертификаты таких Участников (получателей).

10 Защита электронных документов

10.1 Криптографический файловый менеджер

Для обеспечения защиты электронного документа в *Системе* используется криптографический менеджер «КриптоАРМ» (разработчик — ООО «Цифровые технологии»).

Криптографический файловый менеджер предназначен для удобного проведения операций шифрования и электронной подписи электронных документов по российским государственным криптографическим стандартам.

«КриптоАРМ» имеет расширенные возможности использования электронной подписи (соподпись, заверяющая подпись и поддержка расширенных свойств электронной подписи, например, возможность поставить комментарий к ней), а также гибкую настройку криптографических операций под индивидуальные задачи пользователя с помощью комплексных настроек (профилей) пользователя для разных задач.

Правила настройки и работы с криптографическим менеджером описаны в эксплуатационной документации.

10.2 Порядок создания защищенного электронного документа

Электронные документы и их приложения создаются в установленном (согласованном участниками соответствующего обмена) формате (например, doc, xls, pdf, jpg и т.п.) в соответствии с правилами электронного документооборота Участников взаимодействия. Электронная подпись формируется в отдельный файл (отделенная), имеющий соответствующее расширение (.sig). Рекомендуется использовать DER-кодировку (Distinguished Encoding Rules — правила кодирования структур данных, созданных в соответствии с ASN.1 (Abstract Syntax Notation One) по X.680/ГОСТ Р ИСО/МЭК 8824-1-2001 и X.690/ГОСТ Р ИСО/МЭК 8825-93).

Документ (все файлы, в т.ч. приложения) передаются на подпись уполномоченному должностному лицу, имеющему право подписывать данный вид документов, являющемуся владельцем сертификата. Документ подписываются с

использованием криптографического файлового менеджера. После подписания электронного документа внесение изменений в его содержание запрещается.

На соответствующих этапах формирования документа, внутреннего согласования и т.п. возможно формирование несколько электронных подписей на один файл, в т.ч. соподпись и заверяющая подпись.

Регистрация документа после его подписания производится путем создания уполномоченным сотрудником подразделения делопроизводства отдельного служебного файла (.doc или .txt), содержащего реквизиты, отсутствующие в подписанном документе, и подписания его электронной подписью с использованием криптографического файлового менеджера. Такой дополнительный служебный файл является неотъемлемой частью документа и отправляется вместе с документом. Если электронный документ, подписанный электронной подписью, содержит регистрационный номер и дату, то служебный файл не создается.

При необходимости обеспечения конфиденциальности электронных документов при их хранении, а также при передаче по каналам связи (в случае отсутствия таких механизмов в используемых для этого протоколах обмена) уполномоченный сотрудник подразделения делопроизводства с использованием криптографического файлового менеджера производит зашифрование документа, указывая при этом сертификаты всех легитимных пользователей данного документа.

После указанных процедур зарегистрированным защищенным электронным документом считается комплект файлов содержащих документы и электронную подпись к ним, а также служебный файл с подписью. Документ для уменьшения объема передаваемой информации может упаковываться (сжиматься) в файл-архив (.zip или .rar). Для уникальности документов имя файла-архива рекомендуется создавать с учетом регистрационного номера документа. Документ (файл-архив) направляется, как правило, с использованием защищенного почтового сообщения.

Документ помещается в хранилище электронных документов. Сроки и условия хранения электронных документов устанавливаются внутренними нормативными документами *Участника Системы* (как правило, срок аналогичен сроку хранения документа на бумажном носителе).

10.3 Порядок приема защищенного электронного документа

При получении защищенного электронного документа с помощью криптографического файлового менеджера производится его расшифрование и проверка электронной подписи всех входящих в документ файлов, а также проверка сертификата уполномоченного должностного лица на предмет возможности использования этого сертификата применительно к этому виду документов.

В случае нарушения электронной подписи документ не принимается к дальнейшей обработке и отправителю направляется соответствующее сообщение о необходимости повторного направления документа.

В случае корректности электронной подписи документ регистрируется и передается для последующего рассмотрения или обработки в соответствии правилами внутреннего документооборота.

Копия документа помещается в хранилище электронных документов. Сроки и условия хранения электронных документов устанавливаются внутренними нормативными документами *Участника Системы*.

