УТВЕРЖДЕН

приказом БУ «Центр информационных технологий» Мининформполитики Чувашии от 30.08.2018 № 73

РЕГЛАМЕНТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА БУ «ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ» МИНИНФОРМПОЛИТИКИ ЧУВАШИИ

г. Чебоксары, 2018

СОДЕРЖАНИЕ

1. Сведения об Удостоверяющем центре

Бюджетное учреждение Чувашской Республики «Центр информационных технологий» Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики осуществляет деятельность по предоставлению услуг удостоверяющего центра в соответствии с федеральными законами «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», принимаемыми в соответствии с ним правовыми актами, Регламентом Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии (далее также – Регламент).

Удостоверяющий центр БУ «Центр информационных технологий» Мининформполитики Чувашии (далее также – Удостоверяющий центр) осуществляет свою деятельность на основании:

лицензии 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), выданной Управлением ФСБ России по Чувашской Республике от 18 апреля 2017 г. № 113. Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности: работы, предусмотренные пунктами 2, 3, 7, 8, 9, 11-15, 17, 18, 20-28 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313;

Свидетельства об аккредитации удостоверяющего центра, выданного Министерством связи и массовых коммуникаций Российской Федерации от 19 октября 2017 г. № 800.

Реквизиты БУ «Центр информационных технологий» Мининформполитики Чувашии:

Полное наименование юридического лица: Бюджетное учреждение Чувашской Республики «Центр информационных технологий» Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики.

Сокращенное наименование юридического лица: БУ «Центр информационных технологий» Мининформполитики Чувашии.

Место нахождение и фактический адрес: 428022, Чувашская Республика, г. Чебоксары. ул. Калинина, 112.

ОГРН: 1162130063501, ИНН: 2130176633, КПП: 213001001

Банковские реквизиты:

Отделение – НБ Чувашской Республики г. Чебоксары

р/с 40601810600003000003

л/с 20266Б02401 (Минфин Чувашии)

БИК 049706001

Контактная информация:

Адрес сайта БУ «Центр информационных технологий» Мининформполитики Чувашии в информационно-телекоммуникационной сети «Интернет» http://cit.cap.ru.

Адрес сайта Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии в информационно-телекоммуникационной сети «Интернет» http://uc-cit.cap.ru.

Контактные телефоны сотрудников УЦ:

Телефон: (8352) 56-54-94, 56-54-99; e-mail: uc-info@cap.ru

2. Термины и определения

В настоящем Регламенте используются термины и определения, установленные Федеральным законом «Об электронной подписи», а также термины и определения, их дополняющие и конкретизирующие, а именно:

Администратор Удостоверяющего центра (далее также – Администратор УЦ) – уполномоченное лицо Удостоверяющего центра, являющееся сотрудником БУ «Центр информационных технологий» Мининформполитики Чувашии, наделенное полномочиями по созданию ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, управлению (выдача, аннулирование, прекращение, приостановление и возобновление действия) сертификатами ключей проверки электронной подписи Пользователей Операторов, и программно-аппаратных средств Удостоверяющего центра, полномочиями по заверению копий сертификатов ключей проверки электронной подписи на бумажном носителе, выданных Удостоверяющим центром, а также иными полномочиями согласно настоящему Регламенту.

Ключ электронной подписи Удостоверяющего центра – ключ электронной подписи, использующийся Удостоверяющим центром для создания сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.

Копия сертификата ключа проверки электронной подписи - документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра и заверенный печатью Удостоверяющего центра. Содержательная часть копии сертификата ключа проверки электронной подписи соответствует содержательной части сертификата ключа проверки электронной подписи. Структура копии сертификата ключа проверки электронной подписи определяется настоящим Регламентом.

Оператор Удостоверяющего центра (далее также – Оператор УЦ) – уполномоченное лицо Удостоверяющего центра, являющееся сотрудником БУ «Центр информационных технологий» Мининформполитики Чувашии, наделенное полномочиями по обеспечению создания ключей электронной подписи, ключей проверки электронной подписи, сертификатов ключей проверки электронной подписи, управлению (выдача, аннулирование, прекращение) сертификатами ключей проверки электронной подписи Пользователей Удостоверяющего центра, а также полномочиями по заверению копий сертификатов ключей проверки электронной подписи на бумажном носителе, выданных Удостоверяющим центром.

Пользователь Удостоверяющего центра (далее также – Пользователь УЦ) – физическое лицо, являющееся владельцем ключа проверки электронной подписи, либо физическое лицо, действующее от имени владельца ключа проверки электронной подписи, если владелец ключа проверки электронной подписи – юридическое лицо, и указанное в сертификате ключа проверки электронной подписи наряду с наименованием

этого юридического лица. Допускается не указывать в сертификате ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в том случае, если указанный сертификат используется для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 08:00 до 12:00 и с 13.00 до 17.00 (время Московское) ежедневно с понедельника по пятницу за исключением выходных и праздничных дней.

Сертификат ключа проверки электронной подписи Удостоверяющего центра – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи Удостоверяющего центра в созданных им сертификатах ключей проверки электронной подписи и списках отозванных сертификатов.

Сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в электронных ответах Службы актуальных статусов сертификатов, содержащих информацию о статусе сертификатов, выданных Удостоверяющим центром.

Сертификат ключа проверки электронной подписи Службы штампов времени Удостоверяющего центра – сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в штампах времени, сформированных Службой штампов времени Удостоверяющего центра.

Служба актуальных статусов сертификатов – сервис Удостоверяющего центра (построенный на базе протокола OCSP), с использованием которого подписываются квалифицированной электронной подписью и предоставляются Пользователям УЦ электронные ответы, содержащие информацию о статусе сертификатов, выданных Удостоверяющим центром.

Служба штампов времени – сервис Удостоверяющего центра (построенный на базе протокола TSP), с использованием которого подписываются квалифицированной электронной подписью и предоставляются Пользователям УЦ штампы времени.

Список отозванных сертификатов (СОС) – электронный документ с квалифицированной электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на этот определенный момент времени аннулированы или действие которых приостановлено.

Удостоверяющий центр – структурное подразделение БУ «Центр информационных технологий» Мининформполитики Чувашии, осуществляющее выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи». Удостоверяющий центр с момента аккредитации уполномоченным федеральным органом исполнительной власти Российской Федерации в сфере использования электронной подписи осуществляет создание и выдачу квалифицированных сертификатов ключей проверки электронной подписи.

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

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.

CryptographicMessageSyntax (CMS) – стандарт, определяющий формат и синтаксис криптографических сообщений.

3. Статус Регламента

3.1. Регламент Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии, разработан в соответствии с федеральными законами «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения в области информационных технологий и использования электронных подписей.

3.2. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

3.3. Настоящий Регламент определяет порядок реализации функций, осуществления прав и исполнения обязанностей Удостоверяющего центра, порядок и условия предоставления услуг Удостоверяющего центра, а также права, обязанности, ответственность лиц, присоединившихся к Регламенту.

3.4. Настоящий Регламент распространяется:

в форме электронного документа путем размещения на сайте Удостоверяющего центра в информационно-телекоммуникационной сети «Интернет» по адресу http://uc-cit.cap.ru;

в форме документа на бумажном носителе по адресу: 428022, Чувашская Республика, г. Чебоксары. ул. Калинина, 112.

4. Общие положения

4.1. Присоединение к Регламенту

4.1.1. Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления заинтересованным лицом в Удостоверяющий центр Заявления о присоединении к Регламенту по форме Приложения № 1 настоящего Регламента.

4.1.2. С момента регистрации Заявления о присоединении к Регламенту в Удостоверяющем центре лицо, подавшее Заявление, считается присоединившимся к Регламенту и является Стороной Регламента.

4.1.3. Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации Заявления о присоединении к Регламенту в случае ненадлежащего оформления необходимых регистрационных документов, ненадлежащего оформления Заявления об изготовлении сертификата, предоставление документов не в полном объеме или предоставление документов, подлинность которых вызывает сомнения.

4.1.4. Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении в реестре Удостоверяющего центра. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

4.1.5. После присоединения к Регламенту Удостоверяющий центр и Сторона, присоединившаяся к Регламенту, вступают в соответствующие договорные отношения.

4.2. Порядок расторжения Регламента

4.2.1. Действие настоящего Регламента может быть прекращено по инициативе одной из Сторон в следующих случаях:

по собственному желанию одной из Сторон;

нарушения одной из Сторон условий настоящего Регламента.

4.2.2. В случае расторжения Регламента инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за 30 (тридцать) календарных дней до даты расторжения Регламента. Регламент считается расторгнутым после выполнения Сторонами своих обязательств.

4.2.3. Прекращение действия Регламента не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

4.3. Изменение (дополнение) Регламента

4.3.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

4.3.2. Уведомление о внесении изменений (дополнений) в Регламент осуществляется Удостоверяющим центром путем обязательного размещения на сайте Удостоверяющего центра в информационно-телекоммуникационной сети «Интернет» (далее также – сайт Удостоверяющего центра) по адресу http://uc-cit.cap.ru новой версии Регламента, включающего внесенные изменения.

4.3.3. Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент, не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными по истечении одного месяца с даты размещения указанных изменений и дополнений в Регламенте на сайте Удостоверяющего центра по адресу http://uc-cit.cap.ru.

4.3.4. Все изменения (дополнения), вносимые Удостоверяющим центром в Регламент в связи с изменениями в нормативных правовых актах, регулирующих отношения в области использования электронных подписей, вступают в силу одновременно с вступлением в силу изменений в указанных нормативных правовых актах.

4.3.5. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Сторона Регламента имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренном п.4.2. настоящего Регламента.

4.3.6. Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

4.4. Применение Регламента

4.4.1. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

4.4.2. В случае противоречия и (или) расхождения названия какого-либо раздела Регламента со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

4.4.3. В случае противоречия и (или) расхождения положений какого-либо приложения к настоящему Регламенту с положениями собственно Регламента, Стороны считают доминирующим смысл и формулировки Регламента.

5. Предоставление информации

5.1. Удостоверяющий центр осуществляет свою деятельность в качестве аккредитованного в соответствии с Федеральным законом «об электронной подписи» удостоверяющего центра. С информацией об аккредитованном Удостоверяющем центре БУ «Центр информационных технологий» Мининформполитики Чувашии можно ознакомиться на портале уполномоченного федерального органа в области использования электронной подписи по адресу https://e-trust.gosuslugi.ru/CA.

5.2. Документы и иная информация, касающаяся деятельности Удостоверяющего центра, размещается в электронном виде на сайте Удостоверяющего центра по адресу http://uc-cit.cap.ru.

