Зарегистрировано в Минюсте РФ 24 апреля 2009 г. N 13831

МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 23 марта 2009 г. N 41

ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ТЕХНОЛОГИЯМ, ФОРМАТАМ, ПРОТОКОЛАМ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ, УНИФИЦИРОВАННЫМ ПРОГРАММНО-ТЕХНИЧЕСКИМ СРЕДСТВАМ ПОДСИСТЕМЫ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ ОБЩЕРОССИЙСКОГО ГОСУДАРСТВЕННОГО ИНФОРМАЦИОННОГО ЦЕНТРА

Во исполнение Постановления Правительства Российской Федерации от 25 декабря 2007 г. N 931 "О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям" (Собрание законодательства Российской Федерации, 2007, N 53, ст. 6627) и Приказа Министерства информационных технологий и связи Российской Федерации от 11 марта 2008 г. N 32 "Об утверждении Положения об общероссийском государственном информационном центре" (зарегистрирован в Министерстве юстиции Российской Федерации 21 марта 2008 г., регистрационный N 11394) приказываю:

1. Утвердить прилагаемые Требования к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам подсистемы удостоверяющих центров общероссийского государственного информационного центра.

2. Направить настоящий Приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

3. Контроль за исполнением настоящего Приказа оставляю за собой.

Министр
И.О.ЩЕГОЛЕВ

Утверждено
Приказом Министерства связи
и массовых коммуникаций
Российской Федерации
от 23.03.2009 N 41

ТРЕБОВАНИЯ К ТЕХНОЛОГИЯМ, ФОРМАТАМ, ПРОТОКОЛАМ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ, УНИФИЦИРОВАННЫМ ПРОГРАММНО-ТЕХНИЧЕСКИМ СРЕДСТВАМ ПОДСИСТЕМЫ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ ОБЩЕРОССИЙСКОГО ГОСУДАРСТВЕННОГО ИНФОРМАЦИОННОГО ЦЕНТРА

I. Общие положения

1. Требования к технологиям, форматам, протоколам информационного взаимодействия, унифицированным программно-техническим средствам (далее - требования) устанавливают принципы и необходимые условия функционирования подсистемы удостоверяющих центров общероссийского государственного информационного центра (далее - подсистема УЦ ОГИЦ).

Подсистема УЦ ОГИЦ предназначена для оказания государственных услуг гражданам и организациям в электронном виде с использованием электронной цифровой подписи, позволяющей однозначно определить (идентифицировать) правомочность уполномоченных должностных лиц органов государственной власти и местного самоуправления, осуществляющих информационное взаимодействие, дату и время осуществления информационного взаимодействия, а также гарантировать целостность, неизменность и идентичность информации, отправленной одним участником информационного взаимодействия и полученной другим участником информационного взаимодействия.

2. Регламент подсистемы УЦ ОГИЦ (далее - Регламент) разрабатывается и утверждается Федеральным агентством по информационным технологиям.

3. Обеспечение защиты информации в подсистеме УЦ ОГИЦ должно осуществляться в соответствии с законодательством Российской Федерации.

4. Порядок взаимодействия подсистемы УЦ ОГИЦ с информационными системами федеральных органов исполнительной власти в целях оказания государственных и муниципальных услуг устанавливается совместными регламентами, утверждаемыми Министерством связи и массовых коммуникаций Российской Федерации и федеральными органами исполнительной власти, участвующими в информационном взаимодействии с целью предоставления соответствующих государственных услуг.

5. Условия взаимодействия подсистемы УЦ ОГИЦ с иными информационными системами в целях оказания государственных услуг устанавливается соглашением, заключаемым Федеральным агентством по информационным технологиям и оператором соответствующей информационной системы.

