Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

УТВЕРЖДЕНО
приказом от 24.04.2018 № 4

Руководство по безопасности системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб»)

Редакция № 1

КРИПТОВЕБ
ЗАЩИЩЕННЫЙ ДОКУМЕНТООБОРОТ

Ижевск 2018

Реферат

Настоящий документ содержит описание регламентных работ по обеспечению информационной безопасности при эксплуатации системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») Общества с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект».

Руководство разработано в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

Данное руководство предназначено для администратора безопасности *Оператора Системы* и для администраторов безопасности пользователей *Системы*.

Содержание

1 Определения

Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» (КриптоВеб) (Система) — корпоративная информационная система, устроителем которой является Организатор Системы, основанная на технологии Инфраструктуры открытых ключей (ИОК, PKI), в которой используются сертификаты, изготовленные Удостоверяющим центром, построенная на базе программных продуктов КриптоВеб, включая программное обеспечение клиентского рабочего места КриптоВеб, и предназначенная для оказания услуг в области использования электронной подписи/шифрования данных и телематических услуг связи пользователям Системы, действующая по правилам, установленным Оператором Системы в соответствии с нормативными правовыми и иными актами, регулирующими защищенный электронный документооборот и применение электронной подписи.

Оператор Системы/Оператор ЭДО — ООО НПП «Ижинформпроект», устроитель корпоративной информационной системы для обеспечения электронного документооборота с применением электронной подписи, организующий и обеспечивающий предоставление услуг пользователям Системы.

Доверенный способ передачи информации — способ передачи информации, обеспечивающий требуемую степень ее защищенности.

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 Регламент.

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

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).

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

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 (перечень публикуется на сайте www.infotrust.ru), а также аккредитованные удостоверяющие центры, входящие в Перечень доверенных удостоверяющих центров *Системы* (перечень публикуется на сайте www.cryptoweb.ru).

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.

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.

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

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

2 Обозначения и сокращения

CMS	Cryptographic Message Syntax (Синтаксис криптографических сообщений)
CPS	Certification Practice Statement (Регламент Удостоверяющего центра)
PKI	Public Key Infrastructure (Инфраструктура Открытых Ключей)
RFC	Request For Comments
TLS	Transport Layer Security Protocol (Протокол криптографической защиты на транспортном уровне)
URL	Uniform Resource Locator (Единый локатор ресурса)
UTC/GMT	Universal Time Coordinated/Greenwich Mean Time (Универсальное координированное время/Всемирное время «по Гринвичу»)
КСКПЭП	Квалифицированный сертификат ключа проверки электронной подписи (Квалифицированный сертификат)
КС	Квалифицированный сертификат (Квалифицированный сертификат ключа проверки электронной подписи)
КЭП	Квалифицированная электронная подпись
ПО	Программное обеспечение
УЦ	Удостоверяющий центр
ЭДО	Электронный документооборот

3 Введение

3.1 Назначение Системы

Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») — это современный Web-портал защищенного электронного юридически значимого документооборота.

Система «КриптоВеб» включает в себя развитую подсистему электронной отчетности, позволяющую вести юридически значимый обмен данными с контролирующими органами и организациями. Проводится большая работа по увеличению охвата технологией представления электронной отчетности по телекоммуникационным каналам связи, используя пятнадцатилетний опыт работы в системе «КриптоСвязь»{Отчетность через Интернет}.

Система «КриптоВеб» является платформой для создания прикладных защищенных сервисов для комплексной автоматизации процессов, связанных с обработкой конфиденциальной информации.

Серверные компоненты *Системы* «КриптоВеб» размещаются на территории Российской Федерации и располагаются в серверных помещениях *Оператора Системы*, действующего соответствии с требованиями законодательства Российской Федерации и имеющего лицензии ФСБ России и Роскомнадзора.