5.3. Удостоверяющий центр вправе запросить, а Сторона, присоединившаяся к Регламенту, обязана предоставить сведения, необходимые для изготовления квалифицированного сертификата ключа проверки электронной подписи (далее также – сертификат), а также следующие документы либо их надлежащим образом заверенные копии:

5.3.1. Заявители, являющиеся юридическими лицами, предоставляют:

1) основной документ, удостоверяющий личность, либо его надлежащим образом заверенную копию (для должностного лица, сведения о котором включаются в сертификат наряду с указанием наименования юридического лица);

2) страховое свидетельство государственного пенсионного страхования либо ее надлежащим образом заверенную копию (предоставляется в случае необходимости включения в сертификат данных СНИЛС);

3) учредительные документы либо их надлежащим образом заверенные копии, содержащие сведения о наименовании и месте нахождении юридического лица;

4) свидетельство о постановке на учет юридического лица в налоговом органе либо ее надлежащим образом заверенную копию

5) свидетельство о государственной регистрации юридического лица или свидетельство о внесении записи в Единый государственный реестр юридических лиц о юридическом лице, зарегистрированном до 1 июля 2002 года, либо ее надлежащим образом заверенную копию;

6) выписку из Единого государственного реестра юридических лиц, полученную не ранее чем за один месяц до момента обращения в Удостоверяющий центр, либо ее надлежащим образом заверенную копию;

7) документы или сведения (информация об официальном источнике опубликования и (или) общедоступных изданиях и информационных системах), подтверждающие полномочия лица, обращающегося за получением сертификата, действовать от имени юридического лица;

8) доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц (если заявитель действует от имени других лиц);

9) сведения, необходимые для направления в единую систему идентификации и аутентификации (далее также – ЕСИА) о лице, получающим сертификат, в объеме, необходимом для регистрации в ЕСИА;

10) иные документы, подтверждающие сведения, включаемые в сертификат и необходимые для использования электронной подписи в информационных системах.

Заявитель вправе по собственной инициативе представить надлежащим образом заверенные копии документов, указанных в подпунктах 3-6 пункта 5.3.1 настоящего Регламента, либо копии указанных документов в электронном виде, подписанные усиленной квалифицированной электронной подписью лица, имеющего право действовать от имени заявителя – юридического лица.

5.3.2. Заявители, являющиеся индивидуальными предпринимателями, предоставляют:

1) основной документ, удостоверяющий личность, либо его нотариально заверенную копию;

2) страховое свидетельство государственного пенсионного страхования либо ее нотариально заверенную копию;

3) свидетельство о постановке на учет физического лица в налоговом органе либо ее нотариально заверенную копию;

4) свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя, либо ее нотариально заверенную копию;

5) выписку из Единого государственного реестра индивидуальных предпринимателей, полученную не ранее чем за один месяц до момента обращения в Удостоверяющий центр, либо ее нотариально заверенную копию;

6) нотариально заверенную доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц (если заявитель действует от имени других лиц);

7) сведения, необходимые для направления в ЕСИА о лице, получающим сертификат, в объеме, необходимом для регистрации в ЕСИА;

8) иные документы, подтверждающие сведения, включаемые в сертификат и необходимые для использования электронной подписи в информационных системах.

Заявитель вправе по собственной инициативе представить нотариально заверенные копии документов, указанных в подпунктах 4-5 пункта 5.3.2 настоящего Регламента, либо копии указанных документов в электронном виде, подписанные усиленной квалифицированной электронной подписью заявителя.

5.3.3. Заявители, являющиеся физическими лицами, предоставляют:

1) основной документ, удостоверяющий личность, либо его нотариально заверенную копию;

2) страховое свидетельство государственного пенсионного страхования либо ее нотариально заверенную копию;

3) свидетельство о постановке на учет физического лица в налоговом органе либо ее нотариально заверенную копию;

4) нотариально заверенную доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц (если заявитель действует от имени других лиц);

5) сведения, необходимые для направления в ЕСИА о лице, получающим сертификат, в объеме, необходимом для регистрации в ЕСИА.

6) иные документы, подтверждающие сведения, включаемые в сертификат и необходимые для использования электронной подписи в информационных системах.

6. Права и обязанности сторон

6.1. Удостоверяющий центр обязан:

6.1.1. Предоставить Пользователю УЦ сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме.

6.1.2. Использовать для создания ключа электронной подписи Удостоверяющего центра и формирования электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

6.1.3. Использовать ключ электронной подписи Удостоверяющего центра только для электронной подписи создаваемых им сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.

6.1.4. Принять меры по защите ключа электронной подписи Удостоверяющего центра от несанкционированного доступа.

6.1.5. Организовать свою работу с учетом часового пояса по местонахождению Удостоверяющего центра и обеспечить синхронизацию по времени средств Удостоверяющего центра.

6.1.6. Изготовить сертификат ключа проверки электронной подписи Пользователя УЦ по заявлению на изготовление сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Регламенте.

6.1.7. Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей проверки электронной подписи.

6.1.8. Обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах ключей проверки электронной подписи Пользователей УЦ.

6.1.9. Обеспечить конфиденциальность созданных Удостоверяющим центром ключей электронных подписей в пределах средств, находящихся в зоне ответственности Удостоверяющего центра, в том числе конфиденциальность ключей электронных подписей Пользователя УЦ до момента их передачи Пользователю УЦ.

6.1.10. Прекратить, приостановить и возобновить действие сертификата ключа проверки электронной подписи Пользователя УЦ по соответствующему заявлению на прекращение, приостановлению и возобновлению действия сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Регламенте.

6.1.11. Прекратить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра, если истек установленный срок, на который действие данного сертификата было приостановлено.

6.1.12. Прекратить действие сертификата ключа проверки электронной подписи Пользователя УЦ в случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи Пользователя УЦ.

6.1.13. Официально уведомить об аннулировании, прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи всех лиц, зарегистрированных в Удостоверяющем центре, посредством публикации списка отозванных сертификатов.

6.1.14. Публиковать список отозванных сертификатов на сайте Удостоверяющего центра по адресу http://uc-cit.cap.ru/cdp/ с периодичностью, обеспечивающей его актуальность, а также и обеспечить его круглосуточную доступность. Период публикации списка отозванных сертификатов может изменяться Удостоверяющим центром в одностороннем порядке. Точки распространения списка отозванных сертификатов указываются в сертификатах Пользователей УЦ.

6.1.15. Вести реестр сертификатов ключей проверки электронных подписей (далее также – реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования.

6.1.16. Заносить сведения о прекратившем действие сертификате ключа проверки электронной подписи в реестр сертификатов в течение 12 (двенадцати) часов с момента поступления заявления владельца сертификата ключа проверки электронной подписи о досрочном прекращении действия сертификата ключа проверки электронной подписи либо в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало

известно о наступлении обстоятельств, влекущих прекращение действие или аннулирование сертификата ключа проверки электронной подписи.

6.1.17. Заносить сведения об аннулированном сертификате в реестр сертификатов в течение одного рабочего дня со дня вступления в законную силу решения суда, явившегося основанием для аннулирования.

6.1.18. Направить в единую систему идентификации и аутентификации сведения о лице, получившем сертификат, и о полученном им сертификате.

6.1.19. Обеспечить любому лицу безвозмездный доступ к реестру сертификатов, созданных Удостоверяющим центром, в любое время в течение всего срока его деятельности.

6.2. Сторона, присоединившаяся к Регламенту, обязана:

6.2.1. С целью обеспечения гарантированного ознакомления Стороны, присоединившейся к Регламенту, с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра по адресу http://uc-cit.cap.ru за сведениями об изменениях и дополнениях в Регламент.

6.2.2. Пользователь Удостоверяющего центра обязан:

6.2.2.1. Обеспечить конфиденциальность ключей электронных подписей.

6.2.2.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

6.2.2.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

6.2.2.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи, если такие ограничения были установлены.

6.2.2.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

6.2.2.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия, которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

6.2.2.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия, которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

6.2.2.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.

6.2.2.9. Использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии Федеральным законом «Об электронной подписи».

6.3. Удостоверяющий центр имеет право:

6.3.1. Отказать в создании сертификата ключа проверки электронной подписи Пользователя УЦ в случае ненадлежащего оформления заявления на создание сертификата ключа проверки электронной подписи.

6.3.2. Отказать в создании сертификата ключа проверки электронной подписи Пользователя УЦ в случае не предоставления и (или) ненадлежащего предоставления документов, установленных п. 5.3 настоящего Регламента.

6.3.3. Отказать в прекращении, приостановлении и возобновлении действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления на прекращение, приостановление и возобновление действия сертификата ключа проверки электронной подписи.

6.3.4. Отказать в прекращении приостановлении и возобновлении действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия ключа электронной подписи, соответствующего сертификату.

6.3.5. В одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра с обязательным уведомлением владельца сертификата ключа проверки электронной подписи, действие которого приостановлено, и указанием обоснованных причин.

6.4. Пользователь Удостоверяющего центра имеет право:

6.4.1. Применять сертификат ключа проверки электронной подписи Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в сертификатах ключей проверки электронных подписей, созданных Удостоверяющим центром.

6.4.2. Применять список отозванных сертификатов ключей проверки электронных подписей, созданный Удостоверяющим центром для установления статуса сертификатов ключей проверки электронной подписи, созданных Удостоверяющим центром.

6.4.3. Для хранения ключа электронной подписи применять ключевой носитель, поддерживаемый средством электронной подписи, определённым сертификатом ключа проверки электронной подписи, соответствующим ключу электронной подписи.

6.4.4. Получить копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную Удостоверяющим центром.

6.4.5. Обратиться в Удостоверяющий центр с заявлениями на выполнение Удостоверяющим центром действий, установленных настоящим Регламентом.

6.4.6. Пользоваться сервисами Службы актуальных статусов сертификатов и Службы штампов времени Удостоверяющего центра.

7. Стоимость услуг Удостоверяющего центра. Сроки и порядок расчетов

7.1. В соответствии с государственным заданием БУ «Центр информационных технологий» Мининформполитики Чувашии, услуги Удостоверяющего центра органам исполнительной власти Чувашской Республики, органам местного самоуправления и

многофункциональным центрам предоставления государственных и муниципальных услуг Чувашской Республики предоставляются безвозмездно.

7.2. Стоимость услуг, оказываемых Удостоверяющим центром, определяется прейскурантом, опубликованном на сайте Удостоверяющего центра по адресу http://uc-cit.cap.ru.

7.3. Предоставление услуг осуществляется Удостоверяющим центром после оплаты соответствующего счета, выставленного Стороне, присоединившейся к Регламенту.

7.4. Создание сертификатов ключей проверки электронной подписи, вызванных внеплановой сменой ключей Пользователей УЦ, связанной с нарушением конфиденциальности ключей электронной подписи Удостоверяющего центра, осуществляется Удостоверяющим центром безвозмездно.

8. Ответственность сторон

8.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

8.2. Стороны не несут ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

8.3. Удостоверяющий центр не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях Стороны, присоединившейся к Регламенту, и в предоставленных документах.

8.4. Удостоверяющий центр несет ответственность за убытки при использовании созданного Удостоверяющим центром ключа электронной подписи и сертификата ключа проверки электронной подписи в том случае, если данные убытки возникли по

причине нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра.

8.5. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

9. Разрешение споров

9.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к Регламенту.

9.2. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться действующим законодательством Российской Федерации.

9.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

9.4. Сторона, получившая от другой Стороны претензию, обязана в течение 20 (двадцати) рабочих дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

9.5. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде Чувашской Республики.

10. Порядок предоставления и пользования услугами Удостоверяющего центра

10.1. Изготовление сертификата ключа проверки электронной подписи

10.1.1. Удостоверяющий центр осуществляет изготовление сертификатов ключей проверки электронной подписи лицам, которые присоединились к настоящему Регламенту и являются Стороной настоящего Регламента.

10.1.2. Изготовление сертификата ключа проверки электронной подписи осуществляется на основании заявления на изготовление сертификата ключа проверки электронной подписи. Форма заявления на изготовление сертификата ключа проверки электронной подписи приведена в Приложении № 2 настоящего Регламента.

