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).

17. Требования к проверке сертификата ключа проверки электронной подписи

17.1. При проверке квалифицированной электронной подписи в электронном документе и подписании квитанции с результатом такой проверки средства ДТС проверяют действительность каждого следующего сертификата, в том числе действительность электронной подписи, которыми подписаны эти сертификаты:

17.1.1. 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.

17.1.2. 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.

17.1.3. Корневого сертификата ключа проверки электронной подписи головного удостоверяющего центра, на котором основана электронная подпись, которой подписан сертификат ключа проверки электронной подписи 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.

17.1.4. 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.

17.1.5. 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.

17.1.6. 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.

17.1.7. 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, на момент подписания метки доверенного времени.

17.1.8. 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.

17.1.9. 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 дату 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.

Каждый из перечисленных сертификатов подлежит анализу (разбору) в соответствии с разделом 13 настоящих Требований.

17.2. Проверка электронной подписи в сертификате ключа проверки электронной подписи осуществляется в соответствии с положениями статьи 11 Закона «Об электронной подписи» и ГОСТ Р ИСО/МЭК 9594-8-98 «Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации»[1], включая проверку всех расширений, обязательных в соответствии с приказом ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»[2], и установленными политиками безопасности.

---

[1] Принят и введен в действие постановлением Госстандарта России от 19 мая 1998 г. № 215 (опубликован ИПК «Издательство стандартов», 1998, ИУС 9-98).

[2] Зарегистрирован Минюстом России 27 января 2012 г., регистрационный № 23041.

18. Дополнительные требования

18.1. Для ограничения возможностей по построению атак на средства ДТС с использованием каналов связи должны применяться средства межсетевого экранирования, применяемые северами, обслуживающими сайты, веб-службы и веб-приложения. Средства межсетевого экранирования должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера. Должны применяться средства межсетевого экранирования уровня веб-сервера (тип «Г»), сертифицированные ФСБ России на соответствие требованиям к устройствам типа межсетевой экран не менее чем 3 класса защищенности.

18.2. Для обеспечения обнаружения компьютерных программ или иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также для реагирования на обнаружение этих программ и информации должны применяться средства защиты от компьютерных вирусов, предназначенные для применения на серверах информационных систем (тип «Б») и сертифицированные ФСБ России на соответствие требованиям к антивирусным средствам по классу Б2.

18.3. Для обеспечения обнаружения действий, направленных на несанкционированный доступ к информации, специальных воздействий на средства ДТС в целях добывания, уничтожения, искажения и блокирования доступа к защищаемой информации, а также для реагирования на эти действия (предотвращение этих действий) должны применяться средства защиты от компьютерных атак, сертифицированные ФСБ России на соответствие требованиям к программным, программно-аппаратным или аппаратным средствам типа «системы обнаружения компьютерных атак» по классу Б.

18.4. Для контроля локального доступа и контроля целостности программной среды средств вычислительной техники, входящих в состав средств ДТС, должны использоваться аппаратно-программные модули

доверенной загрузки уровня платы расширения, сертифицированные ФСБ России на соответствие требованиям к аппаратно-доверенным модулям доверенной загрузки электронно-вычислительных машин по классу 2Б.

18.5. Необходимость соответствия средств ДТС настоящим Требованиям должна быть указана в техническом задании на разработку (модернизацию) средств ДТС.

18.6. Исследования средств ДТС с целью подтверждения его соответствия настоящим Требованиям должны проводиться с использованием определяемых ФСБ России числовых значений параметров и характеристик механизмов защиты, реализуемых в средствах ДТС.

II. Требования к используемым ДТС средствам электронной подписи

1. Общие требования

1.1. Настоящие Требования устанавливают требования к средству электронной подписи, предназначенному для использования ДТС.

1.2. Средства электронной подписи должны обеспечивать возможность их функционирования в двух режимах: создания электронной подписи и ее автоматической проверки.

В указанных режимах средства электронной подписи под руководством администратора должны:

а) при создании электронной подписи:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

- создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

- однозначно показывать, что электронная подпись создана;

б) при автоматической проверке электронной подписи:

- показывать содержание электронного документа, подписанного электронной подписью;

- показывать информацию о внесении изменений в подписанный

электронной подписью электронный документ;

- указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

2. Требования к программному обеспечению средства электронной подписи

2.1. ПО средства электронной подписи не должно содержать средств, позволяющих модифицировать или искажать алгоритмы работы ПО.

