Р 50. . — 20

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ**

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 50.1. — 201

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

**Москва
Стандартинформ
2017**

Предисловие

1 РАЗРАБОТАНЫ Центром защиты информации и специальной связи Федеральной службы безопасности Российской Федерации (ФСБ России)

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от №

3 ВВЕДЕНЫ ВПЕРВЫЕ

Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Существующий в настоящее время в Российской Федерации порядок разработки шифровальных (криптографических) средств защиты информации, не содержащей сведений, составляющих государственную тайну (далее — СКЗИ), определяется «Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ – 2005) [1].

В соответствии с Положением ПКЗ – 2005 осуществляется взаимодействие между заказчиком СКЗИ, разработчиком СКЗИ, специализированной организацией, проводящей тематические исследования СКЗИ, и ФСБ России, осуществляющей экспертизу результатов тематических исследований, по результатам которой определяется возможность допуска СКЗИ к эксплуатации.

Настоящий документ носит методический характер и содержит в себе принципы, на которых должна основываться разработка и/или модернизация действующих СКЗИ.

Область применения документа — взаимодействие заказчиков и разработчиков СКЗИ при их общении:

- между собой;
- со специализированными организациями, проводящими тематические исследования;
- с ФСБ России, осуществляющей экспертизу результатов тематических исследований.

Заказчикам СКЗИ настоящий документ позволяет сориентироваться и ознакомиться с проблемами, возникающими при разработке и эксплуатации СКЗИ. Изложенные в настоящем документе принципы позволяют заказчику СКЗИ определиться с положениями, которые должны включаться в техническое задание на разработку и/или модернизацию СКЗИ, а также в соответствии с принятыми в Российской Федерации правилами классификации средств защиты определить класс разрабатываемого СКЗИ и обеспечить необходимый уровень безопасности защищаемой информации.

Разработчикам СКЗИ настоящий документ позволяет обосновать при общении с заказчиком перечень необходимых для разработки и/или модернизации СКЗИ работ, а также организовать взаимодействие со специализированными организациями, получая от них необходимую для разработки СКЗИ информацию.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Information technology
Cryptographic data security
Basic principles of creation and modernization for cryptographic modules

Дата введения — 20 — —

1 Область применения

Настоящие рекомендации распространяются на шифровальные (криптографические) средства защиты информации, предназначенные для использования на территории Российской Федерации.

Настоящие рекомендации определяют принципы разработки и модернизации шифровальных (криптографических) средств защиты информации, не содержащей сведений, составляющих государственную тайну.

Принципы обеспечения безопасности защищаемой информации до ее обработки в СКЗИ в настоящем документе не рассматриваются.

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации, перечисленных в пункте 4 Положения ПКЗ – 2005 [1], могут регулироваться отдельными рекомендациями по стандартизации.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты и рекомендации по стандартизации:

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 19.202 Единая система программной документации. Спецификация. Требования к содержанию и оформлению

ГОСТ 19.401 Единая система программной документации. Текст программы. Требования к содержанию и оформлению

ГОСТ 19.402 Единая система программной документации. Описание программы

ГОСТ 19.501 Единая система программной документации. Формуляр. Требования к содержанию и оформлению

Издание официальное

ГОСТ 19.502 Единая система программной документации. Описание применения. Требования к содержанию и оформлению

ГОСТ Р 50922 – 2006. Защита информации. Основные термины и определения

ГОСТ Р 51275 – 2006 Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 53114 – 2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р 56136 – 2014 Управление жизненным циклом продукции военного назначения. Термины и определения

Примечание – При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных документов в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящих рекомендациях применены следующие термины с соответствующими определениями:

3.1 **аппаратное средство;** АС: Физическое устройство, реализующее одну или несколько заданных функций. В рамках настоящего документа аппаратное средство подразделяется на АС СФ и АС СКЗИ.

3.2 **атака:** Целенаправленные действия с использованием аппаратных средств и/или программного обеспечения с целью нарушения безопасности защищаемой информации или с целью создания условий для этого.

3.3 **аутентификация субъекта доступа:** Совокупность действий, заключающаяся в проверке и подтверждении с использованием криптографических механизмов информации, позволяющей однозначно отличить аутентифицируемый (проверяемый) субъект доступа от других субъектов доступа.

3.4 **биологический датчик случайных чисел;** БДСЧ: Датчик, вырабатывающий случайную последовательность путем реализации случайных испытаний, основанных на случайном характере многократного взаимодействия человека с СКЗИ и средой функционирования СКЗИ.

3.5 **документация:** Совокупность взаимосвязанных документов, объединенных общей целевой направленностью. В рамках настоящего документа документация

подразделяется на документацию ИС, СФ, ПО СКЗИ и АС СКЗИ, а также на документацию СКЗИ, входящую в комплект поставки СКЗИ.

3.6 **жизненный цикл СКЗИ:** Совокупность явлений и процессов, повторяющаяся с периодичностью, определяемой временем существования типовой конструкции (образца) СКЗИ от ее замысла до утилизации или конкретного экземпляра СКЗИ от момента его производства до утилизации (ГОСТ Р 56136-2014, статья 3.16).

3.7

защищаемая информация: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

[ГОСТ Р 50922-2006, статья 2.5.2].

Примечание – Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

3.8 **защищенная информация:** Защищаемая информация, преобразованная СКЗИ при помощи одного или нескольких криптографических механизмов.

3.9 **имитация истинного сообщения (имитация):** Ложное сообщение, воспринимаемое пользователем как истинное сообщение.

3.10 **имитовставка:** Информация в электронной форме, которая присоединена к другой информации в электронной форме (обрабатываемой информации) или иным образом связана с такой информацией и которая используется для защиты обрабатываемой информации с использованием криптографических механизмов от навязывания ложной информации.

3.11 **имитозащита:** Защита обрабатываемой информации с использованием криптографических механизмов от навязывания ложной информации.

3.12 **инженерно-криптографический механизм:** Алгоритмическая или техническая мера, реализуемая в СКЗИ для защиты информации от атак, возникающих вследствие неисправностей или сбоев АС СКЗИ и АС СФ.