При необходимости распечатывания документа на бумажный носитель на нем указываются отсутствующие реквизиты документа (номер и дата из служебного файла), делается заверяющая отметка/штамп о верности электронной подписи.

11 Защита сообщений электронной почты

11.1 Криптографический почтовый клиент

Для обеспечения авторства и конфиденциальности защищенных сообщений электронной почты с помощью электронной подписи и шифрования применяется почтовый клиент, реализующий синтаксис криптографических сообщений, управление сертификатами, процедуры и атрибуты сервисов безопасности для почтовых приложений по протоколу S/MIME (Secure/Multipurpose Internet Mail Extensions) (RFC5751) и ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 и ГОСТ 28147-89 с учетом требований RFC 4357, RFC 4490 и RFC 4491 на основе сертифицированного СКЗИ КриптоПро CSP.

Для обеспечения обмена защищенными сообщениями электронной почты в *Системе* используются почтовые клиенты Почта Windows Mail, Live Mail, Outlook Express из состава Internet Explorer и Microsoft Outlook из состава Microsoft Office.

Указанные почтовые клиенты реализуют контроль доставки сообщений до адресата (безопасные уведомления с электронной подписью получателя). При использовании иных почтовых клиентов с поддержкой S/MIME в установленных случаях необходимо проводить оценку влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований, а также возможно ограничение функционала по контролю доставки сообщений.

Для обеспечения возможности использования почтовых клиентов для обмена защищенными почтовыми сообщениями пользователь должен иметь сертификат, поддерживающий стандартное приложение ИОК «Защищенная электронная почта» (OID 1.3.6.1.5.5.7.3.4) и предназначенный для адреса электронной почты пользователя, указанного в сертификате.

Правила настройки и работы с соответствующим почтовым клиентом установлены эксплуатационной документацией на него.

11.2 Порядок создания и отправки защищенного почтового сообщения

В поле «Тема сообщения» рекомендуется указывать реквизиты (номер и дата) направляемого документа. В теле письма рекомендуется указывать наименование пересылаемого документа и при необходимости другие вспомогательные параметры и комментарии. В случае ответа на запрос в теле письма указывается также номер и дата письма, на которое направляется ответ. К созданному почтовому сообщению присоединяется файл-архив, содержащий направляемый документ.

Адресат выбирается из адресной книги/контактов почтового клиента. Для автоматического выбора сертификатов получателей, в адрес которых требуется зашифровать почтовое сообщение, Участники обмена должны предварительно обменяться сертификатами и установить («привязать») их в адресной книге/контактах к соответствующим адресам электронной почты.

Перед оправкой защищенного почтового сообщения необходимо убедиться, что выбраны нужные адресаты и включены режимы защиты отправляемого сообщения (шифрование и электронная подпись) и требование запроса безопасного уведомления о прочтении почтового сообщения (с электронной подписью получателя). Указанные режимы работы, как правило, устанавливаются для почтового ящика на этапе его настройки и/или перенастройки на новый сертификат.

При отправке почтовое сообщение подписывается почтовым клиентом с СКЗИ электронной подписью отправителя и зашифровывается в адрес получателей (на сертификаты получателей).

Отправитель периодически контролирует доставку сообщения и связывается с адресатом в случае неполучения необходимых уведомлений. В случае неполучения сообщения адресатом отправитель производит повторную отправку сообщения.

Учет отправки конфиденциальных электронных документов рекомендуется производить по соответствующему Журналу (Приложение В).

11.3 Порядок приема защищенного почтового сообщения

При получении сообщения почтовый клиент с СКЗИ производит его расшифрование и проверку электронной подписи. Факт получения электронного сообщения подтверждается путем передачи автоматически формируемого безопасного уведомления (с электронной подписью получателя).

В случае нарушения электронной подписи сообщение не принимается к дальнейшей обработке и отправителю направляется соответствующее сообщение о необходимости повторного направления документа.

В случае корректности электронной подписи документ регистрируется и передается для последующего рассмотрения или обработки в соответствии правилами внутреннего документооборота.

Учет приема конфиденциальных электронных документов рекомендуется производить по соответствующему Журналу (Приложение В).

