МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 61970
от "30" января 2020 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

4 декабря 2020 года Москва № 556

Об утверждении Требований к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи

В соответствии с пунктом 2 части 5 статьи 8 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[1] и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960[2],

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Требования к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи.

2. Настоящий приказ вступает в силу с 1 января 2021 г.

Директор А.Бортников

[1] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2020, № 24, ст. 3755.
[2] Собрание законодательства Российской Федерации, 2003, № 33, ст. 3254; 2018, № 28, ст. 4198.

Утверждены
приказом ФСБ России
от 4 декабря 2020 г.
№ 556

Требования
к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи

I. Требования к средствам доверенной третьей стороны

1. Требования к составу и функциям компонентов средств доверенной третьей стороны

1.1. Средства доверенной третьей стороны (далее – ДТС) содержат следующие компоненты:

1.1.1. Компонент подтверждения действительности электронных подписей, используемых при подписании электронного документа, в том числе установлении фактов того, что соответствующие квалифицированные сертификаты действительны на определенный момент времени, созданы и выданы аккредитованными удостоверяющими центрами, аккредитация которых действительна на день выдачи этих сертификатов (далее – компонент проверки электронной подписи).

1.1.2. Компонент проверки соответствия всех квалифицированных сертификатов, используемых при подписании электронного документа, требованиям, установленным Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»[1] (далее – Закон «Об электронной подписи»), и иным принимаемым в соответствии с ним нормативным правовым актам (далее – компонент проверки квалифицированного сертификата).

1.1.3. Компонент проверки полномочий участников электронного взаимодействия (далее – компонент проверки полномочий).

1.1.4. Компонент создания и подписания квалифицированной электронной подписи ДТС квитанции с результатом проверки

---

[1] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2020, № 24, ст. 3755.

квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания (далее – компонент квитирования).

1.1.5. Компонент создания и проверки метки доверенного времени (далее – TSP-компонент).

1.1.6. Компонент документирования выполняемых средствами ДТС операций.

1.1.7. Компонент предоставления информации об операциях, выполненных средствами ДТС, по запросам участников электронного взаимодействия.

2. Требования к функционированию компонентов средств ДТС

2.1. Компонент проверки электронной подписи должен осуществлять:

2.1.1. Проверку электронной подписи электронного документа, представленного участником электронного взаимодействия, с применением сертификата ключа проверки электронной подписи отправителя, подписавшего данный электронный документ.

2.1.2. Проверку следующей информации, содержащейся в электронной подписи:

- сертификата ключа проверки электронной подписи отправителя;

- сертификата ключа проверки электронной подписи аккредитованного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи отправителя;

- корневого сертификата ключа проверки электронной подписи головного удостоверяющего центра, функции которого осуществляет федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи (далее - головной удостоверяющий центр), на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи аккредитованного удостоверяющего центра, выдавшего сертификат отправителю;

- сертификата ключа проверки электронной подписи ДТС, выданного

удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, и используемого для подписания квитанции с результатом проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания;

- сертификата ключа проверки электронной подписи удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи ДТС;

- корневого сертификата ключа проверки электронной подписи головного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, выдавшего сертификат ДТС, используемый для подписания квитанции с результатом проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания;

- сертификата ключа проверки электронной подписи TSP-компонента, выданного удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, и используемого для подписания метки доверенного времени, создаваемой ДТС;

- сертификата ключа проверки электронной подписи, выданного аккредитованным удостоверяющим центром и используемого для подписания метки доверенного времени в отношении электронного документа отправителя;

- сертификата ключа проверки электронной подписи аккредитованного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи, используемого для подписания метки доверенного времени в отношении электронного

документа отправителя.

2.1.3. Защищенное хранение корневого сертификата ключа проверки электронной подписи головного удостоверяющего центра, исключающее его модификацию, а также несанкционированные добавление и удаление.