10.1.3. Вместе с заявлением на изготовление сертификата в Удостоверяющий центр предоставляются документы, приведенные в п. 5.3 настоящего Регламента.

10.1.4. В случае изготовления сертификата ключа проверки электронной подписи юридическому лицу наряду с указанием в сертификате наименования юридического лица должно указываться физическое лицо, имеющее право действовать от имени юридического лица на основании доверенности или иного документа (приказа (распоряжения) о наделении полномочиями и т.д.). Указанный документ или доверенность должна предоставляться заявителем вместе с заявлением на изготовление сертификата ключа проверки электронной подписи. Доверенность должна оформляться по форме Приложения № 3 настоящего Регламента и быть действительной на момент создания сертификата ключа проверки электронной подписи.

Если ключи электронной подписи и сертификат ключа проверки электронной подписи юридического лица будут использоваться для автоматического создания электронных подписей и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, то физическое лицо может не указываться в сертификате ключа проверки электронной подписи.

10.1.5. Предоставление заявительных документов на изготовление сертификата ключа проверки электронной подписи, а также получение сформированных Удостоверяющим центром ключа электронной подписи и сертификата ключа проверки электронной подписи может быть осуществлено одним из следующих способов:

1) для юридического лица:

физическим лицом, которое указывается в сертификате наряду с наименованием юридического лица;

физическим лицом на основании доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи, оформленной по форме Приложения № 4 к настоящему Регламенту;

2) для физического лица или индивидуального предпринимателя:

непосредственно этим физическим лицом или индивидуальным предпринимателем;

физическим лицом на основании нотариально заверенной доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи, оформленной по форме Приложения № 4 к настоящему Регламенту.

10.1.6. Оператор Удостоверяющего центра на основании предоставленных заявительных документов выполняет действия по формированию ключа электронной подписи и изготовлению сертификата ключа проверки электронной подписи. Ключ электронной подписи и сертификат ключа проверки электронной подписи записываются на предоставляемый заявителем ключевой носитель.

10.1.7. Оператор Удостоверяющего центра распечатывает на бумажном носителе два экземпляра копии сертификата ключа проверки электронной подписи по форме Приложения № 10. Заявитель или его уполномоченный представитель проверяет соответствие сведений, содержащихся в копии сертификата ключа проверки электронной подписи. Копии сертификата ключа проверки электронной подписи заверяются собственноручными подписями владельца сертификата ключа проверки электронной подписи или его уполномоченного представителя и подписью уполномоченного лица Удостоверяющего центра. Один экземпляр заверенной копии сертификата ключа проверки электронной подписи и ключевой носитель, содержащий ключ электронной подписи и сертификат ключа проверки электронной подписи, передается заявителю или его уполномоченному представителю.

10.1.8. Дополнительно, по согласованию с заявителем, Оператором Удостоверяющего центра сообщается ключевая фраза, которая в дальнейшем может использоваться для аутентификации Пользователя УЦ при выполнении регламентных процедур, возникающих при нарушении конфиденциальности (компрометации) ключа электронной подписи Пользователя УЦ.

10.1.9. Создание и выдача сертификатов ключей проверки электронной подписи Удостоверяющим центром осуществляется в день прибытия заявителя или его уполномоченного представителя. День и время прибытия заявителя согласовывается с Оператором Удостоверяющего центра. Удостоверяющий центр вправе отказать в создании сертификатов по заявлениям, поступившим в Удостоверяющим центр без согласования дня прибытия заявителя.

10.2. Прекращение действия сертификата ключа проверки электронной подписи.

Удостоверяющий центр прекращает действие сертификата ключа проверки электронной подписи Пользователя УЦ в следующих случаях:

1) при прекращении действия настоящего Регламента в отношении Стороны, присоединившейся к Регламенту, по усмотрению Удостоверяющего центра;

2) по истечении срока, на который действие сертификата было приостановлено;

3) по заявлению владельца сертификата ключа проверки электронной подписи;

4) в связи с аннулированием сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу;

5) по истечении срока действия сертификата ключа проверки электронной подписи;

6) при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра, с использованием которого был создан сертификат ключа проверки электронной подписи;

7) в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;

8) в случае аннулирования сертификата Удостоверяющего центра, либо в случае аннулирования или истечения срока аккредитации Удостоверяющего центра.

В случаях, указанных в подпунктах 1 – 4 пункта 10.2 настоящего Регламента, Удостоверяющий центр официально уведомляет владельца сертификата и всех Пользователей УЦ о прекращении действия сертификата ключа проверки электронной подписи не позднее одного рабочего дня с момента наступления указанного события.

Официальным уведомлением о факте прекращения действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого прекращено, и изданного не ранее времени наступления произошедшего случая. Временем прекращения действия сертификата ключа проверки электронной подписи признается время внесения записи о прекращения действия сертификата в реестр сертификатов Удостоверяющего центра, соответствующее моменту издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRLDistributionPoint сертификата ключа проверки электронной подписи.

В случае прекращения действия сертификата ключа проверки электронной подписи по истечению срока его действия временем прекращения действия сертификата ключа проверки электронной подписи признается время, хранящееся в поле notAfter поля Validity сертификата ключа проверки электронной подписи. В этом случае информация о сертификате, действие которого прекращено, в список отозванных сертификатов не заносится.

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра временем прекращения действия сертификата ключа проверки электронной подписи Пользователя УЦ признается время нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, фиксирующееся Удостоверяющим центром. При этом информация о сертификате ключа проверки электронной подписи Пользователя УЦ в список отозванных сертификатов не заносится.

10.2.1. Прекращение действия сертификата ключа проверки электронной подписи по заявлению его владельца

Для прекращения действия сертификата ключа проверки электронной подписи владелец сертификата лично подает в Удостоверяющий центр заверенное собственноручной подписью соответствующее заявление по форме Приложения № 5 настоящего Регламента, либо направляет такое заявление в Удостоверяющий центр в электронном виде, подписанное действующей электронной подписью владельца отзываемого сертификата.

В случае подачи заявления в электронном виде владелец сертификата обязан убедится в получении, связавшись в рабочее время с Оператором Удостоверяющего центра по телефону.

После получения Удостоверяющим центром заявления на прекращение действия сертификата ключа проверки электронной подписи уполномоченный сотрудник

Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на прекращение действия сертификата должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в прекращении действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения уполномоченный сотрудник Удостоверяющего центра осуществляет прекращение действия сертификата ключа проверки электронной подписи.

10.3. Приостановление действия сертификата ключа проверки электронной подписи

Удостоверяющий центр приостанавливает действие сертификата ключа проверки электронной подписи в следующих случаях:

по заявлению владельца сертификата ключа проверки электронной подписи;

в иных случаях, предусмотренных положениями настоящего Регламента, по решению Удостоверяющего центра.

Действие сертификата ключа проверки электронной подписи приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата ключа проверки электронной подписи составляет 15 (пятнадцать) дней.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи действие этого сертификата не будет возобновлено, то данный сертификат прекращает своё действие.

Официальным уведомлением о факте приостановления действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, и изданного не ранее времени наступления произошедшего случая. Временем приостановления действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL DistributionPoint сертификата ключа проверки электронной подписи.

10.3.1. Приостановление действия сертификата ключа проверки электронной подписи по заявлению его владельца

Подача заявления в Удостоверяющий центр на приостановление действия сертификата ключа проверки электронной подписи может быть осуществлена посредством почтовой или курьерской связи по форме Приложения № 6 настоящего Регламента либо направлением такого заявления в Удостоверяющий центр в электронном виде, подписанным действующей электронной подписью владельца сертификата.

После получения Удостоверяющим центром заявления на приостановление действия сертификата ключа проверки электронной подписи уполномоченное лицо Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на приостановление действия сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в приостановлении действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения уполномоченный сотрудник Удостоверяющего центра осуществляет приостановление действия сертификата ключа проверки электронной подписи.

10.3.2. Приостановление действия сертификата ключа проверки электронной подписи по заявке его владельца в устной форме.

Приостановление действия сертификата ключа проверки электронной подписи по заявке в устной форме осуществляется исключительно при нарушении конфиденциальности ключа электронной подписи или подозрении в нарушении конфиденциальности ключа электронной подписи Пользователя УЦ.

Заявка подается в Удостоверяющий центр по телефону.

Пользователь УЦ должен сообщить уполномоченному лицу Удостоверяющего центра следующую информацию:

идентификационные данные, содержащиеся в сертификате ключа проверки электронной подписи, действие которого необходимо приостановить;

серийный номер сертификата ключа проверки электронной подписи, действие которого требуется приостановить;

ключевую фразу Пользователя УЦ (ключевая фраза определяется в процессе изготовления сертификата ключа проверки электронной подписи).

Заявка на приостановление действия сертификата принимается Удостоверяющим центром только в случае положительной аутентификации Пользователя УЦ (совпадения ключевой фразы, сообщенной Пользователем УЦ по телефону, и ключевой фразы, хранящейся в УЦ).

После принятия заявки уполномоченное лицо Удостоверяющего центра принимает решение о приостановлении действия сертификата ключа проверки электронной подписи, которое должно быть осуществлено в течение рабочего дня поступления данной заявки.

В случае отказа в приостановлении действия сертификата ключа проверки электронной подписи Пользователь УЦ уведомляется об этом с указанием причины отклонения заявки.

При принятии положительного решения уполномоченное лицо Удостоверяющего центра приостанавливает действие сертификата ключа проверки электронной подписи до окончания срока действия ключа электронной подписи, соответствующего данному сертификату.

Не позднее 5 (пяти) рабочих дней с момента приостановления действия сертификата ключа проверки электронной подписи владелец сертификата должен предоставить в Удостоверяющий центр заявление на прекращение действия сертификата (в том случае, если факт нарушения конфиденциальности ключа электронной подтвердился), либо заявление на возобновление действия сертификата (в том случае, если нарушения конфиденциальности ключа электронной подписи не было).

10.3.3. Приостановление действия сертификата ключа проверки электронной подписи по решению Удостоверяющего центра.

Удостоверяющий центр вправе приостановить действие сертификата ключа проверки электронной подписи в случаях нарушения конфиденциальности или подозрения в нарушении конфиденциальности соответствующего ключа электронной подписи в том случае, если владельцу сертификата ключа проверки электронной подписи не было известно о возможном факте нарушения конфиденциальности ключей,

а также в случаях неисполнения владельцем сертификата ключа проверки электронной подписи обязательств по настоящему Регламенту.

После приостановления действия сертификата ключа проверки электронной подписи уполномоченное лицо Удостоверяющего центра сообщает владельцу сертификата ключа проверки электронной подписи о наступлении события, повлекшего приостановление действия сертификата, и уведомляет его о том, что действие сертификата приостановлено.

10.4. Возобновление действия сертификата ключа проверки электронной подписи

Удостоверяющий центр возобновляет действие сертификата ключа проверки электронной подписи только по заявлению его владельца и только в том случае, если действие сертификата ключа проверки электронной подписи было приостановлено.

Подача заявления в Удостоверяющий центр на возобновление действия сертификата ключа проверки электронной подписи может быть осуществлена посредством почтовой или курьерской связи по форме Приложения № 7 настоящего Регламента.

После получения Удостоверяющим центром заявления на возобновление действия сертификата ключа проверки электронной подписи уполномоченное лицо Удостоверяющего центра осуществляет его рассмотрение и обработку. Обработка заявления на возобновление действия сертификата должна быть осуществлена не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в возобновлении действия сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет об этом его владельца с указанием причин отказа.