12 Защита взаимодействия Веб-обозревателя с Веб-сервером

12.1 Защищенный Веб-сервер и Веб-обозреватель

Для обеспечения защищенного обмена между Веб-обозревателем и Веб-сервером используется протокол криптографической защиты коммуникаций в Интернет на транспортном уровне TLS (The Transport Layer Security Protocol) по RFC 5246 и ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 и ГОСТ 28147-89 с учетом требований RFC 4357, RFC 4490 и RFC 4491 на основе сертифицированного СКЗИ КриптоПро CSP.

При этом может быть произведена аутентификация участников взаимодействия, шифрование и имитозащита трафика. Аутентификация участников взаимодействия может быть двухсторонняя (с подтверждением действительности Веб-сервера и Веб-обозревателя) и односторонняя (с подтверждением действительности только Веб-сервера). Для обеспечения защиты трафика, содержащего конфиденциальную информацию, рекомендуется использовать двустороннюю аутентификацию.

Для обеспечения защищенного обмена в *Системе* используются защищенные Веб-серверы на основе TLS-сервера из состава Internet Information Services и Trusted TLS и защищенный Веб-обозреватель на основе TLS-клиента из состава Internet Explorer. При использовании иных Веб-серверов и Веб-обозревателей в установленных случаях необходимо проводить оценку влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований.

Для обеспечения возможности использования Веб-сервера и Веб-обозревателя для защиты взаимодействия Веб-сервер должен иметь сертификат, содержащий расширение «Проверка подлинности сервера» (OID 1.3.6.1.5.5.7.3.1) и предназначенный для DNS-имени/IP-адреса сервера, указанного в сертификате, а для использования Веб-обозревателя пользователь должен иметь сертификат, содержащий расширение «Проверка подлинности клиента» (OID 1.3.6.1.5.5.7.3.2).

Правила настройки и работы с соответствующим Веб-сервером и Веб-обозревателем установлены эксплуатационной документацией.

12.2 Порядок защищенного взаимодействия

Для организации защищенного взаимодействия с аутентификацией участников, шифрованием и имитозащитой трафика между Веб-сервером и Веб-обозревателем в адресной строке Веб-обозревателя необходимо указать адрес Веб-сервера — Единый указатель ресурсов (Uniform Resource Locator, URL) в виде https://servername.ru. При этом обеспечивается реализация протокола HTTPS (HyperText Transfer Protocol Secure) — расширение протокола HTTP, поддерживающее криптографический протокол TLS. Для HTTPS по умолчанию используется TCP-порт 443.

В случае настройки Веб-сервера на использование двусторонней аутентификации при подключении к нему в Веб-обозревателе потребуется выбрать сертификат, доверенный для данного Веб-сервера.

При подключении в защищенном режиме в Веб-обозревателе появляется индикатор статуса, как правило, в виде символа замка. При просмотре свойств подключения доступна информация о сертификате Веб-сервера и используемых криптографических протоколах/алгоритмах. Пользователь должен убедиться в выборе правильного адреса Веб-сервера. Рекомендуется сохранить правильный адрес Веб-сервера в избранных закладках/ярлыках Веб-обозревателя.

13 Особенности применения шифрования

При использовании шифрования имеется ряд особенностей, которые необходимо учитывать при использовании защищенного электронного документооборота.

В целях обеспечения конфиденциальности электронных документов необходимо обеспечить своевременное удаление исходного файла после процедуры зашифрования с использованием безопасных методов (без возможности восстановления).

Уничтожение криптографических ключей во избежание утраты зашифрованной информации можно проводить только после проведения процедур расшифрования информации и зашифрования на новые криптографические ключи/сертификаты.

В связи с невозможностью обнаружения и блокирования на телекоммуникационных серверах компьютерных вирусов и вредоносного программного обеспечения в зашифрованных сообщениях/соединениях автоматизированное рабочее место защищенного электронного документооборота должно быть оснащено средствами антивирусной защиты и обнаружения компьютерных атак с регулярно обновляемыми базами знаний. Перед зашифрованием и после расшифрования требуется проверять обрабатываемые файлы антивирусными средствами во избежание распространения компьютерных вирусов.