6. Подсистема УЦ ОГИЦ должна создаваться и функционировать в соответствии с положениями, определенными Федеральным законом от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи" (Собрание законодательства Российской Федерации, 2002, N 2, ст. 127; 2007, N 46, ст. 5554); Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448); Постановлением Правительства Российской Федерации от 25 декабря 2007 г. N 931 "О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям" (Собрание законодательства Российской Федерации, 2007, N 53, ст. 6627) и Приказом Министерства связи и массовых коммуникаций Российской Федерации от 11 марта 2008 г. N 32 "Об утверждении Положения об общероссийском государственном информационном центре" (зарегистрирован в Министерстве юстиции Российской Федерации 21 марта 2008 г. N 11394).

II. Требования к составу и программно-техническим средствам

7. В состав подсистемы УЦ ОГИЦ должны быть включены следующие компоненты:

УЦ ОГИЦ ПУ;

УЦ ОГИЦ ВУ (один или несколько);

подсистема ведения реестра (реестров);

подсистема, используемая для оказания государственных услуг в электронном виде при трансграничном международном взаимодействии;

подсистема, используемая для реализации сервисов УЦ ОГИЦ в соответствии с перечнем сервисов подсистемы ведения реестров;

подсистема защиты информации УЦ ОГИЦ;

подсистема информирования;

автоматизированные рабочие места УЦ ОГИЦ;

идентификационные элементы на электронных носителях (далее -электронные идентификационные элементы);

носители ключевой информации (закрытого/открытого ключей и сертификата) электронной цифровой подписи.

8. Компоненты подсистемы УЦ ОГИЦ должны обеспечивать реализацию следующих функций (информационных технологий):

1) УЦ ОГИЦ ПУ должен обеспечивать:

формирование сертификатов ключей подписи уполномоченных лиц УЦ ОГИЦ ПУ;

формирование сертификатов ключей подписей (далее - СКП) уполномоченных лиц УЦ ОГИЦ ВУ (далее - СКП УЦ ОГИЦ ВУ), включая изготовление ключей ЭЦП;

временное приостановление действия СКП УЦ ОГИЦ ВУ;

возобновление действия СКП УЦ ОГИЦ ВУ;

аннулирование (отзыв) СКП УЦ ОГИЦ ВУ;

формирование и распространение списков аннулированных (отозванных) и приостановленных СКП УЦ ОГИЦ ВУ;

ведение архива СКП УЦ ОГИЦ ВУ;

ведение реестра СКП УЦ ОГИЦ ВУ;

2) УЦ ОГИЦ ВУ должен обеспечивать:

формирование СКП уполномоченных лиц удостоверяющих центров в федеральных округах и уполномоченных лиц информационных систем, включая изготовление ключей ЭЦП;

временное приостановление действия СКП;

возобновление действия СКП;

аннулирование (отзыв) СКП;

формирование и распространение списков аннулированных (отозванных) и приостановленных СКП;

ведение архива СКП;

ведение реестра СКП;

3) подсистема ведения реестров должна обеспечивать:

а) размещение следующей информации в реестре (реестрах):

о сертификатах ключей подписей (единый государственный реестр СКП);

о СКП уполномоченных лиц федеральных органов государственной власти;

о СКП уполномоченных лиц информационных систем ОГИЦ;

о сервисах и услугах, предоставляемых УЦ ОГИЦ и взаимодействующих с ним удостоверяющими центрами и информационными системами;

об объектных идентификаторах, используемых в ОГИЦ;

об удостоверяющих центрах, взаимодействующих с подсистемой УЦ ОГИЦ на основе Соглашения о взаимодействии между Федеральным агентством по информационным технологиям и удостоверяющим центром в рамках подсистемы УЦ ОГИЦ;

б) регистрацию пользователей, включая уполномоченных лиц удостоверяющих центров, федеральных органов государственной власти, информационных систем;

в) идентификацию пользователей, зарегистрированных в подсистеме реестров;

г) права пользователей в отношении получения и направления в их адрес информации;

д) возможность поддержания в актуальном состоянии информации, хранящейся в реестрах;

е) возможность свободного доступа заинтересованных лиц к информации из реестра, размещенной в информационно-телекоммуникационной сети Интернет на официальном сайте ОГИЦ;

ж) предоставление по запросам заинтересованным лицам информации (выписки) из реестров, в том числе для целей осуществления правосудия;