3.13 **инициализирующая последовательность (исходная ключевая информация):** Совокупность данных, используемая ПДСЧ для выработки псевдослучайной последовательности.

3.14 **информативный сигнал:** Сигнал, по значениям и/или параметрам которого может быть определена защищаемая или криптографически опасная информация (Рекомендации [2], статья 3.2.6).

3.15 **информационная система;** ИС: Система, предназначенная для представления, хранения, обработки, поиска, распространения и передачи по каналам связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. В случае использования СКЗИ для защиты обрабатываемой в ИС информации, информационная система представляет собой одну или совокупность нескольких сред функционирования СКЗИ.

3.16 **канал связи:** Совокупность технических средств, обеспечивающих передачу информации от источника к получателю. В совокупность технических средств могут

входить, в частности, передатчик, линия связи, носитель информации, приемник, аппаратные и/или программные средства.

Примечание – Примерами каналов связи могут служить: проводные, беспроводные, радио каналы, а также каналы, реализуемые с использованием отчуждаемых (съемных) носителей информации.

3.17 **ключ аутентификации:** Криптографический ключ, используемый для аутентификации субъекта доступа.

Примечание – В настоящем документе под ключами аутентификации подразумеваются пары – секретный и открытый ключ, используемые в асимметричных криптографических схемах и протоколах. В качестве ключей аутентификации могут выступать ключ электронной подписи и ключ проверки электронной подписи, открытый и секретный ключи участников протокола выработки общего ключа или асимметричной (гибридной) схемы шифрования. Также к ключам аутентификации относятся пароли.

3.18 **ключ проверки электронной подписи:** Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (Федеральный закон [3], статья 2, пункт 6).

3.19 **ключ электронной подписи:** Криптографический ключ, представляющий собой уникальную последовательность символов, предназначенную для создания электронной подписи (Федеральный закон [3], статья 2, пункт 5).

3.20 **ключевая информация:** Специальным образом организованная совокупность данных и/или криптографических ключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока времени.

3.21 **ключевой документ:** Ключевой носитель информации, содержащий в себе ключевую информацию и/или инициализирующую последовательность, а также при необходимости, контрольную, служебную и технологическую информацию.

3.22 **ключевой носитель:** Физический носитель определенной структуры, предназначенный для размещения и хранения на нем ключевой информации и/или инициализирующей последовательности. Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.).

3.23 **конструкторская документация:** Документация на СКЗИ, АС, СФ и ИС, содержащая детальную информацию о принципах функционирования и процессе разработки СКЗИ, АС, СФ и ИС.

3.24 **контролируемая зона:** Пространство, в пределах которого располагаются штатные средства и осуществляется контроль за пребыванием и действиями лиц и/или транспортных средств.

Примечание – Границей контролируемой зоны может быть, например, периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

3.25 **криптографическая функция:** Параметрическая функция, реализуемая СКЗИ и предназначенная для обеспечения безопасности защищаемой информации. Одним из параметров криптографической функции может являться криптографический ключ.

Примечание - В настоящем документе под криптографическими функциями, которые могут быть реализованы СКЗИ, следует понимать:

- функцию выработки псевдослучайных последовательностей;
- функцию зашифрования/расшифрования данных;
- функцию имитозащиты (функцию контроля целостности данных);
- функцию создания электронной подписи;
- функцию проверки электронной подписи;
- функцию создания ключа электронной подписи и ключа проверки электронной подписи;
- функцию изготовления ключевых документов;
- функцию передачи ключевой информации по каналам связи;
- функцию аутентификации.

3.26 **криптографически опасная информация:** Любая информация, хранимая и/или вырабатываемая на этапе эксплуатации СКЗИ, обладание которой нарушителем может привести к нарушению безопасности защищаемой и/или защищенной информации.

3.27 **ключ (криптографический ключ):** Изменяемый элемент (параметр), каждому значению которого однозначно соответствует одно из отображений (криптографических функций), реализуемых СКЗИ (Словарь [5], стр. 31).

Примечание – В настоящем документе криптографические ключи подразделяются на секретные ключи и открытые ключи.

3.28 **криптографический механизм:** Алгоритм, протокол или схема, в ходе выполнения которых происходит преобразование информации с использованием криптографического ключа (криптографическое преобразование).

3.29 **навязывание:** Атака, осуществляемая путем доведения до пользователя имитации истинного сообщения, полученной путем формирования ложного сообщения или модификации реально передаваемого или хранящегося сообщения.

3.30

недекларированные возможности (программного обеспечения): Функциональные возможности программного обеспечения, не описанные в документации.

[Рекомендации [4], статья 3.2.14]

Примечание – В настоящем документе под недекларированными возможностями следует понимать функциональные возможности программного обеспечения, а также аппаратных средств, эксплуатация которых может привести к нарушению безопасности защищаемой информации или к созданию условий для этого.

3.31

несанкционированный доступ к информации: Доступ к информации, осуществляемый с нарушением установленных прав и/или правил доступа к информации.

[Рекомендации [2], статья 3.2.10]

Примечания

1 Несанкционированный доступ может осуществляться юридическим лицом, физическим лицом, группой физических лиц, в том числе, общественной организацией.

2 В качестве информации, для которой не разрешен несанкционированный доступ, может выступать, в частности, защищаемая информация, ключевая информация, криптографически опасная информация.

3.32 **место эксплуатации СКЗИ:** Место расположения штатных средств, на котором происходит эксплуатация СКЗИ.

3.33

объект информатизации: Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены.

[ГОСТ Р 51275-2006, статья 3.1]

Примечание – В настоящем документе к объектам информатизации отнесены, в частности, ИС, СФ, СКЗИ, штатные средства, помещения, в которых размещены штатные средства, каналы связи.

3.34

организационные меры обеспечения информационной безопасности: Меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объектов информатизации.

[ГОСТ Р 53114-2008, статья 3.6.4].