14 Обработка электронных документов

14.1 Хранение электронных документов

Рекомендуется хранить электронные документы в том формате, в котором они были отправлены или получены, позволяющем установить, что отправленные или полученные данные, содержащиеся в электронном сообщении, не искажены.

При хранении конфиденциальных документов необходимо использовать средства защиты от несанкционированного доступа в соответствии с установленными требованиями по обработке конфиденциальных сведений. Возможно хранение документов в зашифрованном виде.

14.2 Копии электронных документов на бумажных носителях

Электронные документы, подписанные электронной подписью, признаются подлинниками, не требуют дублирования/копирования на бумажные носители и являются юридически значимыми, подлежат хранению и могут использоваться в качестве доказательств в соответствии с законодательством Российской Федерации.

При необходимости распечатывания документа на бумажный носитель на нем указываются отсутствующие реквизиты документа (номер и дата из служебного файла), делается заверяющая отметка/штамп о верности электронной подписи с подписью уполномоченного лица.

15 Технические условия

Требования к автоматизированному рабочему месту защищенного электронного документооборота (АРМ-ЗЭД):

— IBM PC-совместимый компьютер с процессором Pentium-200 или выше;

— ОЗУ не менее 64 Мбайт;

— не менее 150 Мбайт свободного дискового пространства;

— Свободный порт USB (в случае использования Рутокен/JaCarta/eToken);

— Свободный слот PCI/PCI-E (в случае использования ЭЗ Соболь/Аккорд);

— Операционная система Microsoft Windows Vista или выше;

— WEB–обозреватель Microsoft Internet Explorer версии 8 или выше;

— Почтовый клиент — Почта Windows Mail, Live Mail, Microsoft Outlook Express из состава Internet Explorer и Microsoft Outlook из пакета Microsoft Office.

Требования к обеспечению сетевого взаимодействия:

— Подключение к сети Интернет (через модем, выделенную линию или локальную сеть) на скорости не менее 28800 бит/сек;

— Подключение к почтовому серверу по протоколам SMTP/POP3;

— Поддержка S/MIME используемым почтовым сервером;

— Наличие зарегистрированного и функционирующего адреса электронной почты, который указан в сертификате уполномоченного пользователя.

Базовое программно-аппаратное обеспечение:

— Средство криптографической защиты информации «КриптоПро CSP»;

— Криптографический файловый менеджер «КриптоАРМ».

— Устройства защищенного хранения ключевых документов (электронные идентификаторы/ключи) USB-ключи/Смарт-карты со считывателями;

Дополнительное программно-аппаратное обеспечение:

— Средства защиты от несанкционированного доступа, в т.ч. СЗИ НСД типа «электронный замок».

— Средства антивирусной защиты, средства обнаружения вторжений, персональный межсетевой экран.

16 Дополнительные условия взаимодействия

Участники Системы перед организацией обмена защищенными электронными документами должны согласовать параметры, не установленные настоящим *Регламентом*:

— Перечень видов документов, обмен которыми осуществляется через *Систему*;

— Требования к содержанию/оформлению соответствующих документов;

— Требования к форматам/формам файлов с учетом конкретных приложений и их версий, обеспечивающих автоматизированную обработку;

— Периодичность обмена информацией;

— Перечень уполномоченных должностных лиц, владельцев сертификатов, наделенных правом подписывать соответствующие электронные документы и электронные сообщения (их координатами для оперативного взаимодействия);

— Адреса электронной почты *Участников Системы*;

— Требования внутреннего учета документов;

— Требования к обеспечению конфиденциальности передаваемых сведений.

При необходимости закрепления соглашений в виде отдельного документа рекомендуется использовать Типовое Соглашение об информационном взаимодействии (Приложение А).

17 Ограничения

Оператор не несет ответственность за содержание и достоверность информации, передаваемой между *Участниками Системы*.

Оператор не отвечает за последствия компрометации Участниками своих криптографических ключей, иных нарушений условий использования средств криптографической защиты информации.

18 Разрешение конфликтных ситуаций

В *Системе* возможны конфликтные ситуации, связанные различиями мнениями участников относительно статуса сертификата (действительность электронной подписи) и электронной подписи электронного документа.