При принятии положительного решения уполномоченное лицо Удостоверяющего центра осуществляет возобновление действия сертификата ключа проверки электронной подписи.

Официальным уведомлением о факте возобновления действия сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, не содержащего сведения о сертификате, действие которого было возобновлено, и изданного не ранее времени предоставления заявления на возобновление действия сертификата. Временем возобновления действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром сертификаты ключей проверки электронной подписи в расширение CRL DistributionPoint.

10.5. Получение информации о статусе сертификата ключа проверки электронной подписи

Получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром, осуществляется на основании заявления Стороны, присоединившейся к Регламенту. Данное заявление оформляется по форме Приложения № 8 настоящего Регламента и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

дата и время подачи заявления;

время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключа проверки электронной подписи;

идентификационные данные владельца, статус сертификата ключа проверки электронной подписи которого требуется установить;

серийный номер сертификата ключа проверки электронной подписи, статус которого требуется установить.

По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата ключа проверки электронной подписи, которая предоставляется заявителю.

Предоставление заявителю справки о статусе сертификата ключа проверки электронной подписи должно быть осуществлено не позднее 10 (десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

10.6. Проверка подлинности электронной подписи в электронном документе

По желанию Стороны, присоединившейся к Регламенту, Удостоверяющий центр осуществляет проведение экспертных работ по проверке подлинности электронной подписи в электронном документе, сформированной с использованием ключа электронной подписи, соответствующего сертификату ключа проверки электронной подписи, изготовленного Удостоверяющим центром.

В том случае, если формат представления электронной подписи (формат представления электронного документа с электронной подписью) соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то Удостоверяющий центр обеспечивает проверку подлинности электронной подписи в электронном документе. Решение о соответствии формата представления электронной подписи (формата представления электронного документа с электронной подписью) стандарту CMS принимает Удостоверяющий центр.

Для проверки подлинности электронной подписи в электронных документах Сторона, присоединившаяся к Регламенту, подает заявление в Удостоверяющий центр по форме, приведенной в Приложении № 9 настоящего Регламента.

Заявление должно содержать следующую информацию:

дата и время подачи заявления;

идентификационные данные владельца сертификата, электронную подпись которого необходимо проверить в электронном документе;

дата и время формирования электронной подписи электронного документа;

дата и время, на момент наступления которых требуется проверить подлинность электронной подписи (в том случае, если информация о дате и времени подписания электронного документа отсутствует).

Обязательным приложением к заявлению на проверку подлинности электронной подписи в электронном документе является носитель, содержащий:

сертификат ключа проверки электронной подписи, с использованием которого необходимо проверить подлинность электронной подписи в электронном документе – в виде файла стандарта CMS;

электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

Проведение работ по проверке подлинности электронной подписи в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

Результатом проведения работ по проверке подлинности электронной подписи в электронном документе является заключение Удостоверяющего центра.

Заключение содержит:

состав комиссии, осуществлявшей проверку;

основание для проведения проверки;

данные, предоставленные комиссии для проведения проверки.

результат проверки электронной подписи электронного документа.

Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по проверке подлинности электронной подписи в одном электронном документе и предоставлению заявителю заключения по выполненной проверке составляет 10 (десять) рабочих дней с момента поступления заявления в Удостоверяющий центр.

В том случае, если формат представления электронной подписи (формат представления электронного документа с электронной подписью) не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то проведение экспертных работ по проверке подлинности электронной подписи осуществляется в рамках заключения отдельного договора между Удостоверяющим центром и Стороной, присоединившейся к Регламенту. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором.

10.7. Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени

Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе сертификатов ключей проверки электронной подписи посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам Пользователей Удостоверяющего центра формирует и предоставляет этим пользователям OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата ключа проверки электронной подписи.

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра http://ra-cit.cap.ru/ocsp/ocsp.srf.

Указанный адрес заносится в расширение Authority Information Access (AIA) создаваемых Удостоверяющим центров сертификатов ключей проверки электронной подписи.

Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени. Адрес обращения к Службе штампов времени Удостоверяющего центра http://ra-cit.cap.ru/tsp/tsp.srf.

11. Форма сертификата ключа проверки электронной подписи, списка отозванных сертификатов и сроки действия ключевых документов

11.1. Форма сертификата ключа проверки электронной подписи, изготавливаемого Удостоверяющим центром

Форма сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, соответствует требованиям приказа Федеральной службы безопасности Российской федерации от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

11.2. Форма сертификата ключа проверки электронной подписи Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 / ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CN = Головной удостоверяющий центр ИНН = 007710474375 ОГРН = 1047702026701 O = Минкомсвязь России STREET = 125375 г. Москва, ул. Тверская, д. 7 L = Москва S = 77 г. Москва C = RU E = dit@minsvyaz.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = БУ "Центр информационных технологий" Мининформполитики Чувашии O = БУ "Центр информационных технологий" Мининформполитики Чувашии E = uc-info@cap.ru STREET = ул. Калинина, д.112 L = Чебоксары S = 21 Чувашская Республика- Чувашия C = RU ИНН = 002130176633 ОГРН = 1162130063501
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТР 34.11/34.10-2001 / ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 / ГОСТ Р 34.11/34.10-2012
Дополнения сертификата		
CRL Distribution Point	Точки распространения списков отзыва (CRL)	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://rostelecom.ru/cdp/guc.crl [2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://reestr-pki.ru/cdp/guc.crl
Key Usage	Использование ключа	Цифровая подпись, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего Центра, соответствующего данному сертификату
Basic Constraints	Основные ограничения	SybjectType (Тип владельца сертификата) =ЦС PathLengthConstraint (Ограничение на длину пути – ограничивает количество уровней иерархии при создании подчиненных удостоверяющих центров)= 0

11.3. Форма сертификата пользователя Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 / ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CN = БУ "Центр информационных технологий" Мининформполитики Чувашии O = БУ "Центр информационных технологий" Мининформполитики Чувашии E = uc-info@cap.ru STREET = ул. Калинина, д.112 L = Чебоксары S = 21 Чувашская Республика- Чувашия C = RU ИНН = 002130176633 ОГРН = 1162130063501
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = ФИО владельца сертификата OrganizationUnit = Подразделение организации Title = Должность Organization = Наименование организации SurName = Фамилия GivenName = Имя и Отчество Title = Должность StreetAddress = Название улицы, номер дома Locality = Наименование населенного пункта State = Субъект Федерации (с двухзначным кодом) Country = Страна = RU SNILS = СНИЛС INN = ИНН юридического лица или физического лица OGRN = ОГРН организации Компонента имени CN обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТР 34.11/34.10-2001 / ГОСТ Р 34.11/34.10-2012
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 / ГОСТ Р 34.11/34.10-2012
Расширения сертификата		
Private Key Validity Period	Срок действия закрытого ключа, соответствующего сертификату	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Key Usage	Использование ключа	Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей
Extended Key Usage	Улучшеный ключ	Базовый набор областей использования ключей и сертификатов из перечня областей использования, зарегистрированных в удостоверяющем центре: Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

Название	Описание	Содержание
		Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Дополнительный набор областей использования, включаемых по обращению заявителя, указан в п. 11.4 настоящего Регламента
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор закрытого ключа Уполномоченного лица удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов
В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280 и RFC 5280		

11.4. Список областей использования ключей (объектных идентификаторов), включаемых в сертификаты ключей проверки электронной подписи, выдаваемых Удостоверяющим центром

Объектный идентификатор	Наименование
Стандартные области использования ключа, включаемые в сертификат	
1.3.6.1.5.5.7.3.2	Проверка подлинности клиента
1.3.6.1.5.5.7.3.4	Защищенная электронная почта
1.2.643.2.2.34.6	Пользователь Центра Регистрации, HTTP, TLS клиент
1.2.643.2.2.34.26	Пользователь службы актуальных статусов
1.2.643.2.2.34.25	Пользователь службы штампов времени
Дополнительные области использования ключа, включаемые в сертификат по желанию заявителя	
1.2.643.100.2.1	Доступ к СМЭВ (ЭП-СП)
1.2.643.100.2.2	Доступ к СМЭВ (ЭП-ОВ)
1.2.643.5.1.24.2.6	Руководитель органа государственной власти субъекта Российской Федерации или иное уполномоченное лицо данного органа *(для ИС Росреестра)*
1.2.643.5.1.24.2.19	Руководитель органа местного самоуправления или иное уполномоченное лицо данного органа *(для ИС Росреестра)*
1.2.643.5.1.24.2.43	Руководитель территориального органа федерального органа исполнительной власти или иное уполномоченное лицо данного органа *(для ИС Росреестра)*
1.2.643.5.1.24.2.32	Руководитель органа прокуратуры или иное уполномоченное должностное лицо данного органа *(для ИС Росреестра)*
1.2.643.3.7.1	Подписание документов в рамках Системы «Контур-Экстерн». Подписание документов уполномоченным представителем
1.2.643.3.7.1.1.1	Абонент Системы Контур-Экстерн
1.2.643.3.7.3.15	Информационная система Диадок
1.2.643.7.2.21.1.2	Размещение сведений в сводном реестре *(для ИС ОГИЦ)*

Список областей использования ключей может изменяться и дополняться в ходе деятельности по предоставлению услуг Удостоверяющего центра.

11.5. Форма списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = БУ "Центр информационных технологий" Мининформполитики Чувашии O = БУ "Центр информационных технологий" Мининформполитики Чувашии E = uc-info@cap.ru STREET = ул. Калинина, д.112 L = Чебоксары S = 21 Чувашская Республика- Чувашия C = RU ИНН = 002130176633 ОГРН = 1162130063501
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки события, повлекшего прекращение действия сертификата (Time) 3. Код причины прекращения действия сертификата (ResonCode) "0" Не указана "1" Компрометация ключа (нарушение конфиденциальности ключа) "2" Компрометация ЦС (нарушение конфиденциальности ключа Удостоверяющего центра) "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Прекращение действия
signatureAlgorithm	Алгоритм электронной подписи	ГОСТ Р 34.11/34.10-2001 / ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 / ГОСТ Р 34.11/34.10-2012
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Удостоверяющего Центра

11.6. Сроки действия ключевых документов

11.6.1. Сроки действия ключевых документов Удостоверяющего центра

Срок действия ключа электронной подписи Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра, и для средства электронной

подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени генерации ключа электронной подписи Удостоверяющего центра.

Срок действия сертификата ключа проверки электронной подписи Удостоверяющего центра не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

Срок действия ключа электронной подписи Службы актуальных статусов сертификатов составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи Службы актуальных статусов сертификатов исчисляется с даты и времени создания сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов.

Срок действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

Срок действия ключа электронной подписи Службы штампов времени составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи Службы штампов времени исчисляется с даты и времени создания сертификата ключа проверки электронной подписи Службы штампов времени.

Срок действия сертификата ключа проверки электронной подписи Службы штампов времени не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы штампов времени и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

11.6.2. Сроки действия ключевых документов Пользователя Удостоверяющего центра

Срок действия ключа электронной подписи пользователя Удостоверяющего центра составляет 1 (один) год.

Начало периода действия ключа электронной подписи пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

Срок действия сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно.

12. Дополнительные положения

12.1. Плановая смена ключей Удостоверяющего центра

Плановая смена ключа электронной подписи и соответствующего ему сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется в период действия ключа электронной подписи Удостоверяющего центра. Процедура плановой смены ключей Удостоверяющего центра осуществляется в следующем порядке:

Удостоверяющий центр создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;

Удостоверяющий центр создает новый сертификат ключа проверки электронной подписи.