з) возможность архивного хранения информации, содержащейся в реестрах;

и) возможность использования ЭЦП и сертификата ключа подписи, выданного УЦ ОГИЦ ПУ для обеспечения целостности информации в реестре и заверения электронных документов, содержащих информацию из реестров и размещаемых в информационно-телекоммуникационной сети Интернет на официальном сайте ОГИЦ;

к) возможность использования ЭЦП уполномоченного лица УЦ ОГИЦ ПУ при информационном обмене между реестрами;

4) подсистема, используемая для оказания государственных услуг в электронном виде при трансграничном международном взаимодействии, должна обеспечивать реализацию следующих функций (информационных технологий):

проверку действительности (подлинности) ЭЦП в электронном документе при трансграничном электронном документообороте и формирование квитанции от текущей даты проверки (метки времени);

проверку действительности (подлинности) ЭЦП в документе при электронном документообороте внутри Российской Федерации;

проверку действительности (подлинности) сертификата открытого ключа, изготовленного иным удостоверяющим центром;

5) подсистема, используемая для реализации сервисов УЦ ОГИЦ, должна обеспечивать реализацию сервисов при оказании государственных услуг в электронном виде, включая предоставление услуги по определению актуального статуса сертификата, по фиксации времени, разбору конфликтных ситуаций, подтверждению подлинности ЭЦП уполномоченных лиц в выданных СКП;

6) автоматизированные рабочие места УЦ ОГИЦ, оборудованные современными средствами идентификации участников информационного взаимодействия, должны обеспечивать доступ (локальный и удаленный) к компонентам подсистемы УЦ ОГИЦ и обеспечивать процедуру изготовления и хранения сертификатов и ключей ЭЦП для уполномоченных лиц, административного персонала и пользователей (далее - пользователи) на носителях ключевой информации, применяемых в подсистеме УЦ ОГИЦ;

7) электронные идентификационные элементы и носители ключевой информации должны обеспечивать:

механизмы аутентификации пользователя и приложений, базирующиеся на использовании российских сертифицированных криптографических алгоритмов, сертификатов ключей подписей, совместимые с подсистемой регламентированного доступа ОГИЦ;

конфиденциальность и целостность идентификационной и ключевой информации, передаваемой при взаимодействии с прикладным программным обеспечением;

8) программно-аппаратный комплекс средств защиты информации должен обеспечить:

управление доступом к ресурсам подсистемы УЦ ОГИЦ, включая использование электронных идентификационных элементов и носителей ключевой информации;

регистрацию и учет действий пользователей подсистемы УЦ ОГИЦ;

защищенный обмен пользователей подсистемы УЦ ОГИЦ;

сохранение целостности ресурсов подсистемы УЦ ОГИЦ;

защиту оборудования подсистемы УЦ ОГИЦ от утечки информации по техническим и побочным каналам.

III. Требования к форматам и протоколам информационного взаимодействия

9. Требования к программной и информационной совместимости компонентов:

1) в части программной совместимости должна быть обеспечена совместимость компонентов, реализованных на платформе базовой операционной системы, с основными производителями аппаратного обеспечения, сетевых плат;

2) операционная система, в рамках которой должен функционировать УЦ ОГИЦ ПУ и УЦ ОГИЦ ВУ, должна обеспечивать возможность поддержки RAID-массивов;

3) в части информационной совместимости должны использоваться стандартные протоколы сетевого и информационного взаимодействия.

10. Требования к алгоритмам и стандартам, используемым для обеспечения информационной безопасности в подсистеме УЦ ОГИЦ.