3.35 **организационно-технические меры:** Совокупность действий, направленных на совместное применение организационных мер обеспечения информационной безопасности, технических и криптографических способов защиты информации, с использованием средств, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения информационной безопасности.

3.36 **открытый ключ:** Несекретный криптографический ключ, который однозначно связан с секретным ключом СКЗИ (Словарь [5], стр. 32).

Примечание – Примером открытого ключа служит ключ проверки электронной подписи.

3.37 **пароль:** Криптографический ключ, принимающий значения из множества малой мощности. Как правило, представляется в виде конечной последовательности символов из фиксированного алфавита и используется для аутентификации субъекта доступа к СКЗИ.

3.38 **программное обеспечение;** ПО: Совокупность данных и команд, представленная в виде исходного и/или исполняемого кода и предназначенная для функционирования на аппаратных средствах специального и общего назначения с целью получения определенного результата.

Примечание – В рамках настоящего документа программное обеспечение подразделяется на ПО СФ, ПО АС СФ, ПО СКЗИ и ПО АС СКЗИ.

3.39 **программный датчик случайных чисел;** ПДСЧ: Датчик, вырабатывающий псевдослучайную последовательность путем детерминированного преобразования инициализирующей последовательности (исходной ключевой информации).

3.40 **ролевая аутентификация субъектов доступа:** Аутентификация субъектов доступа, успешное завершение которой позволяет связать с субъектом доступа заранее определенную совокупность правил взаимодействия субъекта доступа с СКЗИ.

3.41 **секретный ключ:** Криптографический ключ, сохраняемый в секрете от лиц, не имеющих прав доступа к защищаемой информации, криптографическим ключам СКЗИ и/или к использованию криптографических функций СКЗИ (Словарь [5], стр. 32).

3.42 **специализированная организация:** Организация, имеющая право на осуществление отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами, и выполняющая тематические исследования (Положение ПКЗ-2005 [1], статья 2, пункт 32).

3.43 **среда функционирования СКЗИ;** СФ: Совокупность одного или нескольких аппаратных средств (АС СФ) и программного обеспечения (ПО), совместно с которыми штатно функционирует СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

Программное обеспечение среды функционирования подразделяется на

- программное обеспечение аппаратных средств среды функционирования (ПО АС СФ), представляющее собой программное обеспечение, функционирующее в рамках одного аппаратного средства и предназначенное для решения узкоспециализированного круга задач, например, BIOS, драйвер контроллера жесткого диска и т.п.;

- программное обеспечение среды функционирования (ПО СФ), которое подразделяется на:

1) операционную систему (ОС),

2) прикладное программное обеспечение (ППО), которое должно функционировать или функционирует в операционной системе.

Схематично, среда функционирования может быть представлена следующим образом (см. рисунок 1)

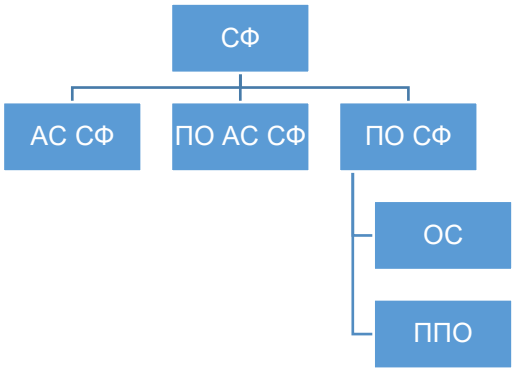

рисунок 1

3.44 **средство криптографической защиты информации;** СКЗИ: Шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну [6], и представляющее собой совокупность одной или нескольких составляющих:

- программного обеспечения (ПО СКЗИ);
- аппаратных средств (АС СКЗИ);
- программного обеспечения аппаратных средств (ПО АС СКЗИ).

Схематично, СКЗИ может быть представлено следующим образом (см. рисунок 2).

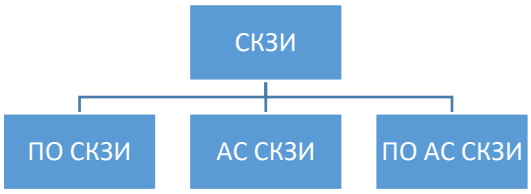

рисунок 2

3.45

субъект доступа: Лицо или процесс информационной системы, действия которого по доступу к ресурсам информационной системы регламентируются правилами разграничения доступа.

[Р 50.1.056-2005, статья 3.2.8]

Примечание – В качестве субъекта доступа к СКЗИ, в частности, может выступать физическое лицо, использующее криптографические функции СКЗИ для обеспечения безопасности защищаемой информации, или процесс информационной системы, взаимодействующий с СКЗИ.

3.46 **тактико-технические требования на ключевые документы;** ТТТ: Документ, определяющий криптографические, специальные и технические требования, которым должны удовлетворять ключевые документы (Положение ПКЗ-2005 [1], статья 2, пункт 28)/

Примечание – Тактико-технические требования разрабатываются разработчиком СКЗИ и утверждаются ФСБ России.

3.47 **тематические исследования:** Комплекс криптографических, инженерно криптографических и специальных исследований, направленных на оценку соответствия СКЗИ требованиям по безопасности информации, предъявляемых к СКЗИ (Положение ПКЗ-2005 [1], статья 2, пункт 31).

3.48 **технические характеристики СКЗИ:** Параметры программного обеспечения и аппаратных средств СКЗИ, а также методов обеспечения безопасности защищаемой информации и/или защищенной СКЗИ информации в процессе ее хранения или передачи по каналам связи, значения которых позволяют обеспечить необходимый уровень обеспечения безопасности.

Примечание – К техническим характеристикам СКЗИ могут быть отнесены, в частности, объем информации, зашифровываемый на одном секретном ключе, вероятности неисправностей или сбоев аппаратных средств СКЗИ и/или среды функционирования СКЗИ, параметры информативных сигналов.

3.49 **универсальное программное обеспечение;** УПО: Программное обеспечение общего применения пользователями, круг которых не определен. Универсальное программное обеспечение, разрабатывается без ориентации на какую-либо конкретную сферу деятельности и входит в состав ПО СФ.