2.2. ПО средства электронной подписи должно использовать только документированные функции операционной системы.

2.3. Системное ПО, используемое средством электронной подписи, не должно содержать известных уязвимостей.

2.4. Исходные тексты ПО средства электронной подписи должны пройти проверку на отсутствие недекларированных возможностей. ПО средства электронной подписи должно соответствовать уровню контроля отсутствия недекларированных возможностей, установленному в техническом задании на разработку (модернизацию) средства электронной подписи.

2.5. В состав ПО средства электронной подписи должен входить механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения информации ограниченного доступа, при освобождении (перераспределении) памяти путем записи маскирующей информации (случайной или псевдослучайной последовательности символов) в память.

2.6. В состав ПО средства электронной подписи должны входить компоненты, обеспечивающие экстренное стирание информации ограниченного доступа. Перечень такой информации и требования к реализации и надежности стирания задаются в техническом задании на разработку (модернизацию) средства электронной подписи.

2.7. Исходные тексты ПО средства электронной подписи 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 системное программное обеспечение с целью поиска уязвимостей.

2.8. Инженерно-криптографическая защита средства электронной подписи должна исключить события, приводящие к возможности проведения успешных атак в условиях возможных неисправностей или сбоев аппаратных средств средства электронной подписи или аппаратного компонента средства вычислительной техники, на котором реализовано средство электронной подписи.

3. Требования к аппаратным средствам средства электронной подписи

3.1. Должна проводиться проверка совместно с анализом исходного кода BIOS реализации целевых функций средства электронной подписи на основе установленных в соответствии с техническим заданием на разработку (модернизацию) средства электронной подписи тестов для АС средства электронной подписи.

3.2. Должна проводиться оценка параметров надежности функционирования АС средства электронной подписи.

3.3. АС средства электронной подписи должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации, а также исследованиям на соответствие требованиям по защите от утечки информации по каналам побочных электромагнитных излучений и наводок, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации.

3.4. Для создания и проверки электронной подписи средство электронной подписи должно использовать криптографический модуль, имеющий средства отображения результатов создания/проверки электронной подписи.

4. Требования к целостности

4.1. Средство электронной подписи должно содержать механизм контроля несанкционированного случайного и (или) преднамеренного искажения (изменения, модификации) и (или) разрушения информации, средства электронной подписи (далее – контроль целостности).

4.2. Контроль целостности средства электронной подписи должен выполняться при каждой перезагрузке операционной системы до ее загрузки, динамически при функционировании средства электронной подписи, а также в ходе регламентных проверок средства электронной подписи на местах эксплуатации (регламентный контроль).

Динамический контроль целостности должен выполняться не реже одного раза в сутки. Механизм регламентного контроля целостности должен входить в состав средства электронной подписи. Период регламентного контроля определяется и обосновывается в техническом задании на разработку (модернизацию) средства электронной подписи.

4.3. Должны иметься средства восстановления целостности средства электронной подписи.

5. Требование к управлению доступом

5.1. Реализация управления доступом субъектов к различным компонентам и (или) целевым функциям средства электронной подписи осуществляется средствами ДТС, в составе которых функционирует данное средство электронной подписи, в соответствии с требованиями к средствам ДТС.

6. Требования к идентификации и аутентификации

6.1. Идентификация и аутентификация включают в себя распознавание пользователя средством электронной подписи или процесса и проверку их подлинности. Механизм аутентификации должен блокировать доступ субъектов к функциям средства электронной подписи при отрицательном результате аутентификации.

6.2. В средстве электронной подписи 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 электронной подписи должен быть заблокирован на промежуток времени, который указывается в техническом задании на разработку (модернизацию) средства электронной подписи.

6.3. При доступе к средству электронной подписи должна проводиться двухфакторная аутентификация.

6.4. Допускается использование механизмов удаленной аутентификации с использованием сертификатов аутентификации на основе криптографических средств, разработанных в соответствии с требованиями Закона «Об электронной подписи».

6.5. При осуществлении локального доступа к средству электронной подписи аутентификация пользователя средства электронной подписи должна выполняться до перехода в рабочее состояние этого средства электронной подписи (например, до загрузки операционной системы, используемой этим средством).

6.6. 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.