Для выполнения криптографических преобразований должны использоваться алгоритмы, устанавливаемые государственными стандартами Российской Федерации:

алгоритм формирования и проверки ЭЦП, реализованный в соответствии с требованиями ГОСТ Р 34.10-2001 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи";

алгоритм выработки значения хэш-функции, реализованный в соответствии с требованиями ГОСТ Р 34.11-94 "Информационная технология. Криптографическая защита информации. Функция хэширования";

алгоритм зашифрования/расшифрования данных и вычисления имитовставки, реализованный в соответствии с требованиями ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

11. Требования к структуре сертификатов ключа подписи, списку отозванных сертификатов и используемым протоколам:

1) структура и состав сертификата ключа подписи должны соответствовать требованиям Федерального закона от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи" (Собрание законодательства Российской Федерации, 2002, N 2, ст. 127; 2007, N 46, ст. 5554);

2) сертификаты ключей подписей должны содержать следующие базовые поля:

Signature:	Электронная цифровая подпись уполномоченного лица УЦ
Issuer:	Идентифицирующие данные уполномоченного лица УЦ
Validity:	Даты начала и окончания срока действия сертификата
Subject:	Идентифицирующие данные владельца сертификата открытого ключа
SubjectPublicKeylnformation:	Идентификатор алгоритма средства электронной цифровой подписи, с которыми используется данный открытый ключ, значение открытого ключа
Version:	Версия сертификата формата X.509 - версия 3
SerialNumber:	Уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов открытых ключей УЦ

3) Сертификаты ключей подписей должны содержать следующие дополнительные поля:

AuthorityKeyIdentifier	Идентификатор ключа уполномоченного лица УЦ
SubjectKeyIdentifier	Идентификатор ключа владельца сертификата

ExtendedKeyUsage	Допустимая (легитимная) область (области) использования ключа техническими протоколами и алгоритмами
CertificatePolicies	Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение
CRLDistributionPoint	Точка распространения списка аннулированных (отозванных) сертификатов открытых ключей, изданных УЦ
KeyUsage	Назначение ключа
FreshestCRL	Точка распространения обновлений к регулярному списку аннулированных (отозванных) сертификатов открытых ключей, изданных УЦ (в соответствии с RFC 5280 используется для прикладных систем, в которых оперативная реакция на изменения статуса сертификата является ключевым требованием)

4) обязательными атрибутами поля идентификационных данных уполномоченного лица удостоверяющего центра должны являться:

Common Name или pseudonym	Фамилия, имя, отчество или псевдоним
SerialNumber	Серийный номер (в соответствии с RFC 5280 указывается для обеспечения уникальности различимых имен владельцев сертификатов ключа подписи)
Organization Unit	Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего Центра
Email	Адрес электронной почты (в соответствии с RFC 5280 возможна запись в SubjectAltName)
Country	RU (Российская Федерация)
Location	Место регистрации организации, являющейся владельцем УЦ

5) обязательными атрибутами поля идентификационных данных сертификата пользователя должны являться:

Common Name или pseudonym	Фамилия, имя, отчество или псевдоним
SerialNumber	Серийный номер имени (в соответствии с RFC 5280 указывается для обеспечения уникальности различимых имен владельцев сертификатов ключа подписи)
Organization Unit	Наименование подразделения
Email	Адрес электронной почты (в соответствии с RFC 5280 возможна запись в SubjectAltName)
Country	RU (Российская Федерация)

6) список отозванных сертификатов ключей подписи, который издает удостоверяющий центр, должен соответствовать формату X.509 версии 2 с возможным использованием следующих дополнительных полей:

Authority Key Identifier	Идентификатор ключа уполномоченного лица удостоверяющего Центра
Reason Code	Код причины отзыва сертификата открытого ключа

SzOID_CERTSRV_CA_VERSION	Объектный идентификатор MS Certificate Server, определяющий версию службы сертификации MS CA только для УЦ, построенных на базе MS Certificate Server

12. Требования к объектным идентификаторам:

в целях обеспечения унификации определения сведений об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение, удостоверяющие центры подсистемы УЦ ОГИЦ должны обеспечивать возможность формирования единых объектных идентификаторов в издаваемых ими сертификатах ключей подписи, учитывая ГОСТ Р ИСО/МЭК 8824-4-2003 "Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1)" и следующие рекомендации:

для общероссийского государственного информационного центра корневым идентификатором является 1.2.643.7.2;

для удостоверяющего центра УЦ ОГИЦ ПУ общероссийского государственного информационного центра корневым идентификатором является 1.2.643.7.2.1;

для идентификации базовых политик, используемых в сертификатах удостоверяющих центров, корневым идентификатором является 1.2.643.7.2.1.1;

для идентификации удостоверяющих центров второго уровня общероссийского государственного информационного центра (УЦ ОГИЦ ВУ) корневым идентификатором является 1.2.643.7.2.1.2;

для идентификации сведений (политик применения) об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение, корневым идентификатором является 1.2.643.7.2.1.3.