3.50 **успешная атака:** Атака, достигшая своей цели.

3.51 **уязвимость:** Свойство АС и/или ПО, вытекающее, в частности, из ошибок реализации и/или существования недекларированных возможностей и позволяющее реализовывать успешные атаки на СКЗИ.

3.52 **физический датчик случайных чисел;** ФДСЧ: Датчик, вырабатывающий случайную последовательность путем преобразования сигнала случайного процесса, генерируемого недетерминированной физической системой, устойчивой по отношению к реально возможным изменениям внешних условий и своих параметров.

3.53 **штатные средства:** Совокупность АС и ПО, на которых реализованы ИС, СФ и СКЗИ.

3.54 **экспортируемая функция:** Реализованная в ПО СКЗИ и описанная в документации на ПО СКЗИ функция, которая предоставляется разработчикам, осуществляющим встраивание СКЗИ в ИС.

3.55 **электронная подпись;** ЭП: Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (Федеральный закон [3], статья 2, пункт 1).

Примечание – Видами электронных подписей являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

3.56 **этап жизненного цикла СКЗИ:** Часть жизненного цикла СКЗИ, выделяемая по признакам моментов контроля (контрольных рубежей), в которые предусматривается проверка характеристик проектных решений типовой конструкции

СКЗИ и/или физических характеристик экземпляров СКЗИ (ГОСТ Р 56136 – 2014, статья 3.18).

Примечание – В настоящем документе рассматриваются только следующие этапы жизненного цикла СКЗИ: разработка (модернизация), производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы) и эксплуатация СКЗИ.

4 Общие принципы построения СКЗИ

В настоящем разделе приводятся общие принципы, на которых основывается разработка новых или модификация действующих СКЗИ.

4.1 СКЗИ должно обеспечивать безопасность защищаемой информации при реализации атак в процессе обработки защищаемой информации в СКЗИ и/или при условии несанкционированного доступа к защищенной СКЗИ информации в процессе ее хранения или передачи по каналам связи.

4.2 СКЗИ должно реализовывать одну или несколько криптографических функций. В зависимости от реализуемых криптографических функции СКЗИ может быть отнесено к одному или нескольким средствам [1]:

а) средству шифрования;

б) средству имитозащиты;

в) средству электронной подписи;

г) средству кодирования;

д) средству изготовления ключевых документов;

е) ключевому документу.

4.3 В настоящем документе средства кодирования не рассматриваются.

4.4 Все СКЗИ подразделяются на 5 классов, упорядоченных по старшинству:

а) класс КС1 – младший по отношению к классам КС2, КС3, КВ и КА;

б) класс КС2 – младший по отношению к классам КС3, КВ, КА и старший по отношению к классу КС1;

в) класс КС3 – младший по отношению к классам КВ, КА и старший по отношению к классам КС1, КС2;

г) класс КВ – младший по отношению к классу КА и старший по отношению к классам КС1, КС2, КС3;

д) класс КА – старший по отношению к классам КС1, КС2, КС3, КВ.

4.5 Класс разрабатываемого (модернизируемого) СКЗИ определяется заказчиком СКЗИ путем формирования перечня подлежащих защите объектов ИС и совокупности возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак на указанные объекты, с учетом применяемых в ИС информационных технологий, среды функционирования и аппаратных средств.

4.6 Совокупность возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак, должна формироваться на основе приведенной в приложении А базовой совокупности и согласовываться с ФСБ России.

4.7 Класс разрабатываемого (модернизируемого) СКЗИ, совокупность возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак, и состав криптографических функций СКЗИ должны определяться в ТЗ на разработку (модернизацию) СКЗИ.

4.8 Разрабатываемые (модернизируемые) СКЗИ должны удовлетворять требованиям по безопасности информации, устанавливаемым в соответствии с законодательством Российской Федерации (Положение ПКЗ-2005 [1], статья 1, пункт 12). Совокупность предъявляемых к СКЗИ требований определяется:

а) классом СКЗИ;

б) составом криптографических функций, которые должны быть реализованы в СКЗИ.

4.9 В ТЗ на разработку (модернизацию) СКЗИ могут предъявляться дополнительные требования к СКЗИ, не противоречащие принципам настоящего документа.

4.10 Допускается проведение процедуры оценки соответствия СКЗИ произвольной совокупности из предъявленных к нему требований с выдачей заключения ФСБ России о соответствии (несоответствии) СКЗИ данной совокупности требований.

4.11 Сертификат соответствия СКЗИ выдается только в том случае, если для ввода СКЗИ в эксплуатацию не требуется проведение дополнительных тематических исследований СКЗИ после утверждения положительного заключения ФСБ России о соответствии СКЗИ всем предъявляемым к нему требованиям.

4.12 В отдельных случаях, при наличии соответствующего обоснования по решению ФСБ России может быть разрешена эксплуатация СКЗИ, когда отдельные положения требований по безопасности информации к ним не выполнены.

5 Принципы применения криптографических механизмов защиты

В настоящем разделе приводятся принципы применения криптографических механизмов защиты информации, датчиков случайных чисел, принципы выработки и использования ключевой информации, а также аутентификации субъектов доступа к СКЗИ.

5.1 Применение криптографических механизмов

Применение криптографических механизмов в СКЗИ основывается на следующих принципах:

5.1.1 При разработке (модернизации) СКЗИ должны использоваться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта, или криптографические механизмы, имеющие положительное заключение ФСБ России по результатам их экспертных криптографических исследований.

5.1.2 Значения параметров криптографических механизмов должны удовлетворять условиям, определяемым в рекомендациях по выбору параметров криптографических механизмов, утверждаемых ФСБ России.

5.1.3 Криптографические механизмы, а также преобразования, реализующие обработку ключевой информации, ее выработку и удаление, должны быть реализованы непосредственно в СКЗИ.

5.2 Применение датчиков случайных чисел

Применение датчиков случайных чисел в СКЗИ основывается на следующих принципах:

5.2.1 Датчик случайных чисел является составной частью СКЗИ и должен проходить тематические исследования совместно с СКЗИ, в котором он применяется.