2.2. Компонент проверки квалифицированного сертификата должен осуществлять:

2.2.1. Проверку действительности:

- сертификата ключа проверки электронной подписи отправителя на момент подписания им электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

- сертификата ключа проверки электронной подписи аккредитованного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи отправителя, на момент подписания сертификата отправителя (при наличии достоверной информации о моменте подписания сертификата отправителя) или на день проверки действительности проверяемого сертификата, если момент подписания сертификата отправителя не определен;

- корневого сертификата ключа проверки электронной подписи головного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи аккредитованного удостоверяющего центра, выдавшего сертификат отправителю, на момент подписания сертификата удостоверяющего центра (при наличии достоверной информации о моменте подписания сертификата удостоверяющего центра) или на день проверки действительности проверяемого сертификата, если момент подписания сертификата удостоверяющего центра не определен;

- сертификата ключа проверки электронной подписи ДТС, выданного удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, на момент подписания ДТС квитанции с результатом

проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания;

- сертификата ключа проверки электронной подписи удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи ДТС, на момент подписания сертификата ключа проверки электронной подписи ДТС (при наличии достоверной информации о моменте подписания) или на день проверки действительности проверяемого сертификата, если момент подписания сертификата ключа проверки электронной подписи ДТС не определен;

- корневого сертификата ключа проверки электронной подписи головного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, выдавшего сертификат ДТС, используемый для подписания квитанции ДТС, на момент подписания сертификата удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц (при наличии достоверной информации о моменте подписания), или на день проверки действительности проверяемого сертификата, если момент подписания сертификата удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, не определен;

- сертификата ключа проверки электронной подписи TSP-компонента, выданного удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, и используемого для подписания метки доверенного времени, создаваемой ДТС, на момент подписания метки доверенного времени;

- сертификата ключа проверки электронной подписи, выданного аккредитованным удостоверяющим центром и используемого для подписания метки доверенного времени в отношении электронного документа отправителя, на момент проверки метки доверенного времени;

- сертификата ключа проверки электронной подписи аккредитованного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи, используемого для подписания метки доверенного времени в отношении электронного документа отправителя (при наличии достоверной информации о моменте подписания), или на день проверки действительности проверяемого сертификата, если момент подписания сертификата ключа проверки электронной подписи, используемого для подписания метки доверенного времени в отношении электронного документа отправителя, не определен.

2.2.2. Проверку соответствия предъявляемых к сертификатам требований законодательства Российской Федерации, включая требования к их форме, содержанию, к средствам удостоверяющего центра, с использованием которых они созданы, и средствам электронной подписи, с использованием которых они подписаны:

- сертификата ключа проверки электронной подписи отправителя;

- сертификата ключа проверки электронной подписи аккредитованного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи отправителя;

- корневого сертификата ключа проверки электронной подписи головного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи аккредитованного удостоверяющего центра, выдавшего сертификат отправителю;

- сертификата ключа проверки электронной подписи ДТС, выданного удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц;

- сертификата ключа проверки электронной подписи удостоверяющего

центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи ДТС;

- корневого сертификата ключа проверки электронной подписи головного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, выдавшего сертификат ДТС;

- сертификата ключа проверки электронной подписи TSP-компонента, выданного удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, и используемого для подписания метки доверенного времени ДТС;

- сертификата ключа проверки электронной подписи, выданного аккредитованным удостоверяющим центром и используемого для подписания метки доверенного времени в отношении электронного документа отправителя;

- сертификата ключа проверки электронной подписи аккредитованного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи, используемого для подписания метки доверенного времени в отношении электронного документа отправителя.

2.3. Компонент проверки полномочий должен осуществлять проверку полномочий должностного лица – отправителя электронного документа, являющегося владельцем сертификата ключа проверки электронной подписи.

2.4. Компонент квитирования должен осуществлять формирование и подписание электронной подписью ДТС, основанной на сертификате ключа проверки электронной подписи, выданном ей удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, квитанции с

результатом проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания.

2.5. TSP-компонент должен осуществлять создание и проверку метки доверенного времени для сформированной и подписанной квитанции с результатом проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания.

2.6. Компонент документирования выполняемых средствами ДТС операций должен предусматривать хранение электронных документов, соответствующих выполненным ДТС операциям, в течение установленного времени. По истечении срока действия ключа проверки электронной подписи, которой подписаны указанные электронные документы, должны быть предусмотрены процедура переподписания этих электронных документов электронной подписью, основанной на очередном действующем сертификате ключа проверки электронной подписи, выданном ДТС удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, а также преемственность полномочий должностных лиц, наделенных правом производить переподписание таких электронных документов.

2.7. Компонент предоставления информации об операциях, выполненных средствами ДТС, должен осуществлять предоставление информации в соответствии с требованиями, установленными законодательством Российской Федерации, по запросам участников электронного взаимодействия.

3. Требования к программному обеспечению средств ДТС

3.1. Программное обеспечение (далее – ПО) средств ДТС не должно содержать средств, позволяющих модифицировать или искажать алгоритмы работы ПО средств ДТС.