IV. Требования к унифицированным программно-техническим средствам

13. Требования к техническим средствам и помещениям:

1) требования к техническим средствам:

а) размещение технических средств подсистемы УЦ ОГИЦ должно быть выполнено с учетом требований нормативных документов, определяющих порядок использования средств защиты информации в составе компонент подсистемы УЦ ОГИЦ;

б) технические средства УЦ ОГИЦ должны быть размещены в контролируемой зоне с выделением отдельных изолированных помещений;

в) программно-аппаратные комплексы подсистемы УЦ ОГИЦ должны быть подключены к источникам бесперебойного питания;

2) требования к помещениям:

а) входные двери помещений должны быть оборудованы электронной системой контроля доступа;

б) помещения должны быть оборудованы охранно-пожарной и тревожной сигнализацией, средствами вентиляции и кондиционирования воздуха;

в) в качестве оконечных устройств сигнализации должны использоваться датчики, не обладающие эффектом электроакустических преобразований.

14. Требования к электронным идентификационным элементам:

1) в качестве электронного идентификационного элемента пользователя подсистемы УЦ ОГИЦ должны использоваться электронные носители, реализующие функции персонального электронного идентификатора ОГИЦ;

2) в электронном идентификационном элементе должны быть реализованы:

а) механизм выполнения арифметических операций в группе точек на эллиптических кривых;

б) хранение и использование закрытого ключа ЭЦП, исключающие факт доступа посторонних лиц к нему, или подозрение на такой доступ, в принятой модели нарушителя, путем применения принципа разделения ключа на отдельные доли.

15. Требования к носителям ключевой информации:

1) в качестве носителя ключевой информации для пользователя подсистемы УЦ ОГИЦ должны использоваться носители, защищенные с использованием средств криптографической защиты информации;

2) в носителе ключевой информации должны быть реализованы:

а) механизм выполнения операций в группе точек на эллиптических кривых;

б) хранение и использование закрытого ключа ЭЦП, исключающие факт доступа посторонних лиц к нему, или подозрение на такой доступ, в принятой модели нарушителя, путем применения принципа разделения ключа на отдельные доли.

16. Требования к основным техническим характеристикам.

Заданные функции подсистемы УЦ ОГИЦ должны быть реализованы ее техническим средствам с следующими количественными характеристиками по работоспособности, производительности и надежности:

1) подсистема УЦ ОГИЦ должна обеспечивать выполнение целевых функций круглосуточно в течение всего года, используя необходимые организационно-технические мероприятия, в частности резервирование и внеплановую замену аппаратных компонентов, резервирование баз данных подсистемы;

2) производительность подсистемы УЦ ОГИЦ должна характеризоваться следующими данными:

а) программно-аппаратный комплекс, реализующий функции УЦ ОГИЦ ПУ, должен обеспечивать возможность:

формирования до 360 сертификатов ключей подписей в сутки;

ведения архива сертификатов не менее чем на 2 000 000 СКП;

б) программно-аппаратный комплекс, реализующий функции УЦ ОГИЦ ВУ, должен обеспечивать возможность:

формирования до 360 СКП пользователей УЦ на каждом автоматизированном рабочем месте в сутки;

ведения архива сертификатов не менее чем на 2 000 000 СКП;

в) программно-аппаратный комплекс, реализующий функции подсистемы ведения реестра(ов), должен обеспечивать возможность:

размещения информации не менее чем на 20 000 СКП уполномоченных лиц удостоверяющих центров;

ведение архива не менее чем на 150 000 аннулированных СКП уполномоченных лиц удостоверяющих центров;