7. Требования к регистрации событий

7.1. В состав средства электронной подписи должно входить средство, производящее регистрацию в защищенном электронном журнале событий, связанных с выполнением средством электронной подписи своих целевых функций. Требования к указанному средству и перечень регистрируемых событий определяются и обосновываются в техническом задании на разработку (модернизацию) средства электронной подписи.

7.2. Журнал регистрации событий должен быть доступен только лицам, определенным оператором информационной системы, в которой

используется средство электронной подписи. При этом доступ к журналу регистрации событий должен осуществляться только для просмотра записей и для перемещения содержимого журнала регистрации событий на архивные носители. Пользователю средства электронной подписи журнал должен быть доступен только для просмотра.

8. Требования по надежности и устойчивости функционирования средств электронной подписи

8.1. Должен быть проведен расчет вероятности сбоев и неисправностей АС средства электронной подписи, приводящих к невыполнению средством своих функций.

8.2. Средняя наработка АС средства электронной подписи на отказ - не менее 20000 ч.

9. Требования к датчику случайных чисел

9.1. Выработка ключей электронной подписи и создание электронной подписи должны производиться средством электронной подписи с использованием физического датчика случайных чисел, вырабатывающего случайную последовательность путем преобразования сигнала случайного процесса, генерируемого недетерминируемой физической системой, устойчивой по отношению к реально возможным изменениям внешних условий и своих параметров (далее – ФДСЧ), являющегося составной частью средства электронной подписи.

9.2. Для ФДСЧ, входящего в состав средства электронной подписи, должна быть разработана теоретико-вероятностная модель используемого в ФДСЧ случайного физического процесса, а также должна быть проведена экспериментальная проверка соответствия указанной модели реализации ФДСЧ. По параметрам теоретико-вероятностной модели должна быть теоретически обоснована оценка качества выходной последовательности ФДСЧ, а также проведена статистическая проверка полученной оценки для реализации ФДСЧ.

9.3. При эксплуатации средства электронной подписи должна

осуществляться проверка статистического качества выходной последовательности ФДСЧ. Данная проверка должна осуществляться:

- в ходе регламентных проверок ФДСЧ (регламентный контроль);

- в автоматическом режиме в процессе функционирования средства электронной подписи (динамический контроль).

Период регламентного контроля, а также способ проверки статистического качества выходной последовательности ФДСЧ в ходе регламентного и динамического контроля определяются и обосновываются в техническом задании на разработку (модернизацию) средства электронной подписи.

10. Требования к ключевой информации

10.1. Порядок создания, использования, хранения и уничтожения ключевой информации определяется в соответствии с требованиями эксплуатационной документации на средства электронной подписи.

10.2. Копирование ключевых документов должно осуществляться только в соответствии с эксплуатационной документацией на средство электронной подписи. Не допускается копирование ключей электронной подписи на носители (например, жесткий диск), не являющиеся специализированными ключевыми носителями, без ее предварительного шифрования.

10.3. Криптографические протоколы, обеспечивающие операции с ключевой информацией средства электронной подписи, должны быть реализованы непосредственно в средстве электронной подписи.

10.4. Сроки действия ключей электронной подписи и ключей проверки электронной подписи, используемых средством электронной подписи, определяются в соответствии с эксплуатационной документацией на средство электронной подписи, но не должны быть более трех и семи лет соответственно.

10.5. В средстве электронной подписи должен быть реализован механизм контроля срока действия ключей электронной подписи. Механизм контроля срока действия указанных ключей должен позволять задавать срок

действия ключа электронной подписи и сигнализировать о завершении срока действия ключа электронной подписи в течение заданного интервала времени до завершения срока действия ключа электронной подписи, а также блокировать работу средства электронной подписи, срок действия ключа электронной подписи которых завершен. Интервал времени о сигнализации завершения срока действия ключа электронной подписи определяется в техническом задании на разработку (модернизацию) средства электронной подписи.

11. Требование к криптографическим стандартам

11.1. Средство электронной подписи должно реализовывать только криптографические алгоритмы, указанные в приказе ФСБ России № 796.

12. Требование к проверке сертификата ключа проверки электронной подписи

12.1. Проверка действительности сертификата ключа проверки электронной подписи осуществляется средствами ДТС, в составе которых функционирует данное средство электронной подписи, в соответствии с требованиями к средствам ДТС.

13. Дополнительное требование

13.1. Исследования средств электронной подписи с целью подтверждения их соответствия настоящим Требованиям должны проводиться с использованием числовых значений параметров и характеристик механизмов защиты, реализуемых в средствах электронной подписи.