Получение информации о статусе сертификата, изданного *Удостоверяющим центром,* осуществляется на основании соответствующего заявления. Заявление должно содержать время и дату, на момент наступления которых требуется установить статус сертификата, и серийный номер сертификата, статус которого требуется установить. По результатам проведения работ по Заявлению оформляется справка, содержащая информацию о статусе сертификата, которая предоставляется заявителю.

Удостоверяющий центр осуществляет проведение экспертных работ по подтверждению подлинности электронной подписи в электронном документе, если формат электронного документа с подписью соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS). Для подтверждения подлинности подписи в электронных документах *Пользователь УЦ* подает Заявление в *Удостоверяющий центр.* Заявление должно содержать время и дату, на момент наступления которых требуется установить подлинность подписи.

Обязательным приложением к заявлению на подтверждение подлинности подписи в электронном документе является сертификат *Пользователя УЦ*, с использованием которого необходимо осуществить подтверждение подлинности подписи в электронном документе (в виде файла стандарта CMS) м проверяемый электронный документ: в виде одного файла (стандарт CMS), содержащего подписанные данные и значение подписи этих данных, или двух файлов — один из которых содержит данные, а другой значение подписи этих данных (стандарт CMS).

Результатом проведения работ по подтверждению подлинности подписи в электронном документе является заключение *Удостоверяющего центра*, содержащее результат проверки подписи электронного документа и обоснованный отчет по выполненной проверке.

В случае если стороны конфликта не приходят к его разрешению, то дальнейшие процедуры проводятся в соответствии с Положением по разрешению споров, связанных с подлинностью электронных документов

Кроме того, участники могут проверить действительность сертификатов и электронной подписи электронных документов с помощью общедоступного сервиса Подтверждение подлинности электронной подписи Минкомсязи России. Предоставляемая сервисом услуга носит информационный характер и не может быть использована в качестве доказательств в судах различных инстанций.

С помощью указанного сервиса можно подтвердить подлинность электронной подписи корневого (самоподписанного) сертификата аккредитованного удостоверяющего центра или подлинность электронной подписи сертификата, изданного аккредитованным удостоверяющим центром.

Указанный сервис предназначен для подтверждения подлинности электронной подписи, основанной на сертификате, изданном аккредитованным удостоверяющим центром, формата PKCS#7 (стандарт CMS) в электронных документах (присоединенная и отсоединенная).

19 Рекомендации по организации защищенного электронного документооборота

Для организации защищенного электронного документооборота рекомендуется назначать необходимое количество уполномоченных должностных лиц, имеющих право подписывать соответствующие электронные документы, при котором обеспечивается бесперебойная работа.

Для хранения ключевой информации пользователей рекомендуется применять надежные защищенные носители криптографических ключей.

На рабочих местах пользователей, производящих обработку зашифрованных документов, должны быть решены вопросы по антивирусной защите, обнаружению вторжений, межсетевому экранированию и защите подключения к сети Интернет.

Хранилища электронных документов должны иметь надежные сертифицированные средства защиты информации, а также регламентированный порядок резервирования информации.

Рекомендуется использовать Журналы учета отправки/получения почтовых сообщений при обмене конфиденциальной информацией. Форма журналов должна соответствовать требованиям, установленным для конфиденциального документооборота.

В целях принятия обоснованного решения о выборе технологии защищенного обмена электронными документами возможно проведение пилотного проекта. В ходе пилотного проекта выполняется установка, проверка работоспособности, тестирование всех функциональных компонентов, производительности и операционных регламентов, а также требований по защите информации в *Системе*, производится оценка *Системы* на предмет защищенности, совместимости и удобства работы с *Системой*, уточняются вопросы обеспечения юридической значимости электронных документов.

Приложение А

Типовое Соглашение об информационном взаимодействии

г. Ижевск «____» _____ 201__ г.

_____

_____

(_____), именуемое в дальнейшем *Первый участник*, в лице _____, действующего на основании _____, и _____

_____

(_____), именуемое в дальнейшем *Второй участник*, в лице _____, действующего на основании _____, с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение об информационном взаимодействии (далее — Соглашение) о нижеследующем:

1 Стороны осуществляют информационное взаимодействие путем обмена конфиденциальными юридически значимыми электронными документами.