размещения информации не менее чем на 20 000 СКП уполномоченных лиц федеральных органов исполнительной власти;

ведение архива не менее чем на 150 000 аннулированных СКП уполномоченных лиц федеральных органов исполнительной власти;

размещения информации не менее чем на 5 000 СКП уполномоченных лиц информационных систем, взаимодействующих с ОГИЦ;

ведение архива не менее чем на 10 000 аннулированных СКП уполномоченных лиц информационных систем, взаимодействующих с ОГИЦ;

размещения информации не менее чем на 10000 записей об удостоверяющих центрах, взаимодействующих с УЦ ОГИЦ, включая записи о текущем статусе взаимодействия с подсистемой УЦ ОГИЦ;

размещения информации не менее чем на 10000 записей о сервисах и услугах, предоставляемых подсистемой УЦ ОГИЦ и взаимодействующими с ней удостоверяющими центрами и информационными системами, включая текущий статус;

размещения информации не менее чем на 10000 записей об объектных идентификаторах, используемых в ОГИЦ;

3) программно-аппаратный комплекс, реализующий функции узла, используемого для оказания государственных услуг в электронном виде при трансграничном (междоменном и международном) взаимодействии, должен обеспечивать возможность:

проверки действительности (подлинности) ЭЦП в электронном документе при трансграничном электронном документообороте и формирование квитанции от текущей даты проверки (метки времени) не менее чем на 1000 документах в сутки;

проверки действительности (подлинности) ЭЦП в документе при электронном документообороте между различными доменами внутри Российской Федерации не менее чем на 10000 документах в сутки;

проверки действительности (подлинности) СКП, изготовленного иным удостоверяющим центром, не менее чем на 10000 документах в сутки;

4) Программно-аппаратный комплекс, реализующий функции узла, используемого для реализации сервисов в соответствии с перечнем сервисов, содержащихся в подсистеме ведения реестров, должен обеспечивать возможность:

определения актуального статуса сертификата ключа подписи в режиме реального времени - не менее 50000 сертификатов в сутки (цифра должна определяться для конкретной системы);

формирования штампов времени для не менее 50000 сертификатов в сутки (цифра должна определяться для конкретной системы);

разбора не менее 10 ситуаций в сутки по подтверждению подлинности ЭЦП уполномоченных лиц в выданных СКП;

5) программно-аппаратный комплекс, реализующий функции автоматизированного рабочего места УЦ ОГИЦ, должен обеспечивать возможность регистрации пользователя и выдачи сертификатов для не менее 100 сертификатов в сутки;

6) носители ключевой информации и электронные идентификационные элементы должны обеспечивать:

устойчивость к воздействию отказов и сбоев, в том числе инициированных внешними воздействиями (облучениями);

эргономические и технические характеристики, пригодные для массового производства и использования.

17. Требования по информационной безопасности:

1) средства криптографической защиты информации (включая средства ЭЦП), используемые в подсистеме УЦ ОГИЦ, должны быть сертифицированы и эксплуатироваться в полном соответствии с требованиями эксплуатационной и нормативной документации;

2) уровень защиты используемых средств криптографической информации должен быть указан в эксплуатационной документации УЦ;

3) требования по полномочиям:

Для выполнения функций УЦ ОГИЦ должно использоваться разграничение членов группы администраторов по полномочиям;

4) требования к управлению доступом:

при выполнении функций в подсистеме УЦ ОГИЦ должно использоваться управление доступом к таким объектам, как базы данных, ключи;

5) требования к идентификации и аутентификации:

идентификация и аутентификация должны включать в себя распознавание пользователя, члена группы администраторов или процесса и проверку их подлинности;

для аутентификации членов группы администраторов при их обращении к средствам вычислительной техники, входящим в состав подсистемы УЦ ОГИЦ, должны использоваться персональные идентификационные элементы и/или периодически изменяющийся пароль;

регистрация владельца сертификата должна осуществляться только при предъявлении им документов, удостоверяющих личность;

в подсистеме УЦ ОГИЦ должен быть реализован механизм аутентификации удаленных пользователей, а также процессов при их обращении к техническим средствам подсистемы УЦ ОГИЦ;

в подсистеме УЦ ОГИЦ должен быть реализован механизм аутентификации локальных пользователей, имеющих доступ к техническим средствам, входящим в состав подсистемы УЦ ОГИЦ, но не входящих в состав группы администраторов.