Уведомление пользователей о проведении смены ключей Удостоверяющего центра осуществляется посредством электронной почты.

Предыдущий ключ электронной подписи Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, создаваемых Удостоверяющим центром в период действия предыдущего ключа электронной подписи Удостоверяющего центра.

12.2. Нарушение конфиденциальности ключевых документов Удостоверяющего центра, внеплановая смена ключей Удостоверяющего центра

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра прекращает действие, Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра на сайте Удостоверяющего центра. Все сертификаты, подписанные с использованием ключа Удостоверяющего центра, конфиденциальность которого нарушена, считаются прекратившими действие.

После прекращения действия сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется процедура внеплановой смены ключей Удостоверяющего центра. Процедура внеплановой смены ключей Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра.

Все действовавшие на момент нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификаты ключей проверки электронной подписи, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

12.3. Нарушение конфиденциальности ключевых документов Пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе нарушения конфиденциальности своего ключа электронной подписи.

В случае нарушения конфиденциальности или угрозы нарушения конфиденциальности ключа электронной подписи Пользователь УЦ обязан прекратить использование соответствующего ключа электронной подписи и немедленно уведомить об этом Удостоверяющий центр, связавшись с уполномоченным лицом Удостоверяющего центра по телефону и заявить о необходимости приостановления действия сертификата ключа проверки электронной подписи, соответствующего ключу, конфиденциальность которого нарушена.

В случае нарушения конфиденциальности ключа электронной подписи Пользователь УЦ направляет в Удостоверяющий центр заявление на прекращение действия сертификата в соответствии с п. 10.2.1 настоящего Регламента.

Если в течение срока приостановления действия сертификата ключа проверки электронной подписи Пользователь не направит в Удостоверяющий центр заявление на возобновление действия указанного сертификата, то Удостоверяющий центр прекращает действие данного сертификата.

12.4. Конфиденциальность информации

12.4.1. Типы конфиденциальной информации

12.4.1.1. Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключей электронных подписей Пользователей УЦ.

12.4.1.2. К конфиденциальной информации относится информация, содержащая персональные данные Пользователя УЦ, за исключением сведений, включаемых в сертификат ключа проверки электронной подписи Пользователя УЦ и сведений, направляемых в единую систему идентификации и аутентификации.

12.4.2. Типы информации, не являющейся конфиденциальной

12.4.2.1. Информация, подлежащая в соответствии с законодательством Российской Федерации размещению в информационно-телекоммуникационной сети «Интернет», доступ к которой не ограничен, считается общедоступной (открытой) информацией.

12.4.2.2. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.

12.4.2.3. Информация, включаемая в сертификаты ключей проверки электронной подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

12.4.2.4. Персональные данные, включаемые в сертификаты ключей проверки электронной подписи, создаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

12.4.2.5. Информация, содержащаяся в настоящем Регламенте, не является конфиденциальной.

12.4.3. Удостоверяющий центр не имеет право раскрывать конфиденциальную информацию третьим лицам, если иное не установлено федеральными законом или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между Удостоверяющим центром и Стороны, присоединившейся к настоящему Регламенту.

12.5. Хранение сертификата ключа проверки электронной подписи в Удостоверяющем центре осуществляется в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации.

12.6. Прекращение оказания услуг Удостоверяющим центром

12.6.1. В случае расторжения договора присоединения к настоящему Регламенту по инициативе Стороны, присоединившейся к Регламенту, действие всех сертификатов ключей проверки электронной подписи, владельцем которых является указанная Сторона, прекращается Удостоверяющим центром.

12.7. Непреодолимая сила (форс-мажор)

12.7.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение

явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

12.7.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства, включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

12.7.3. В случае возникновения форс-мажорных обстоятельств, срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

12.7.4. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

12.7.5. Не извещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

12.7.6. В случае, если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

13. Список приложений

13.1. Приложение № 1. Форма заявления о присоединении к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии.

13.2. Приложение № 2. Форма заявления на изготовление сертификата ключа проверки электронной подписи.

13.3. Приложение № 3. Форма доверенности на право действия от имени юридического лица.

13.4. Приложение № 4. Форма доверенности на получение ключей электронной подписи и сертификата ключа проверки электронной подписи за Пользователя Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии.

13.5. Приложение № 5. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи.

13.6. Приложение № 6. Форма заявления на приостановление действия сертификата ключа проверки электронной подписи.

13.7. Приложение № 7. Форма заявления на возобновление действия сертификата ключа проверки электронной подписи.

13.8. Приложение № 8. Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром БУ «Центр информационных технологий» Мининформполитики Чувашии.

13.9. Приложение № 9. Форма заявления на проверку подлинности электронной

подписи в электронном документе.

13.10. Приложение № 10. Форма копии сертификата ключа проверки электронной подписи на бумажном носителе.

13.11. Приложение № 11. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи.

Приложение № 1
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления о присоединении к Регламенту **для юридических лиц)***

БУ «Центр информационных технологий»
Мининформполитики Чувашии

_____ № _____

_____
(полное наименование организации, включая организационно-правовую форму, ОГРН, ИНН)

в лице _____,
(должность, фамилия, имя, отчество)

действующего на основании _____,
в соответствии со статьей 428 Гражданского кодекса Российской Федерации присоединяется к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии (далее – Регламент), опубликованному на сайте Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии в информационно-телекоммуникационной сети «Интернет» по адресу http://uc-cit.cap.ru.

Должностные лица _____,
(сокращенное наименование организации)

регистрирующиеся в Удостоверяющем центре БУ «Центр информационных технологий» Мининформполитики Чувашии, с Регламентом и приложениями к нему ознакомлены и обязуются соблюдать все его положения.

_____ _____ / _____ /
(должность) (подпись) (расшифровка подписи)

М.П.

* Заявление о присоединении к Регламенту подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное заявление зарегистрировано в реестре Удостоверяющего центра в качестве договора присоединении к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии.

Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии _____ / _____ /
(подпись) (расшифровка подписи)

М.П.

Приложение № 1
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления о присоединении к Регламенту)
Для физических лиц и индивидуальных предпринимателей*

БУ «Центр информационных технологий» Мининформполитики Чувашии

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

_____
(СНИЛС, ИНН, ОГРНИП)

в соответствии со статьёй 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии (далее – Регламент), опубликованному на сайте Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии в информационно-телекоммуникационной сети «Интернет» по адресу http://uc-cit.cap.ru, с Регламентом и приложениями к нему ознакомлен и обязуюсь соблюдать все его положения.

_____ / _____
Подпись Ф.И.О

«____» _____ 20___ г.

(заполняется Оператором Удостоверяющего центра)

Данное заявление зарегистрировано в реестре Удостоверяющего центра в качестве договора присоединении к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии.

Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии _____ / _____ /
(подпись) (расшифровка подписи)

М.П.

* Заявление о присоединении к Регламенту подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

Приложение № 2
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на изготовление сертификата ключа проверки электронной подписи **для юридических лиц**)

БУ «Центр информационных технологий»
Мининформполитики Чувашии

_____ № _____

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность, фамилия, имя, отчество)

действующего на основании _____,
просит изготовить ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, содержащий следующую информацию:

Наименование организации	
Наименование населенного пункта	
Название улицы, номер дома	
Область	21 Чувашская Республика – Чувашия
Страна	RU
ИНН организации *(12 цифр)*	00
ОГРН организации	
Фамилия	
Имя Отчество	
Должность	
Подразделение организации	
СНИЛС	
Адрес электронной почты	
Дополнительные области использования ключа (расширения сертификата)	*При необходимости указать области использования ключа*[*]*, либо указать шаблон (профиль) сертификата:* □ *Сертификат для СМЭВ (ЭП-ОВ, ЭП-СП);* □ *Сертификат для работы в ИС Росреестра;* □ *Сертификат для работы в ФИС ФРДО, иных ИС Рособрнадзора;* □ *Сертификат информационной системы*

[*]Дополнительные области использования ключа приведены в п. 14.4 Регламента УЦ БУ «ЦИТ» Мининформполитики Чувашии

Настоящим _____
(Фамилия, Имя, Отчество лица, на имя которого изготавливается сертификат)
_____
(серия и номер паспорта, кем и когда выдан)
соглашается с обработкой своих персональных данных и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

_____ / _____ /
(подпись и ФИО должностного лица, на имя которого изготавливается сертификат).

_____ _____ / _____ /
(должность) (подпись и Ф.И.О.)

Приложение № 2
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на изготовление сертификата ключа проверки электронной подписи **для физических лиц и индивидуальных предпринимателей)**

БУ «Центр информационных технологий» Мининформполитики Чувашии

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

прошу изготовить ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, содержащий следующую информацию:

Фамилия	
Имя Отчество	
Наименование населенного пункта	
Адрес регистрации	
Область	21 Чувашская Республика – Чувашия
Страна	RU
СНИЛС	
ИНН	
ОГРНИП	
Адрес электронной почты	
Дополнительные области использования ключа (расширения сертификата)	*При необходимости, помимо стандартных, указываются иные дополнительные области использования ключа*[*]

Настоящим _____
(Фамилия, Имя, Отчество лица, на имя которого изготавливается сертификат)

_____
(серия и номер паспорта, кем и когда выдан)

соглашается с обработкой своих персональных данных и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

_____ / _____ /
(подпись и ФИО лица, на имя которого изготавливается сертификат).

«____» _____20___ г.

[*]Дополнительные области использования ключа приведены в п. 14.4 Регламента УЦ БУ «ЦИТ» Мининформполитики Чувашии

Приложение № 3
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма доверенности на право действия от имени **юридического лица**)

Доверенность

г. _____ «_____» _____20___ г.

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,
уполномочивает _____
(фамилия, имя, отчество доверенного лица)

_____
(серия и номер паспорта, кем и когда выдан)

действовать от имени _____
(сокращенно наименование организации)

при использовании электронной подписи электронных документов, выступать в роли Пользователя Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии и осуществлять действия в рамках Регламента Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии, установленные для Пользователя Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии.

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись доверенного лица _____ / _____ подтверждаю.
(Фамилия И.О.) (подпись)

_____ _____ / _____ /
(должность) (подпись) (расшифровка подписи)

М.П.

Приложение № 4
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма доверенности на получение сертификата ключа проверки электронной подписи)
Для юридических лиц

Доверенность

г. _____ «____» _____20___ г.

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,
уполномочивает _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

предоставить в БУ «Центр информационных технологий» Мининформполитики Чувашии необходимые документы для изготовления сертификата ключа проверки электронной подписи, получить ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, созданные для Пользователя Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии.

_____
(фамилия, имя, отчество Пользователя Удостоверяющего центра)

Представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись уполномоченного представителя _____ / _____ подтверждаю.
(Фамилия И.О.) (подпись)

_____ _____ / _____ /
(должность) (подпись) (расшифровка подписи)

М.П.

Приложение № 4
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма доверенности на получение сертификата ключа проверки электронной подписи)
Для физических лиц и индивидуальных предпринимателей

Доверенность*

г. _____ «_____» _____20___ г.