3.2 Сведения об Операторе

Общество с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект»), предоставляющее услуги *Оператора Системы* в соответствии с требованиями законодательства Российской Федерации, 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 18.08.2013 № 111185;

3) лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание телематических услуг связи от 18.08.2013 № 111186.

Реквизиты ООО НПП «Ижинформпроект»:

ИНН 1831014533 КПП 183101001 ОГРН 1021801161140

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

Фактическое местонахождение: ул. Бородина, 21, офис 207, г. Ижевск, Удмуртская Республика, 426057

Банковские реквизиты:

Удмуртское отделение № 8618 ПАО СБЕРБАНК г. Ижевск

р/с 40702810768170101530

к/с 30101810400000000601

БИК 049401601

Контактная информация

телефон/факс: +7 (3412) 918-100,

e-mail: info@cryptoweb.ru

www: www.cryptoweb.ru

3.3 Идентификация документа

Наименование документа — Руководство по безопасности системы защищенного юридически значимого электронного документооборота «КриптоСвязь-Веб» («КриптоВеб»).

Версия: 1.

Дата: 24.04.2018.

Количество страниц в документе: 34.

3.4 Статус документа

Руководство по безопасности системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») (далее — Руководство) разработано в соответствии с действующим законодательством Российской Федерации и определяет требования к организационным и техническим мерам по обеспечению безопасности информации ограниченного доступа с применением сертифицированных средств защиты информации в серверных и клиентских компонентах *Системы* защищенного юридически значимого электронного документооборота.

Любые справки по вопросам, связанным с предоставлением услуг *Оператора*, предоставляются сотрудниками *Оператора* по телефону +7 (3412) 918-100 и info@cryptoweb.ru.

3.5 Изменения (дополнения) документа

Внесение изменений (дополнений) в Руководство, включая приложения к нему, производится *Оператором* в одностороннем порядке.

Все изменения (дополнения), вносимые *Оператором* в Руководство и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными для доверенных удостоверяющих центров по истечении 30 (тридцати) календарных дней с момента направления *Оператором* указанных изменений и дополнений в Руководство.

Все изменения (дополнения), вносимые *Оператором* в Руководство в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

Любые изменения и дополнения в Руководство с момента вступления в силу равно распространяются на всех участников *Системы*.

4 Правовые основания обработки информации с ограниченным доступом

4.1 Ограничение доступа к информации

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет:

— 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;

— оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

— конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Ограничение доступа к информации может быть установлено федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. При этом соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, является обязательным.

Соответствующими федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Профессиональная тайна (информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности), подлежит защите в случаях,

если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

4.2 Виды конфиденциальной информации

В настоящее время в Российской Федерации существует большое количество видов информации с ограниченным доступом, которые можно сгруппировать по категориям:

— Персональные данные (статья 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

— Коммерческая тайна (Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»);

— Служебная тайна (служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами, Указ Президента РФ от 06.03.1997 №188);

— Профессиональная тайна, в том числе:

— Налоговая тайна (статьи 102 и 313 Налогового кодекса РФ);

— Банковская тайна (статья 857 Гражданского кодекса РФ);

— Врачебная тайна (статьи 13, 92 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»);

— Нотариальная тайна (статьи 16 и 28 Основ законодательства Российской Федерации о нотариате от 11.02.1993 № 4462-1);

— Адвокатская тайна (статья 8 Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»);

— Аудиторская тайна (статья 9 Федерального закона от 30.12.2008 № 307-ФЗ «Об аудиторской деятельности»);

— Тайна страхования (статья 946 Гражданского кодекса РФ);

— Тайна ломбарда (статья 3 Федерального закона от 19.07.2007 № 196-ФЗ «О ломбардах»);

— Тайна связи (статья 23 Конституции РФ);

— Тайна завещания (статья 1123 Гражданского кодекса РФ);

— Тайна усыновления (статья 139 Семейного кодекса РФ);

— Тайна следствия (статья 161 Уголовно-процессуального кодекса РФ);