5.2.2 Датчик случайных чисел должен использоваться для генерации случайных (псевдослучайных) последовательностей с целью выработки ключевой информации и/или другой случайной (псевдослучайной) информации, используемой в СКЗИ.

5.2.3 При использовании датчика случайных чисел для целей, отличных от выработки ключевой информации или инициализирующей последовательности ПДСЧ, требования к датчику случайных чисел должны предъявляться в ТЗ и обосновываться в ходе тематических исследований СКЗИ.

5.2.4 При выработке ключевой информации для всех классов СКЗИ допускается использование ФДСЧ и ПДСЧ.

5.2.5 ПДСЧ, входящий в состав СКЗИ, должен использовать для выработки ключевой информации из инициализирующей последовательности криптографический механизм, удовлетворяющий принципам 5.1.

5.2.6 При выработке инициализирующей последовательности для ПДСЧ допускается использовать:

а) ФДСЧ – для СКЗИ всех классов;

б) БДСЧ – для СКЗИ классов КС1, КС2 и КС3.

5.2.7 Инициализирующие последовательности для ПДСЧ могут вырабатываться:

а) ФСБ России – для СКЗИ всех классов;

б) организациями, имеющими лицензии ФСБ России на изготовление и распределение ключевых документов и/или исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов – для СКЗИ всех классов;

в) на местах эксплуатации СКЗИ – для СКЗИ классов КС1, КС2, КС3.

5.2.8 В случае выработки инициализирующей последовательности ПДСЧ на местах эксплуатации СКЗИ (см. 5.2.7, перечисление в), необходимо:

а) в ходе тематических исследований СКЗИ провести построение, обоснование и анализ теоретико-вероятностной модели датчика случайных чисел, формирующего инициализирующую последовательность;

б) обеспечить проверку статистического качества инициализирующей последовательности ПДСЧ, осуществляемую в автоматическом режиме функционирования СКЗИ (динамический контроль);

в) реализовать механизм периодической смены инициализирующей последовательности; указанный период должен определяться и обосновываться в ходе тематических исследований СКЗИ.

5.2.9 Для ФДСЧ, входящих в состав СКЗИ всех классов, в ходе тематических исследований должна быть разработана теоретико-вероятностная модель используемого в ФДСЧ случайного физического процесса, а также должна быть проведена экспериментальная проверка соответствия указанной модели реализации ФДСЧ.

5.2.10 Для ФДСЧ, входящих в состав СКЗИ класса КА, в ходе тематических исследований по параметрам теоретико-вероятностной модели должна быть теоретически обоснована оценка качества выходной последовательности ФДСЧ, а также проведена статистическая проверка полученной оценки для реализации ФДСЧ.

5.2.11 Для всех классов СКЗИ на местах эксплуатации СКЗИ должна осуществляться проверка статистического качества выходной последовательности ДСЧ. Данная проверка должна осуществляться:

а) в ходе регламентных проверок датчика случайных чисел (регламентный контроль) – для всех классов СКЗИ;

б) в автоматическом режиме в процессе функционирования СКЗИ (динамический контроль) – для классов КС3, КВ и КА.

5.2.12 Период регламентного контроля определяется и обосновывается в ходе тематических исследований СКЗИ.

5.2.13 Способ проверки статистического качества инициализирующей и выходной последовательностей ДСЧ в ходе регламентного и динамического контроля (см. 5.2.8, перечисление б, и 5.2.11) определяется и обосновывается в ходе тематических исследований СКЗИ.

5.3 Выработка ключевой информации

Выработка ключевой информации основывается на следующих принципах:

5.3.1 Выработка ключевой информации должна производиться СКЗИ, реализующим криптографическую функцию изготовления ключевых документов и/или функцию создания ключа электронной подписи и ключа проверки электронной подписи.

5.3.2 Для всех классов СКЗИ выработка ключей аутентификации, в частности, ключей электронной подписи, может производиться:

а) ФСБ России;

б) организациями, имеющими лицензии ФСБ России на изготовление и распределение ключевых документов и/или исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов;

в) на местах эксплуатации СКЗИ, с использованием датчика случайных чисел, удовлетворяющего 5.2.

5.3.3 Исходная ключевая информация, используемая СКЗИ для выработки ключевой информации, отличной от ключей аутентификации, может производиться:

а) ФСБ России – для СКЗИ всех классов;

б) организациями, имеющими лицензии ФСБ России на изготовление и распределение ключевых документов и/или исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов – для СКЗИ всех классов;

в) на местах эксплуатации СКЗИ, с использованием датчика случайных чисел, удовлетворяющего 5.2 – для СКЗИ классов КС1, КС2, КС3.

5.3.4 Для всех классов СКЗИ на местах эксплуатации СКЗИ допускается выработка ключевой информации с использованием протоколов выработки общего ключа, удовлетворяющих 5.1 и следующим дополнительным условиям:

а) обязательна аутентификация хотя бы одного субъекта, участвующего в протоколе выработки общего ключа;

б) СКЗИ класса КА должны использовать предварительно распределенный секретный ключ;

в) в протоколах выработки общего ключа должны использоваться датчики случайных чисел, удовлетворяющие 5.2.

5.3.5 Выработка ключевой информации, исходной ключевой информации и изготовление ключевых документов ФСБ России и организациями, имеющими лицензии ФСБ России на изготовление и распределение ключевых документов и/или исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов, производится по утвержденным ФСБ России тактико-техническим требованиям на ключевые документы.

5.4 Использование ключевой информации

Использование ключевой информации в СКЗИ основывается на следующих принципах:

5.4.1 Вся используемая СКЗИ ключевая информация должна быть выработана в соответствии с 5.3.

5.4.2 В случае, если ключевая информация выработана другим СКЗИ, то доведение ключевой информации до использующего ее СКЗИ должно осуществляться СКЗИ, реализующим криптографическую функцию передачи ключевой информации по каналам связи.