18. Требования к программному обеспечению подсистемы УЦ ОГИЦ:

программное обеспечение вычислительных средств, на котором функционирует подсистема УЦ ОГИЦ, не должно содержать средств отладки программ, позволяющих модифицировать или искажать штатные алгоритмы работы технических средств подсистемы УЦ ОГИЦ.

19. Требованиями к аппаратным компонентам подсистемы УЦ ОГИЦ:

аппаратные средства, на которых реализуются компоненты подсистемы УЦ ОГИЦ, должны иметь соответствующие сертификаты качества.

20. Требования к надежности:

надежность подсистемы УЦ ОГИЦ должна обеспечиваться:

наличием в УЦ ОГИЦ механизмов резервного копирования баз данных (включая все реестры);

использованием источников бесперебойного питания, обеспечивающим поддержание работоспособности в течение 1 часа;

использованием комплектующих, которые имеют повышенную наработку на отказ;

восстановлением работоспособности в течение времени, не превышающего одного часа после отказа.

21. Требования к целостности технических средств:

в подсистеме УЦ ОГИЦ должны быть реализованы механизм контроля несанкционированного случайного и/или преднамеренного искажения (изменения, модификации) и/или разрушения информации, программных и аппаратных компонентов подсистемы УЦ ОГИЦ, механизм контроля целостности и восстановления целостности технических средств подсистемы УЦ ОГИЦ.

22. Требования к ключевой информации:

закрытый ключ, используемый для подписи СКП и списка отозванных сертификатов, должен использоваться только для этих целей и храниться на отчуждаемом носителе;

должен быть определен порядок формирования ключевой информации, порядок ее уничтожения, сроки действия всех ключей, описание формируемой и/или хранимой в подсистеме УЦ ОГИЦ ключевой информации.

23. Требования к регистрации событий:

в подсистеме УЦ ОГИЦ должен быть реализован механизм, производящий регистрацию событий в журнале, связанных с выполнением подсистемой УЦ ОГИЦ своих целевых функций.

24. Требования к резервному копированию и восстановлению:

в подсистеме УЦ ОГИЦ должен быть реализован механизм резервного копирования и восстановления УЦ ОГИЦ;

должна быть исключена возможность резервного копирования закрытых ключей.

25. Требования по реализации организационно-технических мер обеспечения информационной безопасности:

необходимость наличия лицензий на деятельности по техническому обслуживанию шифровальных (криптографических) средств, а также их распространению в соответствии с законодательством Российской Федерации;

необходимость применения сертифицированных технических и программных средств защиты информации;

необходимость ограничения прав доступа к техническим средствам;

необходимость опечатывания системных блоков и дверей защищенных шкафов, исключающее возможность несанкционированного изменения аппаратной части (целостность технических средств);

необходимость контроля целостности технических средств и легальности установленных копий программного обеспечения на всех компонентах подсистемы УЦ ОГИЦ.

26. Требования к порядку эксплуатации:

в процессе эксплуатации подсистемы УЦ ОГИЦ необходимо обеспечивать поддержание штатного режима работы ее программно-технических средств (далее - ПТС) при условии обязательного выполнения мероприятий, направленных на обеспечение информационной безопасности подсистемы УЦ ОГИЦ;

ответственность за проведение эксплуатационных мероприятий возлагается на обслуживающий персонал и администраторов подсистемы УЦ ОГИЦ.

27. Требования к проведению профилактических работ:

профилактические мероприятия, выполняемые в процессе эксплуатации подсистемы УЦ ОГИЦ, должны охватывать общесистемное программное обеспечение, аппаратные средства, межсетевые экраны.