3.2. ПО средств ДТС должно использовать только документированные

функции используемой операционной системы.

3.3. Системное ПО средств ДТС не должно содержать известных уязвимостей.

3.4. ПО средств ДТС должно обеспечивать разграничение доступа системного администратора, администратора аудита, администратора безопасности, администратора средств криптографической защиты информации (далее – СКЗИ), оператора и пользователей к информации, обрабатываемой в средствах ДТС, на основании правил разграничения доступа, заданных системным администратором.

3.5. Исходные тексты ПО средств ДТС должны пройти проверку на отсутствие недекларированных возможностей по требованиям, устанавливаемым в техническом задании на разработку (модернизацию) средств ДТС.

3.6. Системное ПО и исходные тексты прикладного ПО средств ДТС должны пройти проверку реализации в них методов и способов защиты информации, которые противостоят атакам, осуществляемым нарушителем из сетей общего пользования, являющимся квалифицированным групповым нарушителем, использующим возможности научных центров, анализирующих ПО с целью поиска уязвимостей.

3.7. В состав ПО средств ДТС должен входить механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения информации ограниченного доступа.

3.8. В ходе проведения тематических исследований должны быть проведены исследования, обосновывающие отсутствие в ПО программных механизмов (в том числе недекларированных возможностей и дефектов), способных привести к реализации угроз информационной безопасности.

4. Требования к аппаратным средствам средств ДТС

4.1. Исходный код BIOS должен пройти анализ на отсутствие известных уязвимостей и возможностей деструктивного воздействия, осуществляемого путем использования программных уязвимостей со

стороны каналов связи.

4.2. Должна проводиться проверка совместно с анализом исходного кода BIOS реализации целевых функций средств ДТС на основе системы тестов для аппаратных средств (далее – АС) средств ДТС, разрабатываемых специализированной организацией, проводящей их тематические исследования, и утверждаемых ФСБ России.

4.3. Должна проводиться оценка параметров надежности функционирования АС средств ДТС.

4.4. В случае планирования размещения средств ДТС в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения ограниченного доступа, АС средств ДТС иностранного производства должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации.

4.5. АС средств ДТС иностранного производства должны соответствовать требованиям по защите от утечки информации ограниченного доступа по каналам побочных электромагнитных излучений и наводок, установленным в техническом задании на разработку (модернизацию) средств ДТС.

4.6. Средства защиты средств ДТС должны исключить события, приводящие к возможности проведения успешных атак в условиях возможных неисправностей или сбоев АС средств ДТС или аппаратного компонента средства вычислительной техники, на котором реализованы средства ДТС.

5. Требования к ролевому разграничению

5.1. Средства ДТС должны поддерживать следующие обязательные роли:

5.1.1. Системного администратора с основными обязанностями инсталляции, конфигурации и поддержки функционирования средств ДТС, создания и поддержки профилей членов группы администраторов и пользователей средств ДТС.

5.1.2. Администратора безопасности.

5.1.3. Администратора СКЗИ с основными обязанностями, предусматривающими создание и проверку электронных подписей, которыми подписаны квитанции с результатами проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания.

5.1.4. Оператора с основными обязанностями по резервному копированию и восстановлению.

5.1.5. Администратора аудита с основными обязанностями, предусматривающими просмотр и поддержку журнала аудита в актуальном состоянии.

5.2. В средствах ДТС должен быть реализован механизм, исключающий возможность авторизации одного члена из группы администраторов средств ДТС для выполнения различных ролей.

6. Требования к целостности средств ДТС

6.1. В средствах ДТС должен быть реализован механизм контроля их целостности, а также определен период контроля целостности, который указывается в эксплуатационной документации на средства ДТС.

6.2. Контроль целостности должен осуществляться:

6.2.1. При каждой перезагрузке (до загрузки) операционной системы и периодически в ходе функционирования.

6.2.2. В автоматическом режиме в процессе функционирования средств ДТС (динамический контроль). Динамический контроль целостности должен выполняться не реже одного раза в сутки.

6.2.3. В ходе регламентных проверок средств ДТС (регламентный контроль).

Периодичность регламентного контроля целостности устанавливается в дополнении к техническому заданию на разработку (модернизацию) средств ДТС и должна быть указана в эксплуатационной документации.

6.3. Должны иметься средства восстановления целостности средств ДТС.