5.4.3 При передаче[1)] ключевой информации по каналам связи должны применяться криптографические механизмы, удовлетворяющие 5.1 и использующие криптографические ключи, выработанные:

а) либо ФСБ России;

[1)] Стоит отметить, что протоколы выработки общего ключа (см. п. 5.3.4) и протоколы передачи ключей имеют принципиальное различие. В первом случае по каналам связи передается вспомогательная информация, на основе которой СКЗИ вырабатывает общий секретный ключ. Во втором случае по каналам связи передается выработанный заранее секретный ключ.

б) либо организациями, имеющими лицензии ФСБ России на изготовление и распределение ключевых документов и/или исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов.

5.4.4 Возможность отказа от использования криптографических ключей, удовлетворяющих 5.4.3, при передаче ключевой информации по каналам связи должна быть обоснована в ходе проведения тематических исследований.

5.4.5 Используемая СКЗИ ключевая информация должна либо храниться непосредственно в СКЗИ на протяжении установленного срока действия, либо вводиться в СКЗИ с ключевого документа.

5.4.6 Перечень типов ключевых носителей, используемых СКЗИ, должен определяться в ТЗ.

5.4.7 Для различных криптографических механизмов необходимо использовать различную ключевую информацию. Использование одной и той же ключевой информации в различных криптографических механизмах должно быть обосновано в ходе тематических исследований.

5.4.8 Для обеспечения подлинности открытых ключей аутентификации должен использоваться механизм сертификатов открытых ключей:

а) в случае использования в СКЗИ открытых ключей аутентификации, область применения которых регулируется Федеральным законом [3], следует использовать механизм, удовлетворяющий требованиям к форме квалифицированного сертификата ключа проверки электронной подписи [7];

б) в остальных случаях механизм сертификатов открытых ключей должен определяться в ТЗ и обосновываться в ходе проведения тематических исследований.

5.4.9 Максимальные сроки действия криптографических ключей СКЗИ должны определяться в ТЗ и уточняться в ходе проведения тематических исследований.

5.4.10 В СКЗИ должен быть реализован механизм контроля срока действия криптографических ключей, основанный на следующих положениях:

а) для СКЗИ классов КС1 и КС2 требования к механизму контроля срока действия криптографических ключей определяются разработчиком СКЗИ и обосновываются в ходе тематических исследований;

б) в СКЗИ класса КС3 должен быть реализован механизм контроля срока действия криптографических ключей, позволяющий сигнализировать о завершении срока действия криптографических ключей в течение заданного интервала времени до завершения срока действия криптографических ключей;

в) в СКЗИ классов КВ и КА механизм контроля срока действия криптографических ключей должен удовлетворять 5.4.10, перечисление б, а также блокировать работу СКЗИ с криптографическими ключами срок действия которых завершен;

г) для СКЗИ классов КС3, КВ и КА интервал времени сигнализации о завершении срока действия криптографических ключей должен определяться в ТЗ.

5.5 Аутентификация субъектов доступа

Аутентификация субъектов доступа основывается на следующих принципах:

5.5.1 В СКЗИ всех классов должны быть реализованы криптографические механизмы, удовлетворяющие 5.1 и обеспечивающие аутентификацию субъектов доступа, осуществляющих доступ или взаимодействующих с СКЗИ.

5.5.2 Использование паролей для аутентификации субъектов доступа, являющихся физическими лицами и осуществляющих доступ к СКЗИ, допускается только для СКЗИ классов КС1 и КС2. Для СКЗИ классов КС3, КВ и КА необходимость использования паролей для аутентификации субъектов доступа должна быть обоснована заказчиком, а требования к паролям определены в ходе тематических исследований.

5.5.3 Для аутентификации субъектов доступа, являющихся физическими лицами и осуществляющих доступ к СКЗИ классов КС3, КВ и КА, рекомендуется использование ключей аутентификации, хранящихся в ключевых документах.

5.5.4 Для СКЗИ классов КС3, КВ и КА при аутентификации субъектов доступа, являющихся физическими лицами и осуществляющих доступ к СКЗИ, должна быть реализована ролевая аутентификация субъектов доступа. При этом требуется поддержка следующих ролей:

а) роль пользователя, в рамках которой выполняются реализованные в СКЗИ криптографические функции;

б) роль привилегированного пользователя, в рамках которой могут выполняться функции управления СКЗИ (настройка, конфигурирование и т.п.).

5.5.5 Для СКЗИ классов КС3, КВ и КА при аутентификации субъектов доступа являющихся процессами и осуществляющих взаимодействие с СКЗИ, должен быть реализован механизм, позволяющий ассоциировать аутентифицируемый процесс с физическим лицом, от имени которого он действует.

5.5.6 Требования к механизму, позволяющему ассоциировать аутентифицируемый процесс с лицом, от имени которого он действует, определяются разработчиком СКЗИ и обосновываются в ходе тематических исследований.

5.5.7 Для всех классов СКЗИ для любого реализованного механизма аутентификации субъектов доступа должен быть реализован механизм ограничения числа следующих подряд неудачных попыток аутентификации одного субъекта доступа.

5.5.8 При превышении числа следующих подряд неудачных попыток аутентификации одного субъекта доступа установленного предельно допустимого значения доступ этого субъекта доступа к СКЗИ следует блокировать на заданный промежуток времени.

5.5.9 Значение промежутка времени, в течение которого выполняется блокировка субъекта доступа, вызванная превышением числа следующих подряд неудачных попыток аутентификации, должно определяться и обосновываться в ходе тематических исследований СКЗИ.

5.5.10 Для СКЗИ класса КА для любого реализованного в СКЗИ механизма аутентификации субъектов доступа должны быть реализованы возможности установки предельно допустимого числа следующих подряд неудачных попыток аутентификации

одного субъекта доступа и установки времени блокировки доступа к СКЗИ на местах эксплуатации СКЗИ привилегированным пользователем.

5.5.11 Для СКЗИ всех классов рекомендуется устанавливать предельно допустимое число следующих подряд неудачных попыток аутентификации одного субъекта доступа в значение, не превышающее десяти.