— Тайна судопроизводства (статья 194 Гражданского процессуального кодекса РФ, статья 20 Арбитражного процессуального кодекса РФ, статьи 298 и 341 Уголовно-процессуального кодекса РФ, статья 175 Кодекса административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ);

и многие другие (конфиденциальность арбитража, сведения о защищаемых лицах, сведения, ставшие известными гражданам в ходе оперативно-розыскной деятельности, сведения экспертизы по административному делу, секрет производства (ноу-хау), кредитная история, конфиденциальность фискальных данных, инсайдерская информация, дактилоскопическая информация, контрольные измерительные материалы при проведении государственной итоговой аттестации, тайна исповеди и т.д.).

4.3 Защита информации

В соответствии со статьей 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

5 Общие методы и механизмы обеспечения безопасности информационных технологий

5.1 Архитектура безопасности взаимосвязи открытых систем

Современные сложные информационные системы проектируются с учетом идеологии эталонной модели взаимосвязи открытых систем, которая позволяет пользователю системы получить доступ к информационным ресурсам.

Архитектура безопасности взаимосвязи открытых систем предусматривает семь уровней иерархии: физический, канальный, сетевой, транспортный, сеансовый, представительный и прикладной. Для защиты информации на физическом и канальном уровне обычно вводится такой механизм защиты, как канальное шифрование с помощью специальных шифраторов. Применение только канального шифрования не обеспечивает полного закрытия информации при ее передаче, так как на узлах коммутации пакетов информация будет находиться в открытом виде. Поэтому несанкционированный доступ нарушителя к аппаратуре одного узла ведет к раскрытию всего потока сообщений, проходящих через этот узел. В том случае, когда устанавливается виртуальное соединение между двумя абонентами сети, необходимо сквозное шифрование (организуется на сетевом и/или транспортном уровнях), когда закрывается информационная часть сообщения, а заголовки сообщений не шифруются. На прикладном уровне реализуется большинство механизмов защиты, необходимых для полного решения проблем обеспечения безопасности данных.

Архитектура безопасности взаимосвязи открытых систем предусматривает следующие службы безопасности:

— обеспечения целостности данных;

— обеспечения конфиденциальности данных;

— контроля доступа;

— аутентификации (одноуровневых объектов и источника данных);

— обеспечения конфиденциальности трафика;

— обеспечения невозможности отказа от факта отправки/получения сообщения.

5.2 Методы и механизмы безопасности

В конечном счете задача защиты информационных технологий разбивается на частные подзадачи, такие как: обеспечение конфиденциальности, целостности и доступности. Для этих подзадач вырабатываются конкретные решения по организации взаимодействия объектов и субъектов информационных систем. К таким решениям относятся методы:

— аутентификации субъектов и объектов информационного взаимодействия, предназначенные для предоставления взаимодействующим сторонам возможности удостовериться, что противоположная сторона действительно является тем, за кого себя выдает;

— шифрования информации, предназначенные для защиты информации в случае перехвата ее третьими лицами;

— контроля целостности, предназначенные для обеспечения того, чтобы информация не была искажена или подменена;

— управления доступом, предназначенные для разграничения доступа к информации различных пользователей;

— повышения надежности и отказоустойчивости функционирования системы, предназначенные для обеспечения гарантий выполнения информационной системой целевых функций;

— управления ключами, предназначенные для организации создания, распространения и использования ключей субъектов и объектов информационной системы, с целью создания необходимого базиса для процедур аутентификации, шифрования, контроля подлинности и управления доступом.

6 Архитектура системы КриптоВеб

6.1 Принципы обработки информации в Системе

При разработке *Системы* были заложены следующие принципы обработки конфиденциальной информации в *Системе* «КриптоВеб»:

— конфиденциальная информация доступна только отправителю и получателю информации, информационные пакеты обрабатываются *Оператором* строго в зашифрованном виде;

— участники идентифицируются по сведениям, содержащимся в квалифицированном сертификате ключа проверки электронной подписи, и имеют соответствующие полномочия;

— для обеспечения криптографической аутентификации и юридической значимости электронных документов используется только квалифицированная электронная подпись;

— технологические цепочки прохождения электронных документов обеспечивают фиксацию времени осуществления всех этапов прохождения документа;

— для криптографической защиты информации используются только сертифицированные средства.