7. Требования к управлению доступом

7.1. В средствах ДТС должен обеспечиваться дискреционный принцип контроля доступа.

7.2. В средствах ДТС должно быть обеспечено создание программной среды, которая допускает существование в ней только фиксированного набора субъектов (программ, процессов) (замкнутая рабочая среда).

8. Требования к идентификации и аутентификации

8.1. Идентификация и аутентификация включают в себя распознавание пользователя средств ДТС, члена группы администраторов средств ДТС или процесса и проверку их подлинности. Механизм аутентификации должен блокировать доступ этих субъектов к функциям средств ДТС при отрицательном результате аутентификации.

8.2. В средствах ДТС для любой реализованной процедуры аутентификации должен быть применен механизм ограничения количества следующих подряд попыток аутентификации одного субъекта доступа, число которых не должно быть больше трех. При превышении числа следующих подряд попыток аутентификации одного субъекта доступа установленного предельного значения доступ этого субъекта доступа к средствам ДТС должен быть заблокирован на промежуток времени, который указывается в техническом задании на разработку (модернизацию) средств ДТС.

8.3. Для всех лиц, осуществляющих доступ к средствам ДТС, должна проводиться двухфакторная аутентификация.

8.4. Для всех пользователей средств ДТС должны использоваться механизмы удаленной аутентификации с использованием сертификатов на основе криптографических средств, имеющих действующее подтверждение соответствия требованиям ФСБ России по классу КС3.

8.5. При осуществлении локального доступа к средствам ДТС аутентификация членов группы администраторов должна выполняться до перехода в рабочее состояние средств ДТС (например, до загрузки используемой операционной системы).

8.6. При использовании для локальной аутентификации символьного периодически изменяющегося пароля он должен состоять не менее чем из 8 символов при мощности алфавита не менее тридцати шести символов. Период изменения пароля не должен быть больше трех месяцев.

9. Требования к защите данных

9.1. Средства ДТС должны обеспечивать передачу данных, содержащих информацию ограниченного доступа, способом, защищенным от несанкционированного доступа.

9.2. Должен быть реализован механизм защиты данных при передаче их между физически разделенными компонентами на основе криптографических средств, имеющих действующее подтверждение соответствия требованиям ФСБ России по классу КС3.

9.3. При организации сетевого взаимодействия компонентов средств ДТС между собой в случае их размещения в разных контролируемых зонах каналы связи (сети связи) между этими компонентами должны быть защищены с использованием СКЗИ класса не ниже КВ2 либо быть выделенными в соответствии с Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи»[1].

9.4. Средства ДТС должны принимать все входящие сообщения, только если они подписаны электронной подписью и проверка электронной подписи имеет положительный результат.

10. Требования к регистрации событий

10.1. Операционная система средств ДТС (средства защиты информации средств ДТС) должна поддерживать ведение защищенного журнала аудита системных событий и событий, связанных с выполнением средств ДТС своих функций. Требования к операционной системе (средствам защиты информации средств ДТС) и перечень регистрируемых событий

---

[1]Собрание законодательства Российской Федерации, 2003, № 28, ст. 2895; 2020, № 42 (ч. II), ст. 6525.

определяются и обосновываются в техническом задании на разработку (модернизацию) средств ДТС.

10.2. Журнал аудита должен быть доступен только администратору аудита, который может осуществлять только его просмотр, копирование и полную очистку. Полная очистка производится только после копирования всей информации, подлежащей очистке. После очистки первой записью в журнале аудита должен автоматически регистрироваться факт очистки с указанием даты, времени и информации о лице, производившем очистку.

11. Требования по надежности и устойчивости функционирования средств ДТС

11.1. Вероятность сбоев и неисправностей аппаратных средств ДТС, приводящих к невыполнению им своих функций, в течение суток не должна превышать аналогичной вероятности для используемых в составе средств ДТС шифровальных (криптографических) средств.

11.2. Должно осуществляться тестирование устойчивости функционирования средств ДТС.

11.3. Время восстановления средств ДТС не должно превышать четырех часов.

11.4. Меры и средства повышения надежности и устойчивости функционирования средств ДТС должны содержать механизмы квотирования ресурсов средств ДТС.

12. Требования к ключевой информации

12.1. Порядок создания, использования, хранения и уничтожения ключевой информации, в том числе сроки ее действия, определяются в соответствии с требованиями эксплуатационной документации на средства электронной подписи и иные криптографические средства, используемые средствами ДТС.

