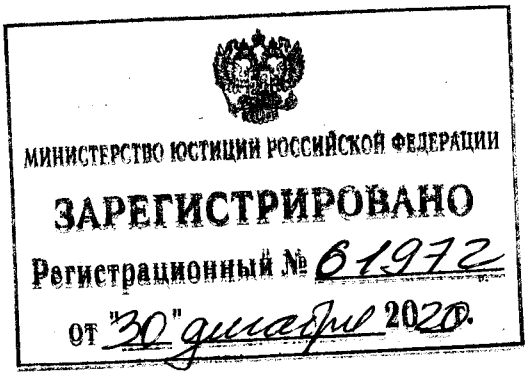
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

4 декабря 2020 года **Москва** № 555

О внесении изменений в приложения № 1 и 2 к приказу ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»



В соответствии с частью 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 «Вопросы Федеральной службы безопасности Российской Федерации»[2],

П Р И К А З Ы В А Ю:

внести в приложения № 1 и 2 к приказу ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной

[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.

подписи и Требований к средствам удостоверяющего центра»[1] изменения согласно приложению.

Директор А.Бортников

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

Приложение
к приказу ФСБ России
от 4 декабря 2020 г.
№ 555

Изменения,
вносимые в приложения № 1 и 2
к приказу ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»

1. В Требованиях к средствам электронной подписи (приложение № 1):

1.1. В подпункте 2 пункта 2 слова «или индивидуальный предприниматель» заменить словами «, индивидуальный предприниматель либо государственный орган или орган местного самоуправления».

1.2. В сноске 1 к пункту 20 слова «2004, № 28, ст. 2883; 2005, № 36, ст. 3665; № 49, ст. 5200; 2006, № 25, ст. 2699; № 31 (ч. I), ст. 3463; 2007, № 1 (ч. I), ст. 205; № 49, ст. 6133; № 53, ст. 6554; 2008, № 36, ст. 4087; № 43, ст. 4921; № 47, ст. 5431; 2010, № 17, ст. 2054; № 20, ст. 2435; 2011, № 2, ст. 267; № 9, ст. 1222» заменить словами «2018, № 28, ст. 4198».

2. В Требованиях к средствам удостоверяющего центра (приложение № 2):

2.1. В пункте 2:

2.1.1. В подпункте 2 слова «или индивидуальный предприниматель» заменить словами «, индивидуальный предприниматель либо государственный орган или орган местного самоуправления».

2.1.2. Подпункт 7 изложить в следующей редакции:

«7) квалифицированный сертификат ключа проверки ЭП (далее – квалифицированный сертификат) – сертификат ключа проверки ЭП, соответствующий требованиям, установленным Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми

актами, созданный аккредитованным УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП (далее – уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;».

2.1.3. Подпункт 9 изложить в следующей редакции:

«9) аккредитация УЦ – признание соответствия УЦ требованиям Федерального закона;».

2.1.4. В подпункте 11 после слова «организации,» дополнить словами «индивидуальные предприниматели,».

2.1.5. Дополнить подпунктом 12 следующего содержания:

«12) метка доверенного времени – достоверная информация в электронной форме о дате и времени подписания электронного документа электронной подписью, создаваемая и проверяемая доверенной третьей стороной, УЦ или оператором информационной системы и полученная в момент подписания электронного документа электронной подписью в установленном уполномоченным федеральным органом порядке с использованием программных и (или) аппаратных средств, прошедших процедуру подтверждения соответствия требованиям, установленным в соответствии с Федеральным законом[1].».

2.1.6. Подпункт 12 дополнить сноской 1 следующего содержания:

«[1] В соответствии с частью 1.1 статьи 3 Федерального закона от 27 декабря 2019 г. № 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (Собрание законодательства Российской Федерации, 2019, № 52 (ч. I) ст. 7794; 2020, № 26, ст. 3997) требования к службе меток доверенного времени применяются с 1 января 2021 г.».

2.2. Дополнить подпунктом 13.5 следующего содержания:

«13.5. Разработка и реализация с использованием аппаратных и программных средств атак, направленных на выявление и использование имеющихся уязвимостей АС УЦ.».

2.3. Подпункты 19.3 и 19.4 изложить в следующей редакции:

«19.3. Требования для средств УЦ классов КС2, КС3 и КВ1 совпадают с требованиями для средств УЦ класса КС1.

19.4. Требования для средств УЦ класса КВ2:

- в средствах УЦ должен быть реализован механизм контроля входящих информационных потоков в целях выявления наличия данных, активирующих недекларированные возможности АС;

- в составе средств УЦ для выполнения функций управления ключами ЭП должны использоваться отдельные СКЗИ на базе выделенных аппаратных платформ. Данные СКЗИ не должны эксплуатироваться совместно с другим программным обеспечением, не входящим в состав СКЗИ, в одной среде функционирования.».

2.4. Дополнить подпунктом 19.5 следующего содержания:

«19.5. Требования для средств УЦ класса КА1:

- проведение специальной проверки технических средств иностранного производства, входящих в состав АС УЦ, в целях выявления устройств, предназначенных для негласного получения информации;

- проведение исследования наличия недекларированных возможностей АС, внесенных на этапе разработки и изготовления электронной компонентной базы, а также на этапах разработки и производства средств вычислительной техники на ее основе;

- проведение полной верификации АС (совместно с анализом программного кода BIOS), на которых реализуются средства УЦ, с целью исключения недекларированных возможностей.».