В ходе эксплуатации *Системы* «КриптоВеб» *Оператор* обеспечивает:

— наличие лицензий на виды деятельности, подлежащие обязательному лицензированию;

— наличие прав на программы для электронных вычислительных машин и базы данных;

— наличие сертификата соответствия ГОСТ Р на используемое программное обеспечение;

— использование сертифицированных средств для криптографической защиты информации и защиты от несанкционированного доступа;

— подтверждение соответствия автоматизированной системы установленным требованиям нормативной документации по безопасности информации.

6.2 Компоненты Системы

В *Системе* «КриптоВеб» для обеспечения технологических процессов защищенного электронного документооборота выделяются следующие компоненты *Системы*:

— Серверные компоненты *Оператора*, предназначенные для хранения информационных ресурсов, организации предоставления доступа к ним, формирования и подписи служебных документов *Оператора*, обеспечения временных отметок служебных документов в соответствии с технологическими процессами;

— АРМ Пользователя — тонкий клиент, предназначенный для подключения к информационным ресурсам *Оператора* по защищенному каналу, обеспечивающий создание электронных документов и отчетов, формирование и проверку квалифицированной электронной подписи, зашифрование и расшифрование электронных документов и отчетов, работу с прикладными защищенными сервисами;

— АРМ Контролирующего органа — тонкий или «толстый» клиент (клиент-приложение), предназначенный для подключения к информационным ресурсам *Оператора* по защищенному каналу, обеспечивающий прием отчетных и служебных документов, формирование и проверку квалифицированной электронной подписи, зашифрование и расшифрование электронных документов и отчетов.

6.3 Механизмы обеспечения безопасности

В *Системе* «КриптоВеб» для решения основных задач для обеспечения защищенного электронного документооборота, представления отчетности и работы прикладных защищенных сервисов, применяются криптографические механизмы, основанные на сертифицированных средствах криптографической защиты информации:

— криптографическая аутентификация пользователей и сервера *Оператора* на основе квалифицированных сертификатов ключей проверки электронных подписей;

— обеспечение невозможности отказа от факта отправки/получения сообщения и юридическая значимость электронных документов на основе квалифицированной электронной подписи;

— шифрование документов и данных на рабочем месте пользователя в адрес получателей и отправителя и шифрование канала связи при соединении АРМ Пользователя с сервером *Оператора*;

— контроль целостности документов и данных с применением квалифицированной электронной подписи и имитозащита канала связи при соединении АРМ Пользователя с сервером *Оператора*;

— управление доступом пользователей к конфиденциальным документам и данным на основе квалифицированных сертификатов ключей проверки электронных подписей;

— управление ключами пользователей информационной системы для обеспечения процедур аутентификации, шифрования, контроля подлинности и управления доступом производится на основе стандартных служб инфраструктуры открытых ключей, формируемой аккредитованным удостоверяющим центром.

В дополнение к указанным механизмам, реализованным в *Системе*, обеспечивается контроль доступа к средствам обработки информации *Оператора* и Пользователя, межсетевое экранирование для защиты подключения к сети Интернет, а также обнаружение компьютерных атак и антивирусная защита информации.

Кроме того, для повышения надежности и отказоустойчивости функционирования *Системы Оператор* принимает меры по обеспечению резервирования и восстановления информации, а также взаимодействие с Интернет-провайдерами, через которых производится подключение оборудования *Оператора* к Сети.

6.4 Используемые средства защиты информации

Для обеспечения криптографических операций *Оператор* применяет сертифицированное по классу КС2 средство криптографической защиты информации.