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан, адрес регистрации)

уполномочиваю _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан, адрес регистрации)

предоставить в БУ «Центр информационных технологий» Мининформполитики Чувашии необходимые документы для изготовления сертификата ключа проверки электронной подписи, для изготовления сертификата ключа проверки электронной подписи, получить ключ электронной подписи, ключ проверки электронной подписи и сертификат ключа проверки электронной подписи, созданные для Пользователя Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии.

Представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «_ _» _____ 20__ г. без права передоверия.

_____ _____ / _____ /
(Фамилия, имя, отчество заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

* Настоящая доверенность должна быть нотариально удостоверена

Приложение № 5
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на прекращение действия сертификата ключа проверки электронной подписи)
Для юридических лиц

БУ «Центр информационных технологий»
Мининформполитики Чувашии

_____ № _____

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,
в связи с _____,
(причина прекращения действия сертификата)

просит прекратить действие сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Наименование организации	
ИНН организации	
ОГРН организации	
Фамилия	
Имя Отчество	
СНИЛС	

_____ _____ / _____ /
(должность) (подпись и Ф.И.О.)

Приложение № 5
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на прекращение действия сертификата ключа проверки электронной подписи)
Для физических лиц и индивидуальных предпринимателей

БУ «Центр информационных технологий» Мининформполитики Чувашии

Я, _____
(фамилия, имя, отчество)

в связи с _____,
(причина прекращения действия сертификата)

прошу прекратить действие моего сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
ИНН	
СНИЛС	

_____ _____ / _____ /
(Ф.И.О заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

Приложение № 6
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на приостановление действия сертификата ключа проверки электронной подписи)
Для юридических лиц

БУ «Центр информационных технологий»
Мининформполитики Чувашии

_____ № _____

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,
в связи с _____,
(причина приостановления действия сертификата)

просит приостановить действие сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Наименование организации	
ИНН организации	
ОГРН организации	
Фамилия	
Имя Отчество	
СНИЛС	

Срок приостановления действия сертификата _____ дней.
(количество прописью)

_____ _____ / _____ /
(должность) (подпись и Ф.И.О.)

Приложение № 6
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на приостановление действия сертификата ключа проверки электронной подписи)
Для физических лиц и индивидуальных предпринимателей

БУ «Центр информационных технологий» Мининформполитики Чувашии

Я, _____
(фамилия, имя, отчество)

в связи с _____,
(причина приостановления действия сертификата)

прошу приостановить действие моего сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
ИНН	
СНИЛС	

_____ _____ / _____ /
(Ф.И.О заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

Приложение № 7
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на возобновление действия сертификата ключа проверки электронной подписи)
Для юридических лиц

БУ «Центр информационных технологий»
Мининформполитики Чувашии

_____ № _____

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,
просит возобновить действие сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Наименование организации	
ИНН организации	
ОГРН организации	
Фамилия	
Имя Отчество	
СНИЛС	

_____ _____ / _____ /
(должность) (подпись и Ф.И.О.)

Приложение № 7
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на возобновление действия сертификата ключа проверки электронной подписи)
Для физических лиц и индивидуальных предпринимателей

БУ «Центр информационных технологий» Мининформполитики Чувашии

Я, _____
(фамилия, имя, отчество)

прошу возобновить действие моего сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
ИНН	
СНИЛС	

_____ _____ / _____ /
(Ф.И.О заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

Приложение № 8
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи)
Для юридических лиц

БУ «Центр информационных технологий»
Мининформполитики Чувашии

_____ № _____

_____
(полное наименование организации, включая организационно-правовую форму)

в лице ___ _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,
просит предоставить информацию о статусе сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Наименование организации	
ОГРН организации	
Фамилия	
Имя Отчество	
СНИЛС	

Период времени* на момент наступления которого требуется установить статус сертификата ключа проверки электронной подписи: с «_____» по «_____».

_____ _____ / _____ /
(должность) (подпись и Ф.И.О.)

*Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение № 8
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи)
Для физических лиц и индивидуальных предпринимателей

БУ «Центр информационных технологий» Мининформполитики Чувашии

Я, _____
(фамилия, имя, отчество)

прошу предоставить информацию о статусе сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
СНИЛС	

Период времени* на момент наступления которого требуется установить статус сертификата ключа проверки электронной подписи: с «_____» по «_____».

_____ _____ / _____ /
(Ф.И.О заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

*Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение № 9
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на проверку подлинности электронной подписи в электронном документе)
Для юридических лиц

БУ «Центр информационных технологий»
Мининформполитики Чувашии

_____ № _____

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,
просит проверить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–XXX;

2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № Н–XXX.

3. Время* подписания электронной подписью электронного документа:
«_____:_____» «_____/_____/_____»;
Час минута день месяц год

Время, на момент наступления которого необходимо проверить подлинность электронной подписи (если момент подписания электронного документа не определен):
«_____:_____» «_____/_____/_____»
Час минута день месяц год

_____ _____ / _____ /
(должность) (подпись и Ф.И.О.)

* Время и дата указываются с учетом часового пояса (по Московскому времени).

Приложение № 9
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма заявления на проверку подлинности электронной подписи в электронном документе)
Для физических лиц и индивидуальных предпринимателей

БУ «Центр информационных технологий» Мининформполитики Чувашии

Я, _____
(фамилия, имя, отчество)

прошу проверить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–ХХХ;

2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № Н–ХХХ.

3. Время* подписания электронной подписью электронного документа:

«_____:_____» «_____/_____/_____»;
Час минута день месяц год

Время, на момент наступления которого необходимо проверить подлинность электронной подписи (если момент подписания электронного документа не определен):

«_____:_____» «_____/_____/_____»
Час минута день месяц год

_____ _____ / _____ /
(Ф.И.О заявителя) (подпись) (расшифровка подписи)

«____» _____ 20___

* Время и дата указываются с учетом часового пояса (по Московскому времени).

Приложение № 10
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма сертификата ключа проверки электронной подписи на бумажном носителе)
Для юридических лиц

Удостоверяющий центр БУ "Центр информационных технологий" Мининформполитики Чувашии
Копия сертификата ключа проверки электронной подписи
Сведения о сертификате:

Версия: 3
Серийный номер: 67F0508A762CBC80E7117EFBD6401B57
Издатель сертификата: CN=БУ "Центр информационных технологий" Мининформполитики Чувашии, O=БУ "Центр информационных технологий" Мининформполитики Чувашии, E=uc-info@cap.ru, STREET=ул. Калинина, д.112, L=Чебоксары, S=21 Чувашская Республика- Чувашия, C=RU, ИНН=002130176633, ОГРН=1162130063501
Владелец сертификата: CN=Орган исполнительной власти, OU=Тестовый отдел, O= Орган исполнительной власти, L=Чебоксары, S=21 Чувашская Республика - Чувашия, C=RU, SN=Иванов, G=Иван Иванович, T=Должностное лицо, STREET=Тестовая ул, 1, ОГРН=0000000000000, ИНН=000000000000, СНИЛС=00000000000
Срок действия:
Действителен с: 01.03.2018 19:19:12
Действителен по: 01.06.2019 19:29:12
Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2001 (1.2.643.2.2.19)
Параметры: 30 12 06 07 2A 85 03 02 02 24 00 06 07 2A 85 03 02 02 1E 01
Значение: 0440 AEAF 9A5D 54F5 0FF8 95AF 5E7E F83D 06FA 8FCF EDDD 735E 1842 0842 C963 A3E7 8A22 FED9 23AE 4C7D CDFA FACD 4C04 15FC 021F C385 5843 BE5D E5EA A3CF AD77 256F A716
Расширения сертификата X.509
Расширение: Использование ключа (критичное)
Идентификатор: 2.5.29.15
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)
Расширение: Идентификатор ключа субъекта
Идентификатор: 2.5.29.14
Значение: 8c 40 33 21 b8 4f 81 ad 91 0b 8e 8e 13 0d a2 d7 88 11 aa fc
Расширение: Идентификатор ключа центра сертификатов
Идентификатор: 2.5.29.35
Значение: Идентификатор ключа=5d 57 b5 97 f5 c9 b0 be 78 64 f2 05 25 9b 7d 2e 7d 52 8e ff, Поставщик сертификата: Адрес каталога:CN=Головной удостоверяющий центр, ИНН=007710474375, ОГРН=1047702026701, O=Минкомсвязь России, STREET="125375 г. Москва, ул. Тверская, д. 7", L=Москва, S=77 г. Москва, C=RU, E=dit@minsvyaz.ru, Серийный номер сертификата=00 b6 b2 a7 60 00 00 00 00 01 ea
Расширение: Улучшенный ключ
Идентификатор: 2.5.29.37
Значение: Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4), Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6), Пользователь службы актуальных статусов (1.2.643.2.2.34.26), Пользователь службы штампов времени (1.2.643.2.2.34.25), Доступ к СМЭВ (ЭП-СП) (1.2.643.100.2.1), Руководитель органа государственной власти субъекта РФ или иное УЛ данного органа (1.2.643.5.1.24.2.6)
Расширение:Политики применения
Идентификатор: 1.3.6.1.4.1.311.21.10
Значение: [1]Политика сертификата приложения:Идентификатор политики=Проверка подлинности клиента, [2]Политика сертификата приложения:Идентификатор политики=Защищенная электронная почта, [3]Политика сертификата приложения:Идентификатор политики=Пользователь Центра Регистрации, HTTP, TLS клиент, [4]Политика сертификата приложения:Идентификатор политики=Пользователь службы актуальных статусов, [5]Политика сертификата приложения:Идентификатор политики=Пользователь службы штампов времени, [6]Политика сертификата приложения:Идентификатор политики=Доступ к СМЭВ (ЭП-СП), [7]Политика сертификата приложения:Идентификатор политики=Руководитель органа государственной власти субъекта РФ или иное УЛ данного органа
Расширение: Политики сертификата
Идентификатор: 2.5.29.32

Значение: [1]Политика сертификата:Идентификатор политики=Класс средства ЭП КС1, [2]Политика сертификата:Идентификатор политики=Класс средства ЭП КС2

Расширение: Дополнительное имя субъекта

Идентификатор: 2.5.29.17

Значение: Имя RFC822=test@cap.ru

Расширение: Средства электронной подписи и УЦ издателя

Идентификатор: 1.2.643.100.112

Значение: Средство электронной подписи: "КриптоПро CSP" (версия 4.0) (заключение: Сертификат соответствия № СФ/124-2864 от 20.03.2016), средство удостоверяющего центра: "КриптоПро УЦ" версии 2.0 (заключение: Сертификат соответствия № СФ/128-2983 от 18.11.2016)

Расширение: Средство электронной подписи владельца

Идентификатор: 1.2.643.100.111

Значение: Средство электронной подписи: "КриптоПро CSP" (версия 4.0)

Расширение: Точки распространения списков отзыва (CRL)

Идентификатор: 2.5.29.31

Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://ra-cit.cap.ru/cdp/5d57b597f5c9b0be7864f205259b7d2e7d528eff.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://uccit.cap.ru/cdp/uc-cit.crl, [3]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://cdp.cap.ru/cdp/uc-cit.crl

Расширение: Доступ к информации о центрах сертификации

Идентификатор: 1.3.6.1.5.5.7.1.1

Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ra-cit.cap.ru/ocsp/ocsp.srf, [2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://ra-cit.cap.ru/aia/5d57b597f5c9b0be7864f205259b7d2e7d528eff.crt, [3]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://uc-cit.cap.ru/aia/uc-cit.crt, [4]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://cdp.cap.ru/aia/uc-cit.crt

Расширение: Период использования ключа электронной подписи

Идентификатор: 2.5.29.16

Значение: Действителен с 1 марта 2018 г. 19:19:11 по 1 марта 2019 г. 19:19:11

Подпись Удостоверяющего центра:

Алгоритм подписи: ГОСТ Р 34.11/34.10-2001 (1.2.643.2.2.3) Параметры:

Значение: EC0B 3956 A36C ACA0 557A A52C 43E7 86A8 3F88 5285 78F4 0A22 1062 3A7C B61A 0400 1F66 059E 0432 F858 C5B3 8D63 CB46 DB81 73EC 3E4A B267 3CB1 814C F935 B3E0 FA91

Подпись владельца сертификата (уполномоченного представителя): _____/_____

"___" _____ 20___ г.