2.5. Подпункт 20.4 дополнить абзацами следующего содержания:

«- должна быть исключена возможность хищения ключевой информации членом группы администраторов;

«- копирование ключевой информации СКЗИ должно быть реализовано в защищенном (зашифрованном) виде.».

2.6. В подпункте 21.2:

2.6.1. Абзац четвертый изложить в следующей редакции:

«- контроль целостности программных средств УЦ должен выполняться при каждом старте функционирования указанных средств, а контроль целостности АС УЦ – при каждой перезагрузке операционной системы (далее – ОС);».

2.6.2. Дополнить абзацем следующего содержания:

«- вероятность ошибки контроля целостности не должна превышать аналогичной вероятности для используемых СКЗИ.».

2.7. Подпункты 21.6 и 21.7 изложить в следующей редакции:

«21.6. Требования для средств УЦ класса КВ2:

- контроль целостности должен осуществляться динамически при функционировании средств УЦ.

21.7. Требования для средств УЦ класса КА1 совпадают с требованиями для средств УЦ класса КВ2.».

2.8. Абзац четвертый подпункта 23.4 дополнить словами «и с применением механизма многофакторной аутентификации, использующего аппаратные идентификаторы».

2.9. Подпункт 24.3 дополнить абзацами следующего содержания:

«- в средствах УЦ должен быть реализован механизм защиты от навязывания ложных сообщений на основе использования средств ЭП, получивших подтверждение соответствия требованиям к средствам ЭП, класс которых соответствует классу средств УЦ;

- в средствах УЦ должен быть реализован механизм защиты данных при передаче их между физически разделенными компонентами на основе использования СКЗИ, класс которых не ниже класса средств УЦ.».

2.10. Подпункт 24.4 изложить в следующей редакции:

«24.4. Требования для средств УЦ классов КС3, КВ1, КВ2 и КА1 совпадают с требованиями для средств УЦ класса КС2.».

2.11. Подпункты 24.5 и 24.6 признать утратившими силу.

2.12. Подпункт 25.2 дополнить абзацем следующего содержания:

«- список регистрируемых событий должен включать факты (попытки) изменения системного времени средств УЦ.».

2.13. В абзаце втором подпункта 25.4 слова «пользователями средств УЦ, не являющимися членами группы администраторов средств УЦ» исключить.

2.14. В абзаце третьем подпункта 27.3 после слов «(далее – список аннулированных сертификатов),» дополнить словами «а также ключи ЭП, используемые для подписи меток доверенного времени».

2.15. Абзац второй подпункта 27.6 изложить в следующей редакции:

«- ключи ЭП, используемые для подписи сертификатов ключей проверки ЭП, списков аннулированных сертификатов и меток доверенного времени, должны генерироваться, храниться, использоваться и уничтожаться в средстве ЭП;».

2.16. Подпункт 29.1 изложить в следующей редакции:

«29.1. Протоколы создания и аннулирования сертификатов ключей проверки ЭП, а также схема передачи заявления на создание сертификата ключа проверки ЭП должны быть описаны в эксплуатационной документации на средства УЦ.».

2.17. Дополнить новым пунктом 33 следующего содержания:

«33. В состав средств УЦ должна входить служба меток доверенного времени.».

2.18. Пункты 33 – 36 считать пунктами 34 – 37 соответственно.

2.19. Пункт 36 изложить в следующей редакции:

«36. При подключении средств УЦ, за исключением средств, реализующих механизм формирования меток доверенного времени, к информационно-телекоммуникационной сети, доступ к которой не

ограничен определенным кругом лиц, указанные средства должны соответствовать требованиям к средствам УЦ класса КВ2 или КА1.».

2.20. В сноске 1 к пункту 37 слова «2004, № 28, ст. 2883; 2005, № 36, ст. 3665; № 49, ст. 5200; 2006, № 25, ст. 2699; № 31 (ч. I), ст. 3463; 2007, № 1 (ч. I), ст. 205; № 49, ст. 6133; № 53, ст. 6554; 2008, № 36, ст. 4087; № 43, ст. 4921; № 47, ст. 5431; 2010, № 17, ст. 2054; № 20, ст. 2435; 2011, № 2, ст. 267; № 9, ст. 1222» заменить словами «2018, № 28, ст. 4198».

2.21. Дополнить пунктом 38 следующего содержания:

«38. Для ограничения возможностей по построению атак с использованием каналов связи на средства, реализующие механизм формирования меток доверенного времени, УЦ 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. Средства межсетевого экранирования должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста.

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 УЦ 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.

Для обеспечения обнаружения действий, направленных на несанкционированный доступ к информации, специальных воздействий на средства, реализующие механизмы формирования меток доверенного времени, в целях добывания, уничтожения, искажения и блокирования доступа к защищаемой информации, а также для реагирования на эти

действия (предотвращение этих действий) УЦ 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.

Для контроля локального доступа и контроля целостности программной среды средств вычислительной техники, входящих в состав средств, реализующих механизмы формирования меток доверенного времени, УЦ должны применяться аппаратно-программные модули доверенной загрузки уровня платы расширения, сертифицированные ФСБ России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки электронно-вычислительных машин по классу 2Б.

Класс СКЗИ средств, реализующих механизмы формирования меток доверенного времени, должен быть не ниже класса КС3. Должно быть обеспечено защищенное хранение криптографических ключей в неэкспортируемом виде.

Исходный код BIOS средств, реализующих механизмы формирования меток доверенного времени, должен пройти анализ на отсутствие известных уязвимостей и возможностей деструктивного воздействия, осуществляемого путем использования программных уязвимостей со стороны каналов связи.».