Для обеспечения защиты от несанкционированного доступа применяются сертифицированные средства, предназначенные для обеспечения защищенности до классов 1Б/УЗ1/ГИС1.

Подключение информационной системы *Оператора* к информационно-телекоммуникационным сетям международного информационного обмена производится с использованием специально предназначенных для этого средств защиты информации, сертифицированных ФСБ России.

Для антивирусной защиты применяется сертифицированное по классам А2/Б2/В2/Г2 средство защиты.

Для обеспечения возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней, применяются специализированные средства резервного копирования.

Для предотвращения несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации, предупреждения возможности неблагоприятных последствий нарушения порядка доступа к информации и недопущения воздействия на технические средства обработки информации, в результате которого нарушается их функционирование, *Оператором* применяются меры пропускного и внутриобъектового режима.

Аттестат соответствия от 13.02.2017 № 02/17К-АЗИ подтверждает, что автоматизированная система «КриптоВеб», имеющая класс защищенности 1Г, соответствует требованиям нормативной документации по безопасности информации, что позволяет организовать защищенную обработку конфиденциальной информации (коммерческая, служебная, профессиональная тайна, персональные данные и т.п.).

7 Криптографические методы защиты информации

7.1 Средства криптографической защиты информации

В *Системе* используются средства криптографической защиты информации «КриптоПро CSP», на основе которого производится шифрование и квалифицированная электронная подпись электронных документов, аутентификация участников и шифрование и имитозащита канала передачи данных. Применяемые версии указанных средств криптографической защиты информации должны соответствовать требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

Для обеспечения аутентификации и защиты канала передачи данных по протоколу TLS, шифрования электронных документов и применения электронных подписей в формате CMS применяются:

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

— алгоритм формирования и проверки электронной 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 использованием RFC 4357, RFC 4490 и RFC 4491.

Максимальные сроки действия криптографических ключей и квалифицированных сертификатов доверенного удостоверяющего центра и *Абонентов Системы* должны удовлетворять требованиям эксплуатационной документации на применяемые сертифицированные в установленном порядке средства криптографической защиты информации и средства удостоверяющего центра.

7.2 Доверенный удостоверяющий центр

Доверенный удостоверяющий центр *Системы* выполняет функции, предусмотренные ст. 13 и ст. 15 Федерального закона Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Доверенный удостоверяющий центр *Системы* имеет:

1) Лицензию Федеральной службы безопасности Российской Федерации на осуществление деятельности 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) по следующим видам выполняемых работ и оказываемых услуг: Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств; Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или

индивидуального предпринимателя); Передача шифровальных (криптографических) средств; Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

2) Свидетельство об аккредитации удостоверяющего центра в соответствии с Федеральным законом Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Ключи электронной подписи и ключи проверки электронной подписи (далее — криптографические ключи) изготавливаются доверенным удостоверяющим центром с условием обеспечения конфиденциальности ключей электронной подписи по поручению владельца квалифицированного сертификата или самостоятельно владельцем с использованием средств, предоставляемых доверенным удостоверяющим центром.

Доверенный удостоверяющий центр использует в своей деятельности сертифицированное средство удостоверяющего центра по классу не ниже КС2. При формировании криптографических ключей удостоверяющим центром и квалифицированных сертификатов используется сертифицированное средство криптографической защиты информации по классу не ниже КС2. Сертификаты соответствия на используемые средства криптографической защиты информации и средства удостоверяющего центра должны быть действительны в течение всего срока действия статуса доверенного удостоверяющего центра.

Автоматизированная система доверенного удостоверяющего центра, содержащая программно-аппаратный комплекс средств обеспечения деятельности, обеспечивает обработку конфиденциальной информации и соответствует установленным требованиям нормативной документации по безопасности информации по классу не ниже 1Г. Аттестат соответствия должен быть действителен в течение всего срока действия статуса доверенного удостоверяющего центра.