12.2. Копирование ключевых документов должно осуществляться только в соответствии с эксплуатационной документацией на используемые криптографические средства. Не допускается копирование информации

ключевых документов (криптографических ключей, в том числе ключей электронной подписи) на носители (например, жесткий диск), не являющиеся специализированными ключевыми носителями, без ее предварительного шифрования (которое должно осуществляться встроенной функцией используемого криптографического средства).

12.3. Ключи электронной подписи, используемые для подписания квитанций, создаваемых ДТС, должны создаваться, храниться, использоваться и уничтожаться в программно-аппаратном криптографическом модуле (HSM), имеющем действующее подтверждение соответствия требованиям ФСБ России по классу КВ.

13. Требования к резервному копированию

13.1. Средства ДТС должны реализовывать функции резервного копирования и восстановления.

13.2. Данные, сохраненные при резервном копировании, должны быть достаточны для восстановления функционирования средств ДТС в состояние, зафиксированное на момент копирования.

13.3. Должны быть приняты меры по обнаружению несанкционированных изменений сохраненных данных.

14. Требования к анализу (разбору) сертификата ключа проверки электронной подписи

14.1. В средствах ДТС должен быть реализован механизм контроля соответствия сертификатов ключей проверки электронной подписи требованиям законодательства Российской Федерации.

14.2. Должны анализироваться расширения сертификата ключа проверки электронной подписи, содержащие наименования средств электронной подписи и средств удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, этого сертификата, наименование средства электронной подписи, используемого владельцем сертификата, а также реквизиты документов, подтверждающих соответствие указанных средств

приказу ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»[1] (далее – приказ ФСБ России № 796).

14.3. Целью анализа указанных расширений является установление фактов использования удостоверяющим центром для создания ключа электронной подписи ключа проверки электронной подписи и подлежащего проверке сертификата, а также использования пользователем для создания подлежащей проверке электронной подписи только средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия установленным требованиям.

14.4. Анализ проводится с учетом информационных ресурсов Российской Федерации, содержащих необходимую информацию о подтверждении соответствия средств электронной подписи и средств удостоверяющего центра приказу ФСБ России № 796.

14.5. Должны также анализироваться расширения сертификата ключа проверки электронной подписи, содержащие сведения о классе средств удостоверяющего центра, с использованием которых он был создан, и сведения о классе средства электронной подписи владельца сертификата ключа проверки электронной подписи на соответствие политике безопасности, установленной и опубликованной ДТС.

14.6. Все расширения сертификата ключа проверки электронной подписи и списка прекративших действие и аннулированных сертификатов должны анализироваться на соответствие требованиям, установленным Законом «Об электронной подписи» и иными принятыми в соответствии с ним нормативными правовыми актами Российской Федерации.

14.7. Анализ проводится во взаимодействии с информационными ресурсами Российской Федерации, содержащими необходимую информацию, в целях установления взаимного соответствия сведений о владельце сертификата ключа проверки электронной подписи, обязанных содержаться в сертификате согласно части 2 статьи 17 Закона «Об электронной подписи».

---

[1]Зарегистрирован Минюстом России 9 февраля 2012 г., регистрационный № 23191.

14.8. Конкретный механизм реализации контроля соответствия сертификатов ключей проверки электронной подписи требованиям законодательства Российской Федерации определяется и обосновывается в техническом задании на разработку (модернизацию) средств ДТС.

15. Требования к СКЗИ

15.1. Средства ДТС должны использовать средства электронной подписи, имеющие действующие подтверждения соответствия требованиям ФСБ России по классу не ниже чем КС3.

15.2. Ключи электронной подписи, используемые для подписания квитанций, создаваемых ДТС, должны создаваться, храниться, использоваться и уничтожаться в программно-аппаратном криптографическом модуле (HSM), имеющем действующее подтверждение соответствия требованиям ФСБ России по классу КВ.

15.3. Иные СКЗИ, используемые средствами ДТС, должны иметь действующие подтверждения соответствия требованиям ФСБ России по классу не ниже, чем КС3.

16. Требование к криптографическим стандартам

16.1. В средствах электронной подписи и иных криптографических средствах ДТС могут использоваться только криптографические алгоритмы, соответствующие требованиям, установленным положениями ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»[1], ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»[2], ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»[3].

---

[1]Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст (опубликован М.: Стандартинформ, 2013).

[2]Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 216-ст (опубликован М.: Стандартинформ, 2013).

[3]Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г. № 749-ст (опубликован М.: Стандартинформ, 2016).