2 Правовую основу заключения соглашения и информационного взаимодействия составляют:

— Гражданский кодекс Российской Федерации;

— Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

— Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— Федеральный Закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

— Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

— иные нормативные правовые акты Российской Федерации.

3 Стороны соглашаются использовать для информационного взаимодействия защищенную информационно-телекоммуникационную систему КриптоСвязь {Защищенный Электронный Документооборот} (далее — Система) ООО Научно-производственное предприятие «Ижинформпроект» (далее — Оператор) в порядке и на условиях, определяемых Регламентом системы КриптоСвязь{Защищенный Электронный Документооборот} (далее — Регламент ЗЭД) и другими документами Оператора.

4 Стороны подтверждают, что на момент подписания настоящего Соглашения Стороны надлежащим образом подключены к Системе (имеют договорные отношения с Оператором, оборудованные в соответствии с установленными требованиями автоматизированные рабочие места защищенного электронного документооборота (далее — АРМ-ЗЭД), обученный персонал и должностных лиц, являющихся владельцами квалифицированных сертификатов ключей проверки электронной подписи (далее — квалифицированный сертификат), уполномоченных подписывать соответствующие электронные документы), и обязуются выполнять требования Регламента ЗЭД.

5 Перечень и формы электронных документов, используемых Сторонами для обмена, и временные характеристики информационного взаимодействия Сторон определены в Приложении 1.

6 Стороны для формирования электронных документов могут использовать форматы электронных документов, определенные Регламентом ЗЭД.

7 Стороны признают электронный документ (независимо от того существует такой документ на бумажном носителе или нет), в Системе, подписанный квалифицированной электронной подписью, равнозначным документу на бумажном носителе, подписанному собственноручной подписью участника Системы, а также заверенному печатью, с учетом требований, определенных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и установленных настоящим Соглашением и Регламентом ЗЭД. К исполнению Стороны принимают только электронные документы, подписанные электронной подписью.

8 Стороны признают надежность используемых в Системе сертифицированных в установленном порядке СКЗИ достаточной для подтверждения подлинности участников взаимодействия и обеспечения конфиденциальности передаваемой информации, доступ к которой ограничен федеральными законами (информация ограниченного доступа/конфиденциальная информация).

9 Электронные документы, которыми обмениваются Стороны, подписываются электронной подписью, владелец квалифицированного сертификата которой уполномочен подписывать электронные документы. Полномочия на подписание электронных документов электронной подписью в Системе представители Сторон имеют на основании закона и/или учредительных документов Сторон или на основании приказов/ доверенностей, выданных Сторонами.

10 До начала информационного взаимодействия Стороны обмениваются квалифицированными сертификатами и адресной информацией в соответствии с Регламентом ЗЭД.

11 Электронные документы оформляются в соответствии с требованиями делопроизводства, подготавливаются на бланках установленного образца, должны иметь исходящий номер и дату. Сведения о наличии приложений и именовании файлов, их содержащих, указываются в тексте.

12 Порядок формирования, передачи, приема, обработки, хранения, отображения и печати (создания копий электронных документов на бумажном носителе) электронных документов, а также порядок обеспечения безопасности информации и использования средств защиты информации установлены Регламентом ЗЭД и другими документами Оператора, с учетом требований внутренних нормативных документов Сторон.

13 Стороны обязуются:

— передавать друг другу сведения в составе и порядке, указанном в настоящем Соглашении, с соблюдением требований по защите информации;

— обеспечивать достоверность информации и представление соответствующих сведений в установленные сроки и в полном объеме;

— хранить электронные документы в том формате, в котором они были отправлены или получены, позволяющем установить, что отправленные или полученные данные, содержащиеся в электронном сообщении, не искажены;

— информировать другую Сторону обо всех случаях возникновения технических неисправностей или других обстоятельствах, препятствующих обмену электронными документами;

— соблюдать установленные правила обеспечения информационной безопасности и обращения с ключевыми документами.

14 Ответственность за ущерб, возникший вследствие нарушения конфиденциальности, несет Сторона, допустившая нарушение.

15 За невыполнение или ненадлежащее выполнение обязательств по настоящему Соглашению виновная Сторона несет ответственность в соответствии с законодательством Российской Федерации.

16 Стороны несут ответственность за правильность оформления электронных документов и правильность применения электронной подписи своих уполномоченных представителей.