Период выпуска доверенным удостоверяющим центром списка отозванных сертификатов не более 24 часов. При этом интервал перекрытия между моментом публикации и сроком действительности не более 4 часов. Доступ к публикуемым спискам отозванных сертификатов обеспечивается по различным каналам связи (публикация списков отозванных сертификатов на двух и более www-серверах, доступных через разные Интернет-провайдеры). Информация о точках публикации списка отозванных сертификатов доверенного удостоверяющего центра включается в изготавливаемые квалифицированные сертификаты.

7.3 Квалифицированные сертификаты

Абоненты Системы используют, принимают и признают квалифицированные сертификаты ключей проверки электронной подписи, созданные Аккредитованным Удостоверяющим центром InfoTrust ООО НПП «Ижинформпроект» и аккредитованными удостоверяющими центрами, входящими в Перечень доверенных удостоверяющих центров *Системы*.

Для получения в *Удостоверяющем центре* квалифицированного сертификата *Абонент Системы* обращается в *Удостоверяющий центр* в порядке, определенном Регламентом *Удостоверяющего центра*.

Квалифицированные сертификаты соответствуют требованиям:

— Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

— Приказа ФСБ РФ от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

8 Соответствие требованиям

8.1 Функции Оператора, лицензирование деятельности

Основные функции *Оператора*:

— обеспечение функционирования программно-аппаратного комплекса *Системы*;

— обеспечение технологических процессов защищенного электронного документооборота и отчетов в *Системе*;

— обеспечение точного времени в *Системе*;

— подключение и техническая поддержка пользователей *Системы*.

Для выполнения своих функций *Оператор* должен иметь следующие лицензии на осуществление своей деятельности на территории Российской Федерации:

— лицензия ФСБ России 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);

— 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;

— лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание телематических услуг связи.

8.2 Обязанности Оператора Системы

Выполнять требования нормативных документов органов исполнительной власти при обеспечении обмена информацией по телекоммуникационным каналам связи в рамках электронного документооборота, в отношении которого такие требования установлены.

Обеспечить функционирование программно-аппаратного комплекса *Системы* в соответствии с требованиями эксплуатационной документации на него.

Осуществлять техническую поддержку программных средств *Абонентов Системы*.

8.3 Обязанности Удостоверяющего центра

Выполнять функции, предусмотренные Федеральным законом Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Выполнять требования нормативных документов органов исполнительной власти при осуществлении функций удостоверяющего центра.

Использовать сертифицированные средства криптографической защиты информации и средства удостоверяющего центра в соответствии с требованиями, определенными эксплуатационной документацией.

Принимать меры для предотвращения несанкционированного доступа к средствам удостоверяющего центра с установленными на них средствами криптографической информации, а также в помещения, в которых они установлены. Своевременно проводить оценку соответствия автоматизированной системы, содержащей программно-аппаратный комплекс средств обеспечения деятельности, установленным требованиям нормативной документации по безопасности информации для обработки конфиденциальной информации.

Своевременно публиковать списки отозванных сертификатов и обеспечивать к ним круглосуточный доступ по различным каналам связи (публикация списков отозванных сертификатов на двух и более www-серверах, доступных через разные Интернет-провайдеры).

Оказывать *Абонентам Системы* техническую поддержку по использованию квалифицированных сертификатов, изготовленных *Удостоверяющим центром*.

Немедленно информировать *Оператора Системы* о факте компрометации ключей электронной подписи и прекратить использование ключей электронной подписи в случае их компрометации.

8.4 Уровни защищенности и классы защиты

Применяемые в *Системе* «КриптоВеб» средства соответствуют уровню криптографической защиты класса КС2, что обеспечивает защиту от воздействий нарушителей типа Н1 и Н2:

— Н1 — нарушитель, не имеющий права доступа в контролируемую зону и не имеющий доступа к функциональным возможностям программно-аппаратных средств, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак;

— Н2 — нарушитель, имеющий право постоянного или разового доступа в контролируемую зону, не имеющий права доступа к средствам вычислительной техники, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак.