5.6 Имитозащита

Реализация имитозащиты в СКЗИ должна основываться на следующих принципах:

5.6.1 Криптографические механизмы, обеспечивающие имитозащиту информации, должны удовлетворять требованиям 5.1.

5.6.2 Допускается использование усиленной электронной подписи для обеспечения имитозащиты передаваемых сообщений.

6 Принципы применения инженерно-криптографических механизмов защиты

6.1 Применение инженерно-криптографических механизмов

Использование инженерно-криптографических механизмов в СКЗИ основывается на следующих принципах:

6.1.1 Инженерно-криптографическая защита СКЗИ должна исключить опасные события, возникающие вследствие неисправностей или сбоев АС СКЗИ и АС СФ и приводящие к возможности осуществления успешных атак на СКЗИ.

6.1.2 Инженерно-криптографическая защита СКЗИ должна предусматривать защиту от возможных непреднамеренных действий пользователя, не предусмотренных правилами пользования СКЗИ и приводящих к возможности осуществления успешных атак на СКЗИ.

6.1.3 В качестве составной части СКЗИ всех классов должна быть реализована система защиты от несанкционированного доступа к используемой СКЗИ ключевой и криптографически опасной информации. Также в качестве составной части СКЗИ классов КС2, КС3, КВ и КА, должна быть реализована система защиты от несанкционированного доступа к защищаемой СКЗИ информации.

6.1.4 В ходе тематических исследований СКЗИ должны быть определены технические характеристики СКЗИ и их предельные значения, позволяющие обеспечить выполнение предъявляемых к СКЗИ требований.

6.1.5 В СКЗИ всех классов должен быть реализован контролирующий механизм, сигнализирующий или блокирующий работу СКЗИ при достижении предельных значений технических характеристик СКЗИ.

6.1.6 Для СКЗИ всех классов контролирующий механизм может допускать возможность санкционированной корректировки предельных значений технических характеристик СКЗИ:

а) для СКЗИ классов КС1 и КС2 регламент корректировки предельных значений технических характеристик СКЗИ следует определять в ТЗ и уточнять в ходе проведения тематических исследований;

б) для СКЗИ классов КС3, КВ и КА корректировку предельных значений следует производить привилегированным пользователем (см. п. 5.5.4, перечисление б).

6.1.7 В СКЗИ любого класса должна предусматриваться реализация блокирования работы СКЗИ:

а) блокировка СКЗИ должна осуществляться в случаях диагностики неисправности СКЗИ (см. 6.1.1), при достижении предельных значений технических характеристик СКЗИ (см. 6.1.5), при истечении срока действия ключей (для СКЗИ классов КВ и КА, см. 5.4.10, перечисление в), нарушении целостности ПО СКЗИ (см. 6.1.9, перечисление и);

б) при блокировке СКЗИ должна обеспечиваться невозможность выхода защищаемой и криптографически опасной информации в канал связи;

в) перечень случаев, когда блокировка СКЗИ является обязательной, уточняется в ходе проведения тематических исследований;

г) промежуток времени, в течение которого блокируется работа СКЗИ, определяется заказчиком СКЗИ и уточняется в ходе проведения тематических исследований.

6.1.8 В начале работы СКЗИ всех классов следует производить диагностический контроль работоспособности мер криптографической и инженерно-криптографической защиты.

6.1.9 Для СКЗИ всех классов должен быть обеспечен контроль целостности СКЗИ на этапах хранения, транспортирования, ввода в эксплуатацию и эксплуатации жизненного цикла СКЗИ, а также контроль целостности СФ на этапе эксплуатации жизненного цикла СКЗИ:

а) для СКЗИ классов КС1, КС2 и КС3 требования к механизму контроля целостности определяются в ТЗ и уточняются в ходе проведения тематических исследований;

б) для СКЗИ класса КС3 рекомендуется использование криптографических механизмов контроля целостности;

в) для СКЗИ классов КВ и КА контроль целостности должен осуществляться только с использованием криптографических механизмов;

г) для СКЗИ классов КВ и КА механизм контроля целостности должен включать средства контроля собственной корректной работы;

д) перечень объектов среды функционирования СКЗИ, контроль целостности которых осуществляется СКЗИ, определяется с учетом 6.4 и обосновывается в ходе проведения тематических исследований;

е) для СКЗИ всех классов контроль целостности следует проводить до начала обработки информации, безопасность которой должна обеспечиваться СКЗИ;

ж) для СКЗИ всех классов должен быть реализован периодический контроль целостности. Период контроля определяется и обосновывается в ходе тематических исследований СКЗИ;

з) для СКЗИ всех классов необходимо проводить контроль целостности в ходе регламентных проверок СКЗИ на местах эксплуатации;

и) в случае обнаружения нарушения целостности следует осуществлять блокировку СКЗИ.

6.1.10 В состав СКЗИ всех классов должен входить механизм, обеспечивающий контроль целостности ключевой и исходной ключевой информации.

6.1.11 В состав СКЗИ всех классов должны входить компоненты, обеспечивающие очистку областей памяти, используемых СКЗИ для хранения защищаемой, ключевой, исходной ключевой и криптографически опасной информации, при освобождении и/или перераспределении областей памяти, путем записи в области памяти случайной информации, вырабатываемой датчиком случайных чисел.

6.1.12 Для СКЗИ классов КВ и КА должен быть реализован механизм аварийного (экстренного) уничтожения ключевой и криптографически опасной информации. Механизм уничтожения, а также перечень ситуаций, в которых производят уничтожение ключевой и криптографически опасной информации, определяется заказчиком и уточняется в ходе тематических исследований СКЗИ.

6.1.13 Для СКЗИ классов КС1 и КС2 необходимость предъявления требований к регистрации событий и их содержание определяются в ТЗ.