Подпись уполномоченного лица УЦ: _____/_____

"___" _____ 20__ г.

М. П.

Приложение № 10
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии
(Форма сертификата ключа проверки электронной подписи на бумажном носителе)

Для физических лиц и индивидуальных предпринимателей

Удостоверяющий центр БУ "Центр информационных технологий" Мининформполитики Чувашии
Копия сертификата ключа проверки электронной подписи
Сведения о сертификате:

Версия: 3
Серийный номер: 76F0508A762CBD80E8116D1D7541DBAB
Издатель сертификата: CN=БУ "Центр информационных технологий" Мининформполитики Чувашии, O=БУ "Центр информационных технологий" Мининформполитики Чувашии, E=uc-info@cap.ru, STREET=ул. Калинина, д.112, L=Чебоксары, S=21 Чувашская Республика- Чувашия, C=RU, ИНН=002130176633, ОГРН=1162130063501
Владелец сертификата: CN= Иванов Иван Иванович, L=Чебоксары, S=21 Чувашская Республика - Чувашия, C=RU, SN=Иванов, G=Иван Иванович, STREET=Тестовая ул, 1, ИНН=000000000000, СНИЛС=00000000000
Срок действия:
Действителен с: 17.01.2018 14:53:00
Действителен по: 17.03.2018 16:03:00
Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2001 (1.2.643.2.2.19)
Параметры: 30 12 06 07 2A 85 03 02 02 24 00 06 07 2A 85 03 02 02 1E 01
Значение: 0440 F256 3C1F 199D 35A3 84B6 D805 BC6D 0E6F 18B6 BCA3 C14D 47D3 64BC 674B 97C5 D2E2 311A A675 A658 77B7 9A21 95E4 E950 CC4D 5BB8 E8F9 6E1D 4A70 BF62 E7FB 5828 D368
Расширения сертификата X.509
Расширение: Использование ключа (критичное)
Идентификатор: 2.5.29.15
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)
Расширение: Идентификатор ключа субъекта
Идентификатор: 2.5.29.14
Значение: b6 7a 9a 1f 59 5b 94 6f de 04 10 70 f5 e5 55 dd 18 06 5e 3b
Расширение: Идентификатор ключа центра сертификатов
Идентификатор: 2.5.29.35
Значение: Идентификатор ключа=5d 57 b5 97 f5 c9 b0 be 78 64 f2 05 25 9b 7d 2e 7d 52 8e ff, Поставщик сертификата: Адрес каталога:CN=Головной удостоверяющий центр, ИНН=007710474375, ОГРН=1047702026701, O=Минкомсвязь России, STREET="125375 г. Москва, ул. Тверская, д. 7", L=Москва, S=77 г. Москва, C=RU, E=dit@minsvyaz.ru, Серийный номер сертификата=00 b6 b2 a7 60 00 00 00 00 01 ea
Расширение: Улучшенный ключ
Идентификатор: 2.5.29.37
Значение: Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4), Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6), Пользователь службы актуальных статусов (1.2.643.2.2.34.26), Пользователь службы штампов времени (1.2.643.2.2.34.25)
Расширение: Политики применения
Идентификатор: 1.3.6.1.4.1.311.21.10
Значение: [1]Политика сертификата приложения:Идентификатор политики=Проверка подлинности клиента, [2]Политика сертификата приложения:Идентификатор политики=Защищенная электронная почта, [3]Политика сертификата приложения:Идентификатор политики=Пользователь Центра Регистрации, HTTP, TLS клиент, [4]Политика сертификата приложения:Идентификатор политики=Пользователь службы актуальных статусов, [5]Политика сертификата приложения:Идентификатор политики=Пользователь службы штампов времени
Расширение: Политики сертификата
Идентификатор: 2.5.29.32
Значение: [1]Политика сертификата:Идентификатор политики=Класс средства ЭП КС1, [2]Политика сертификата:Идентификатор политики=Класс средства ЭП КС2
Расширение: Дополнительное имя субъекта
Идентификатор: 2.5.29.17
Значение: Имя RFC822=test@cap.ru
Расширение: Средства электронной подписи и УЦ издателя
Идентификатор: 1.2.643.100.112

Значение: Средство электронной подписи: "КриптоПро CSP" (версия 4.0) (заключение: Сертификат соответствия № СФ/124-2864 от 20.03.2016), средство удостоверяющего центра: "КриптоПро УЦ" версии 2.0 (заключение: Сертификат соответствия № СФ/128-2983 от 18.11.2016)

Расширение: Средство электронной подписи владельца

Идентификатор: 1.2.643.100.111

Значение: Средство электронной подписи: "КриптоПро CSP" (версия 4.0)

Расширение: Точки распространения списков отзыва (CRL)

Идентификатор: 2.5.29.31

Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://ra-cit.cap.ru/cdp/5d57b597f5c9b0be7864f205259b7d2e7d528eff.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://uccit.cap.ru/cdp/uc-cit.crl, [3]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://cdp.cap.ru/cdp/uc-cit.crl

Расширение: Доступ к информации о центрах сертификации

Идентификатор: 1.3.6.1.5.5.7.1.1

Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния сертификата через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ra-cit.cap.ru/ocsp/ocsp.srf, [2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://ra-cit.cap.ru/aia/5d57b597f5c9b0be7864f205259b7d2e7d528eff.crt, [3]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://uc-cit.cap.ru/aia/uc-cit.crt, [4]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://cdp.cap.ru/aia/uc-cit.crt

Расширение: Период использования ключа электронной подписи

Идентификатор: 2.5.29.16

Подпись Удостоверяющего центра:

Алгоритм подписи: ГОСТ Р 34.11/34.10-2001 (1.2.643.2.2.3) Параметры:

Значение: BEF5 D0C1 46EC AE29 0540 BE0D 7CEE 902D D354 5A63 600D A2AC 16E1 6799 41F5 F8F1 24B1 95AC 2C8B D265 58A3 2DEA C57E 458A 94CB 49FA B287 7BC1 A10A 0D8E 18A5 422C

Подпись владельца сертификата (уполномоченного представителя): _____/_____

"___" _____ 20___ г.

Подпись уполномоченного лица УЦ: _____/_____

"_" _____ 20__ г.

М. П.

Приложение № 11
к Регламенту Удостоверяющего центра БУ «Центр информационных технологий» Мининформполитики Чувашии

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Общие принципы обеспечения информационной безопасности при организации электронного взаимодействия с использованием электронной подписи

Организация электронного взаимодействия с использованием электронной подписи должна осуществляться с учетом требований федеральных законов «Об электронной подписи», «Об информации, информационных технологиях и о защите информации», Постановления Правительства Российской Федерации «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» от 9 февраля 2012 года № 111, Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ №152), других федеральных законов и нормативных правовых актов, осуществляющих правовое регулирование отношений в области обеспечения защиты информации и использования электронной подписи, руководящих документов ФСТЭК России и ФСБ России, эксплуатационной и технической документации на используемые средства электронной подписи, средства криптографической защиты информации (далее - СКЗИ).

Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Риски, связанные с использования электронной подписи и средств электронной подписи

В случае, если электронное взаимодействие с использованием электронной подписи осуществляется без учета требований нормативных правовых актов, регулирующих отношения в области использования электронных подписей, могут возникнуть или существенно возрасти риски, связанные с использованием электронной подписи, основными из которых могут являться:

- риски, связанные с проверкой принадлежности ключа электронной подписи, с помощью которой подписан электронный документ, владельцу сертификата. Лицо, владеющее сертификатом ключа проверки электронной подписи и соответствующим ему ключом электронной подписи, которым был подписан электронный документ, может заявить о том, что электронная подпись, содержащаяся в электронном документе, создана с использованием ключа электронной подписи, который не принадлежит данному владельцу сертификата;

- риски, связанные с внесенными в электронный документ изменениями, произведенными после его подписания. Лицо, ключом электронной подписи которого был подписан электронный документ, может заявить о том, что содержание документа было изменено и не соответствует содержанию документа, подписанному данным лицом;

- риски, связанные с признанием электронного документа, содержащего электронную подпись. Одна из сторон может заявить о том, что подписанный электронной подписью документ не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;

- риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае, если порядок использования электронной подписи и средств электронной подписи не соответствует требованиям нормативных правовых актов Российской Федерации, осуществляющих правовое регулирование отношений в использовании электронной подписи или не соответствует порядку использования электронной подписи, определяемому соглашениями сторон, юридическая значимость подписанных электронной подписью документов может быть поставлена под сомнение;

- риски, связанные с нарушением конфиденциальности ключей электронной подписи (использование ключей электронной подписи без согласия владельца). В случае нарушения конфиденциальности ключей электронной подписи, в том числе компрометации ключей, несанкционированного доступа к ключевым носителям или средствам электронной подписи, может быть принят в исполнение подписанный электронной подписью документ, порождающий юридически значимые последствия и исходящий от имени лица, ключ которого был скомпрометирован;

- риски, связанные с несовместимостью средств электронной подписи, используемых сторонами для организации электронного взаимодействия. Несовместимость средств электронной подписи, протоколов и форматов данных, используемых сторонами для организации электронного взаимодействия, может привести к невозможности проверки электронной подписи или к её некорректной проверке;

- риски, связанные с определением полномочий лица, подписавшего электронной подписью документ. В случае, если участниками межведомственного электронного взаимодействия не определены лица, участвующие в электронном взаимодействии, полномочия данных лиц по подписанию электронных документов от имени участника межведомственного электронного взаимодействия, а также в случае, если полномочия лица по подписанию электронных документов прекращены, одна из сторон может заявить, что полученный электронный документ содержит электронную подпись лица, не уполномоченного на подписание данного документа и не может быть принят в исполнение;

- риски, связанные с использованием сертификатов ключей электронной подписи и ключей электронной подписи, прекративших своё действие. В случае использования для подписания электронных документов ключа электронной подписи, прекратившего своё действие на момент подписания, либо, если момент подписания электронного документа не определен, использования сертификата ключа проверки электронной подписи, недействительного на день проверки электронной подписи, сторона, получившая подписанный электронной подписью документ, может заявить о непризнании такого документа юридически значимым.

В целях минимизации и исключения вышеуказанных рисков участникам электронного взаимодействия необходимо предусмотреть обеспечение комплекса правовых и организационно-технических мероприятий по обеспечению

информационной безопасности при осуществлении электронного взаимодействия с использованием электронной подписи и средств электронной подписи.

Электронное взаимодействие с использованием электронной подписи, осуществляемое с учетом требований Федерального закона «Об электронной подписи», других федеральных законов, принимаемых в соответствии с ними нормативных правовых актов, регулирующих отношения в области использования электронных подписей, позволяет обеспечить:

- неотказуемость от электронного документа, содержащего электронную подпись. Электронная подпись позволяет определить лицо, подписавшее электронный документ;
- целостность электронного документа. Электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания.