9 Требования по обеспечению безопасности АРМ Пользователя

9.1 Общие вопросы

Использовать сертифицированные средства криптографической защиты информации в соответствии с требованиями, определенными эксплуатационной документацией.

Обеспечивать требования нормативных актов контролирующих органов по обеспечению поэкземплярного учета СКЗИ, размещению, специальному оборудованию, охране и организации режима в помещениях с АРМ Пользователя.

Принимать меры для предотвращения несанкционированного доступа к АРМ Пользователя с установленными на них средствами криптографической информации, а также в помещения, в которых они установлены.

9.2 Особенности обработки информации в ИСПДн

В случае использования АРМ Пользователя *Системы* «КриптоВеб» как составной части информационной системы обработки персональных данных организации соответствующего уровня защищенности необходимо обеспечить выполнение требований Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказа ФСТЭК от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9.3 Особенности обработки информации в ГИС

В случае использования АРМ Пользователя *Системы* «КриптоВеб» как составной части государственной информационной системы соответствующего класса защиты необходимо обеспечить выполнение требований статей 11.1 и 14

Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в части обеспечения обмена информацией в форме электронных документов при осуществлении полномочий органов государственной власти и органов местного самоуправления, создания и эксплуатации государственной информационной системы.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

Организационные мероприятия должны производиться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

Необходимо обеспечить выполнение требований Приказа ФСТЭК от 11.02.2013 № 17 «О защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Согласно Указу Президента Российской Федерации от 17.03.2008 года № 351 «О мерах по обеспечению информационной безопасности российской федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» для обеспечения безопасности подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, содержащих информацию, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе СКЗИ, сертифицированных ФСБ России и (или) получивших подтверждение соответствия в ФСТЭК России.

10 Рекомендации по комплексной защите информации

Использовать сертифицированные в соответствии с требованиями по безопасности информации специализированные носители для хранения криптографических ключей — USB-ключи/Смарт-карты.

При подключении к Сети и веб-серверам *Системы* рекомендуется использовать сертифицированные в соответствии с требованиями по безопасности информации межсетевые экраны, средства обнаружения компьютерных атак и анализа защищенности.

Для обеспечения комплексной защиты информации на объекте информатизации рекомендуется своевременно проводить оценку соответствия автоматизированной системы, содержащей АРМ Пользователя, установленным требованиям нормативной документации по безопасности информации для обработки конфиденциальной информации.

11 Конфиденциальность информации

Под конфиденциальной информацией подразумевается любая информация и данные, представляющие собой коммерческую, служебную или иную тайну и персональные данные, доступ к которым ограничивается в соответствии с законодательством Российской Федерации, а также любая иная информация, помеченная как конфиденциальная или в письменном виде явно определенная в качестве таковой.

Участники Системы, получившие конфиденциальную информацию, обязаны охранять ее конфиденциальность и, если иное прямо не установлено законом, не раскрывать эту информацию, как полностью, так и частично, третьим лицам, за исключением работников или контрагентов, которым эта информация необходима для выполнения возложенных на них обязательств.

К конфиденциальной информации не относится информация, которая: была известна стороне, получившей информацию, до ее предоставления; самостоятельно созданная этой Стороной до такого предоставления; стала общеизвестной не по причине действий или бездействия стороны, получившей информацию.

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

Персональные данные, содержащиеся в сертификатах *Пользователей УЦ*, на основании согласия *Пользователя УЦ* относятся к категории общедоступных. В сведениях об учетных записях пользователей *Абонентов Системы*, доступных *Абонентам Системы*, могут быть использованы только общедоступные персональные данные, полученные из сертификатов Пользователей УЦ.

Участники Системы имеют право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

12 Лист регистрации изменений

№ п/п	*Дата, №*	*Редакция документа*	*Содержание изменения*