17 Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Соглашению, если неисполнение явилось следствием обстоятельств непреодолимой силы, которые Сторона не могла предвидеть или предотвратить разумными мерами.

18 При возникновении разногласий и споров, связанных с настоящим Соглашением, Стороны обязуются решать их путем переговоров.

19 Разрешение спорных ситуаций между Сторонами, связанных с использованием в электронных документах электронной подписи осуществляется в соответствии с Регламентом ЭЭД.

20 В случае, если конфликтная ситуация не урегулирована в результате переговоров, Стороны вправе передать неурегулированный спор и разногласия на рассмотрение в Арбитражный суд в соответствии с законодательством Российской Федерации.

21 В случае невозможности передачи электронных документов по телекоммуникационным каналам связи допускается передача электронных документов на магнитном/электронном/оптическом носителе или по другим согласованным каналам связи, при этом порядок использования электронной подписи и шифрования не изменяется. Электронные документы на магнитном/электронном/оптическом носителе доставляются специальной (фельдъегерской) почтовой связью или уполномоченным представителем (курьером) отправителя электронных документов в сроки, определенные настоящим Соглашением.

22 Стороны самостоятельно осуществляют платежи организациям и предприятиям, оказывающим Сторонам услуги по доступу к каналам связи (передачи данных) сети Интернет.

23 Настоящее Соглашение вступает в силу с момента подписания его Сторонами и действует бессрочно.

24 Основанием для прекращения (приостановления) информационного взаимодействия является нарушение требований к информационному взаимодействию, предусмотренных нормативными правовыми актами РФ, регулирующими отношения в сфере информационных технологий и защиты информации с ограниченным доступом, и соглашением Сторон, заявление одной из Сторон о приостановлении информационного взаимодействия, направленное в письменной форме не позднее, чем за три рабочих дня до даты начала приостановления информационного взаимодействия, указанной в заявлении, компрометация ключевой информации одной из Сторон.

25 Все изменения и/или дополнения к настоящему Соглашению действительны, если они совершенны в письменной форме, подписаны полномочными представителями Сторон и заверены оттисками печатей Сторон.

26 Любая Сторона настоящего Соглашения вправе в одностороннем порядке его расторгнуть в любое время его действия, предупредив письменно другую Сторону не позднее, чем за 1 (один) месяц.

27 Настоящее Соглашение составлено в 2 (двух) экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

28 Термины и определения, используемые в настоящем Соглашении, должны пониматься в соответствии с законодательством Российской Федерации, а также в соответствии с терминами и определениями, установленными Регламентом ЗЭД.

29 Юридические адреса сторон:

*Первый участник***:**

_____

_____

_____

Юр. адрес: _____

Факт. адрес: _____

р/счет № _____

Банк _____ БИК _____

кор/счет № _____

ИНН _____ КПП _____ ОГРН _____

Тел. _____ Факс _____ email _____

*Второй участник***:**

_____

_____

_____

Юр. адрес: _____

Факт. адрес: _____

р/счет № _____

Банк _____ БИК _____

кор/счет № _____

ИНН _____ КПП _____ ОГРН _____

Тел. _____ Факс _____ email _____

От *Первый участник*
Генеральный директор

_____ /_____/
«_____» _____201___
м.п.

От *Второй участник*
Генеральный директор

_____ /_____/
«_____» _____201___
м.п.

Приложение 1
к Соглашению об информационном
взаимодействии № _____ от «__» ___ 201__

Перечень и формы электронных документов

1 *Первый участник* в срок до 10 числа каждого месяца (один раз в неделю/ еженедельно):

— выгружает данные за указанный период из Информационного ресурса «123» в формате XML (программы Microsoft Excel 2010),

— подготавливает сопроводительное письмо в формате Microsoft Word 2010,

— электронный документ со всеми приложениями (все файлы) подписываются электронной подписью уполномоченного должностного лица, сжимаются в один файл-архив с помощью программы-упаковщика WinRAR 4.1 и направляются *Второму участнику* вложением к защищенному сообщению электронной почты.