В случае необходимости обеспечения конфиденциальности передаваемой информации ключи электронной подписи и СКЗИ могут использоваться для шифрования электронных документов или для организации передачи данных по защищенным каналам связи.

Средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральными законом «Об электронной подписи», позволяют:

- установить факт изменения подписанного электронного документа после момента его подписания;
- обеспечить практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

При создании электронной подписи средства электронной подписи:

- показывают лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
- создают электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;
- однозначно показывают, что электронная подпись создана.

При проверке электронной подписи средства электронной подписи:

- показывают содержание электронного документа, подписанного электронной подписью;
- показывают информацию о внесении изменений в подписанный электронной подписью электронный документ;
- указывают на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Одной из составных частей инфраструктуры открытых ключей и системы криптографической защиты информации является удостоверяющий центр, выполняющий функции по изготовлению и обслуживанию сертификатов ключей проверки электронных подписей, используемых участниками электронного взаимодействия.

Удостоверяющий центр осуществляет свою деятельность в строгом соответствии с нормативными правовыми актами Российской Федерации, руководящими документами, эксплуатационной документацией на используемые средства, Регламентом Удостоверяющего центра и другими документами, регулирующими вопросы использования электронной подписи.

Сертификаты ключей проверки электронных подписей, изготавливаемые Удостоверяющим центром, заверяются электронной подписью уполномоченного лица удостоверяющего центра, что подтверждает факт принадлежности ключа электронной

подписи конкретному лицу участника электронного взаимодействия. Использование сертификатов позволяет участника электронного взаимодействия идентифицировать лицо, подписавшее электронной подписью документ, а также позволяет подтвердить целостность (неизменность) содержания подписанного электронного документа при проверке электронной подписи. Таким образом, при соблюдении требований нормативных правовых актов, регулирующих отношения в области использования электронных подписей, исключаются риски, связанные с подтверждением подлинности и отказом от содержимого документа и исключаются риски, связанные с юридической значимостью электронных документов.

3. Требования и рекомендации по обеспечению информационной безопасности при использовании средств электронной подписи

В организации, эксплуатирующей средства электронной подписи (СКЗИ), должны быть предусмотрены организационные и организационно-технические мероприятия, направленные на обеспечение информационной безопасности при использовании средств электронной подписи и определяющие требования к ответственным лицам, автоматизированным рабочим местам пользователей (далее также - АРМ), системному и прикладному программному обеспечению, условиям хранения и использования средств электронной подписи, ключей электронной подписи и ключевых носителей.

3.1. Требования и рекомендации по назначению ответственных лиц.

В организации должны быть определены лица, наделенные полномочиями по подписанию электронных документов электронной подписью, лица, ответственные за осуществление электронного взаимодействии с использованием электронной подписи и имеющих доступ к ключевым носителям, а также лица, ответственные за организацию работ по защите информации и соблюдению условий хранения и использования ключей электронной подписи и средств электронной подписи.

К работе со средствами электронной подписи должны допускаться лица, прошедшие соответствующее обучение и ознакомленные с Инструкцией ФАПСИ №152, другими нормативными правовыми актами и руководящими документами, в том числе внутренними организационными документами и инструкциями по защите информации и использованию электронной подписи, а также эксплуатационной документацией на используемые средства электронной подписи и Регламентом Удостоверяющего центра.

В организации, эксплуатирующей СКЗИ, должен быть назначен администратор информационной безопасности, на которого возлагаются задачи организации работ по защите информации, подготовки соответствующих инструкций, обучения и инструктажа пользователей, ведению журналов учета СКЗИ, настройке системного, прикладного программного обеспечения, СКЗИ и средств защиты от несанкционированного доступа, устанавливаемого на АРМ пользователей, контролю за соблюдением требований по безопасности, а также взаимодействия с удостоверяющим центром по вопросам использования электронной подписи.

3.2. Требования и рекомендации к помещениям и размещению технических средств АРМ.

Помещения, в которых расположены АРМ, предназначенные для работы со средствами электронной подписи (далее – спецпомещения), должны соответствовать требованиям Инструкции ФАПСИ №152. Должен быть исключен бесконтрольный допуск лиц, не допущенных к работе в указанных спецпомещениях. В случае необходимости присутствия посторонних лиц в спецпомещениях должен быть обеспечен контроль за их действиями.

Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Размещение АРМ должно производиться с учетом размеров контролируемой зоны и исключать возможность просмотра посторонними лицами работ, осуществляемых на АРМ.

Спецпомещения рекомендуется оснащать охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

3.3. Требования и рекомендации к АРМ пользователей.

Не допускается оставлять без контроля АРМ при включенном питании и подключенными ключевыми носителями. Перед уходом пользователь должен выключить АРМ либо заблокировать рабочую станцию с использованием средств защиты информации от несанкционированного доступа или с использованием средств операционной системы. Рекомендуется настроить автоматическое включение экранной заставки, защищенной паролем.

На АРМ пользователей рекомендуется установить сертифицированные средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД), а также средства антивирусной защиты.

В целях исключения возможности несанкционированного изменения аппаратной части системного блока администратору рекомендуется предусмотреть опечатывание системного блока АРМ.

Необходимо предусмотреть организацию парольной защиты при включении АРМ и загрузке операционной системы с использованием СЗИ от НСД (средств доверенной загрузки), либо средств BIOS и средств операционной системы (далее также – ОС), также рекомендуется определить установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске, отключить возможность загрузки с внешних съемных дисков, привода CD-ROM, исключить нестандартные виды загрузки ОС, включая сетевую загрузку.

3.4. Требования и рекомендации по настройке системного и прикладного программного обеспечения.

На технических средствах АРМ с установленными средствами электронной подписи необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников. Не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

Не допускается установка на АРМ средств разработки и отладки программного обеспечения. Необходимо исключить возможность установки средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также вредоносного программного обеспечения, позволяющего несанкционированно получать привилегии администратора.

Рекомендуется ограничить возможности пользователя запуском только тех приложений, которые разрешены администратором безопасности.

Необходимо регулярно отслеживать и устанавливать обновления безопасности для программного обеспечения АРМ (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.4.1. Настройка операционной системы АРМ.

До начала использования средств электронной подписи администратор информационной безопасности должен произвести настройку операционной системы, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль настроек в соответствии со следующими рекомендациями:

- правом установки и настройки ОС и средств электронной подписи должен обладать только администратор безопасности;
- в целях возможности разграничения прав доступа рекомендуется использовать средства, входящие в состав СЗИ от НСД, для работы ОС рекомендуется использование файловой системы NTFS;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для работы права;
- все привилегии группы Everyone должны быть удалены;
- необходимо исключить использование режима автоматического входа пользователя в операционную систему при ее загрузке без ввода пароля;
- рекомендуется переименовать стандартную учетную запись Administrator;
- рекомендуется отключить учетная запись для гостевого входа Guest;
- исключить возможность удаленного управления, администрирования и модификации ОС и её настроек, системного реестра, для всех, включая группу Administrators;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, службы, сервисы и т.п.);
- должно быть исключено или ограничено использование пользователями сервиса Scheduler (планировщик задач). При использовании данного сервиса состав запускаемого программного обеспечения на АРМ согласовывается с администратором информационной безопасности;
- рекомендуется организовать удаление временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы средств электронной подписи. Если это невыполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
- должны быть отключены средства удаленного администрирования, в т.ч. подключение к рабочему столу с использованием службы терминалов, в случае если такое подключение осуществляется без использования защищенных каналов связи;
- должны быть установлены ограничения на доступ пользователей к системному реестру путем настройки прав доступа к системному реестру;
- на все директории, содержащие системные файлы Windows и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме администратора (Administrator), создателя/владельца (Creator/Owner) и системы (System);
- необходимо обеспечить ведение журналов аудита в ОС, при этом она должна быть настроена на завершение работы при переполнении журналов;
- настройка параметров системного реестра производится в соответствии с эксплуатационной документацией на средства электронной подписи.

3.4.2. Требования и рекомендации при организации парольной защиты.

Рекомендуется разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать правила формирования и хранения паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

- пользователь должен обеспечивать конфиденциальность паролей, не допускается хранить записанные пароли в легкодоступных местах;

- периодичность смены пароля определяется принятой политикой безопасности (инструкцией по организации парольной защиты), но не должна превышать 6 месяцев.

- указанная политика должна применяться для всех учетных записей пользователей, зарегистрированных в операционной системе.

3.4.3. Установка и настройка средств электронной подписи.

Установка и настройка средств электронной подписи (СКЗИ) должна выполняться администратором информационной безопасности либо лицом, ответственным за работоспособность АРМ и прошедшим соответствующее обучение.

Установка средств электронной подписи должна производиться только с дистрибутива, полученного по доверенному каналу, в соответствии с эксплуатационной документацией на средства электронной подписи.

При установке средств электронной подписи должен быть обеспечен контроль целостности устанавливаемого программного обеспечения.

Перед установкой средств электронной подписи необходимо произвести проверку ОС на отсутствие вредоносных программ с помощью антивирусных средств.

После завершения установки осуществляются настройка и контроль работоспособности средств электронной подписи.

3.5. Подключение АРМ к сетям общего пользования.

Не рекомендуется подключать к сетям общего пользования АРМ пользователя средств электронной подписи. В случае необходимости подключения АРМ к сетям связи общего пользования такое подключение рекомендуется производить с использованием сертифицированного межсетевого экрана.

В случае подключения АРМ с установленными средствами электронной подписи к общедоступным сетям передачи данных необходимо ограничить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX и т.д.), полученных из сетей общего пользования, без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносных программ.

3.6. Обращение с ключевыми носителями.

В организации должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации, который должен исключать возможность несанкционированного доступа к ним.

Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

В качестве ключевых носителей рекомендуется использовать сертифицированные USB-ключи и смарт-карты (например eToken, ruToken)

Запрещается:

- выполнять копирование информации с ключевых носителей, которое несанкционированно администратором информационной безопасности;

- знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным;

- устанавливать ключевой носитель в другие ПЭВМ, не предназначенные для работы с ключевой информацией;
- записывать на ключевой носитель постороннюю информацию;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации с использованием средств электронной подписи либо средств, гарантирующих практическую невозможность восстановления информации с ключевых носителей.

Владелец сертификата обязан:

- хранить в тайне ключ электронной подписи;
- немедленно обратиться в удостоверяющий центр для приостановления действия сертификата ключа проверки электронной подписи или его отзыва в случае компрометации ключа электронной подписи или при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- не использовать ключ проверки электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который отозван или действие которого приостановлено.

3.7. Учет и контроль.

Действия, связанные с хранением и эксплуатацией средств электронной подписи и ключей электронной подписи, должны фиксироваться в журналах поэкземплярного учета, ведение которого осуществляется администратором информационной безопасности в соответствии с Инструкцией ФАПСИ № 152

Администратор информационной безопасности должен периодически, не реже одного раза в два месяца, проводить проверку установленного программного обеспечения, журналов аудита операционной системы и средств защиты информации на всех АРМ пользователей, осуществлять контроль за условиями использования и хранения ключевых носителей, а также проводить периодическое тестирование технических и программных средств защиты информации.

В случае обнаружения постороннего программного обеспечения, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией, назначенной руководителем организации, а также организованы работы по анализу и устранению выявленных нарушений.