28. Требования к резервному копированию данных:

при определении данных для архивного хранения и процедур ведения архивов должна быть учтена возможность восстановления рабочего состояния подсистемы ОГИЦ в целом и в отдельности УЦ ПУ ОГИЦ и УЦ ВУ ОГИЦ;

порядок проведения работ по архивированию данных, их периодичность и состав должны определяться регламентом УЦ;

администратор аудита должен регулярно осуществлять архивное копирование журналов аудита на внешние носители информации;

данные архивные копии должны храниться в подсистеме УЦ ОГИЦ не менее срока действия закрытого ключа УЦ ПУ ОГИЦ.

29. Требования к документированию:

в подсистеме УЦ ОГИЦ должны применяться унифицированные порядок и правила документирования информации, операций и процессов в соответствии с ГОСТ Р ИСО 15489-1-2007 "Управление документами. Общие требования".

30. Требования к обеспечению безопасности при модернизации программно-технических средств:

модернизация, а также изменение настроек программно-аппаратных средств подсистемы УЦ ОГИЦ должны осуществляться в соответствии с процедурой, определенной регламентом и внутренними инструкциями подсистемы УЦ ОГИЦ;

все работы по модернизации и изменению настроек компонентов подсистемы УЦ ОГИЦ должны согласовываться с уполномоченным органом в области использования ЭЦП в соответствии с определенным им порядком.

31. Требования к обеспечению качества услуг, предоставляемых подсистемой УЦ ОГИЦ:

для обеспечения качества услуг, предоставляемых подсистемой УЦ ОГИЦ, должен проводиться постоянный контроль качества в соответствии с правилами и процедурами, определенными ГОСТ Р ИСО 9001-2000 "Система менеджмента качества" и внутренними инструкциями подсистемы УЦ ОГИЦ.

V. Требования к информационному взаимодействию

32. Взаимодействие удостоверяющих центров или информационных систем (далее - присоединение) с подсистемой УЦ ОГИЦ при создании единого пространства ЭЦП для

унифицированного оказания государственных услуг в электронном виде и обеспечения межведомственного информационного взаимодействия на территории Российской Федерации в рамках подсистемы УЦ ОГИЦ должно осуществляться на добровольных началах.

33. Техническая реализация присоединения удостоверяющих центров или информационных систем к подсистеме УЦ ОГИЦ должна осуществляться путем включения сертификата ключа подписи уполномоченного лица в подсистему ведения реестров в реестр доверенных УЦ или в реестр доверенных информационных систем.

34. При присоединении УЦ должно быть обеспечено выполнение следующих требований:

1) УЦ должен иметь действительные на протяжении всего срока взаимодействия с подсистемой УЦ ОГИЦ лицензии на следующие виды деятельности:

распространение шифровальных (криптографических) средств;

техническое обслуживание шифровальных (криптографических) средств;

предоставление услуг в области шифрования информации.

2) УЦ должен:

на протяжении всего срока взаимодействия с подсистемой УЦ ОГИЦ следовать единой технологической политике в рамках подсистемы УЦ ОГИЦ;

использовать сертифицированные средства криптографической защиты информации (средства ЭЦП);

использовать источник фиксированного времени от источника времени ОГИЦ для синхронизации функционирования служб и автоматизированных процессов;

применять критерии оценки качества предоставляемых услуг, используемые в подсистеме УЦ ОГИЦ;

использовать электронные идентификационные элементы, принятые к использованию в подсистеме УЦ ОГИЦ;

выдавать СКП для унифицированного оказания государственных услуг в электронном виде, структура которых должна соответствовать структуре сертификатов ключа подписи УЦ ОГИЦ;

в части условий и порядка оказания услуг пользователям в рамках унифицированного оказания государственных услуг в электронном виде должен нести обязательства и ответственность перед пользователями, не противоречащими принятым в подсистеме УЦ ОГИЦ;

представить до начала использования ЭЦП уполномоченного лица УЦ в уполномоченный федеральный орган исполнительной власти СКП уполномоченного лица УЦ в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью УЦ;

обеспечить проведение мероприятий, гарантирующих соответствие установленным требованиям.