2 *Второй участник* в срок до 15 числа каждого месяца (один раз в неделю/ еженедельно):

— выгружает данные за указанный период из Информационного ресурса «321» в формате XML (программы Microsoft Excel 2010),

— подготавливает сопроводительное письмо в формате Microsoft Word 2010,

— электронный документ со всеми приложениями (все файлы) подписываются электронной подписью уполномоченного должностного лица, сжимаются в один файл-архив с помощью программы-упаковщика WinRAR 4.1 и направляются *Первому участнику* вложением к сообщению защищенной электронной почты.

3 Стороны по мере необходимости обмениваются информационными сообщениями, запросами, другими документами и ответами на них в аналогичном порядке. Электронные документы и приложения к ним подготавливаются в формате Microsoft Office 2010, PDF 1.7, а также JPEG. Содержание указанных документов должно соответствовать условиям сложившейся практики «бумажного» документооборота.

От *Первый участник*	От *Второй участник*
Генеральный директор	Генеральный директор
_____ /_____/	_____ /_____/
«_____» _____200___	«_____» _____200___
м.п.	м.п.

Приложение Б

Примеры наименования файлов

При формировании и отправке

1 Формирование исполнителем электронного документа, подлежащего передаче и сопроводительного письма к нему.

Например: peredach.xls + pism0001.doc

2 Передача указанного комплекта файлов уполномоченному лицу

3 Формирование электронной подписи уполномоченным лицом на передаваемых файлах и возврат их исполнителю.

Например:

peredach.xls + peredach.xls.sig + pism0001.doc + pism0001.doc.sig

4 Регистрация передаваемых конфиденциальных документов в соответствии с правилами делопроизводства.

5 Передача подписанных электронных документов оператору электронной почты.

6 Проверка электронной подписи на представленных файлах.

Например:

peredach.xls + peredach.xls.sig + pism0001.doc + pism0001.doc.sig

7 Формирование оператором электронной почты дополнительного файла с регистрационными реквизитами и формирование к нему электронной подписи (оператора).

Например: num0001.doc + num0001.doc.sig

8 Архивирование комплекта указанных файлов для передачи.

Например:

pism0001.rar = peredach.xls + peredach.xls.sig + pism0001.doc + pism0001.doc.sig + num0001.doc + num0001.doc.sig

9 Занесение информации в журнал учета.

10 Передача архивного файла адресату.

При приеме

1 Прием архивного файла.

Например: pism0001.rar

2 Проверка электронной подписи уполномоченных лиц, указанных в сопроводительном письме и оператора.

Например:

peredach.xls + peredach.xls.sig + pism0001.doc + pism0001.doc.sig + num0001.doc + num0001.doc.sig

3 Занесение информации в журнал учета.

4 Распечатывание полученной информации (сопроводительного письма) и регистрация документов в соответствии с правилами делопроизводства с отметкой в журнале учета.

5 Передача электронных документов исполнителю с отметкой в журнале учета.

Приложение В

Журналы учета конфиденциальных документов

Форма Журнала учета отправки конфиденциальных документов

№	Дата документа	Регистрационный № документа	Наименование документа	Получатель	Адрес электронной почты
1	2	3	4	5	6

Дата и время отправки	Подпись оператора	Дата и время уведомления о прочтении	Подпись оператора	Примечание
7	8	9	10	11

Форма Журнала учета получения конфиденциальных документов

№	Отправитель	Адрес электронной почты	Дата документа	Регистрационный № документа	Наименование документа
1	2	3	4	5	6

Дата и время получения	Подпись оператора	Дата и время передачи на регистрацию	Подпись оператора	Примечание
7	8	9	10	11

20 Лист регистрации изменений

№ п/п	*Дата, №*	*Редакция документа*	*Содержание изменения*
1	23.08.2013 № 16	2	Регламент системы КриптоСвязь{Защищенный Электронный Документооборот} ООО Научно-производственное предприятие «Ижинформпроект» является составной частью Регламента удостоверяющего центра InfoTrust и содержит необходимые требования и условия взаимодействия Участников Системы
2	13.07.2015 № 20	2.1	Дополнена информация о реализации в СКЗИ криптоалгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012
3	17.10.2016 № 13	2.2	Обновлена информация о лицензии ФСБ России
4	29.10.2018 № 8	2.3	Обновлена информация о лицензиях Роскомнадзора