6.1.14 В СКЗИ классов КС3, КВ и КА следует реализовывать следующий механизм регистрации событий:

а) в состав СКЗИ классов КС3, КВ и КА должен входить модуль, производящий регистрацию в электронном журнале регистрации событий в СКЗИ и СФ, связанных с выполнением СКЗИ определенных в ТЗ криптографических функций;

б) в перечень регистрируемых событий, в частности, должны входить:

- факты ввода, смены и стирания ключевой информации;

- факты срабатывания блокировки СКЗИ по причине исчерпывания ключевой информации;

- факты окончания срока действия криптографических ключей;

- факты повторного ввода ключей;

- факты отказа от ввода ключей в связи с нарушением требований, устанавливаемых ТТТ на ключевые документы;

- факты срабатывания системы защиты от несанкционированного доступа к информации;

- результаты контроля целостности ПО СКЗИ;

- факты проведения регламентных работ;

в) перечень событий, регистрируемых в журнале регистрации событий, может уточняться в ходе проведения тематических исследований;

г) журнал регистрации событий должен быть доступен только привилегированным пользователям СКЗИ, см. 5.5.4, перечисление б, и только для просмотра записей и перемещения содержимого журнала регистраций событий на архивные носители;

д) в случае невозможности переноса журнала регистрации событий в архив привилегированному пользователю может быть доступна функция стирания журнала. В этом случае СКЗИ должно обеспечивать сохранение информации о последних трех сутках работы СКЗИ, а также регистрацию факта очистки журнала с сохранением в нем даты очистки и информации о привилегированном пользователе, производившем операцию очистки.

6.1.15. В СКЗИ классов КС3, КВ и КА должен быть реализован контроль целостности журналов регистрации событий:

а) необходимость и порядок использования криптографических механизмов контроля целостности для СКЗИ класса КС3 определяются в ТЗ;

б) для СКЗИ классов КВ и КА контроль целостности должен осуществляться только с использованием криптографических механизмов.

6.2 Базовые положения для программного обеспечения СКЗИ

При разработке и встраивании ПО СКЗИ рекомендуется учитывать следующие положения:

6.2.1 Для проведения тематических исследований ПО СКЗИ для всех классов должно быть представлено в виде исходных текстов, исполняемого кода и документации.

6.2.2 Исходные тексты ПО СКЗИ должны удовлетворять следующим условиям:

а) исходные тексты ПО СКЗИ рекомендуется выполнять в соответствии с ГОСТ 19.401. При этом специализированная организация, проводящая тематические исследования, может устанавливать собственные требования к содержанию и оформлению текстов ПО СКЗИ;

б) исходные тексты ПО СКЗИ должны содержать комментарии, достаточные для понимания алгоритма функционирования ПО СКЗИ;

в) исходные тексты ПО СКЗИ должны содержать полный набор файлов, необходимый для воспроизведения из них исполняемого кода, идентичного представленному для проведения тематических исследований;

г) бинарные и ассемблерные вставки, вставки информационных массивов и входящие в состав исходных текстов фрагменты, не имеющие прямого отношения к реализации криптографических функций СКЗИ, должны быть документированы и обоснованы.

6.2.3 Документация на ПО СКЗИ должна включать в себя:

а) спецификацию ПО СКЗИ;

б) описание ПО СКЗИ;

в) описание применения ПО СКЗИ;

г) пояснительную записку.

6.2.4 Спецификация ПО СКЗИ (см. 6.2.3, перечисление а) должна быть выполнена в соответствии с ГОСТ 19.202.

6.2.5 Описание ПО СКЗИ (см. п. 6.2.3, перечисление б) должно быть выполнено в соответствии с ГОСТ 19.402 и содержать, в частности:

а) основные сведения о составе ПО СКЗИ (с указанием контрольных сумм файлов, входящих в состав ПО СКЗИ);

б) логическую структуру ПО СКЗИ;

в) описание ПО СФ СКЗИ;

г) описание методов, приемов и правил эксплуатации средств технологического оснащения, использованных при создании ПО СКЗИ;

д) инструкцию по сборке из исходных текстов ПО СКЗИ загрузочных и исполняемых модулей СКЗИ.

6.2.6. Описание применения ПО СКЗИ (см. п. 6.2.3, перечисление в) должно быть выполнено в соответствии с ГОСТ 19.502-78 и содержать:

а) сведения о назначении ПО СКЗИ;

б) сведения об области применения ПО СКЗИ;

в) сведения о классе решаемых ПО СКЗИ задач;

г) сведения об ограничениях при применении ПО СКЗИ;

д) сведения о минимальной конфигурации технических средств;

е) сведения о СФ;

ж) сведения о порядке работы СКЗИ.

6.2.7 Пояснительная записка (см. п. 6.2.3, перечисление г) должна содержать, в частности:

а) все сведения о назначении компонентов, входящих в состав ПО СКЗИ;

б) перечень всех реализованных в ПО СКЗИ функций;

в) сведения о параметрах (аргументах) реализованных в ПО СКЗИ функций;

г) сведения о формируемых кодах возврата реализованных в ПО СКЗИ функций;

д) перечень экспортируемых функций ПО СКЗИ;

е) описание используемых переменных;

ж) описание алгоритмов функционирования ПО СКЗИ;

з) описание критериев, методики и результатов тестирования реализованных в ПО СКЗИ функций.

6.2.8 Подача на вход любых значений параметров экспортируемых функций ПО СКЗИ не должна приводить к появлению уязвимостей, позволяющих реализовывать успешные атаки на СКЗИ.

6.2.9 В случае выявления при проведении тематических исследований значений параметров экспортируемых функций ПО СКЗИ, приводящих к появлению уязвимостей, позволяющих реализовывать успешные атаки на СКЗИ, составляется список таких функций и значений параметров. Этот список исключается из документации на СКЗИ (см. 6.5.4, перечисление е), представляемой разработчикам, осуществляющим встраивание СКЗИ в ИС. Действие сертификата соответствия СКЗИ на функции из указанного списка не распространяется.

6.3 Положения для аппаратных средств СКЗИ

Использование АС СКЗИ (если в СКЗИ входят АС СКЗИ) должно соответствовать следующим положениям:

6.3.1 В случае планирования размещения СКЗИ в помещениях, в которых присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и/или установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, АС СКЗИ иностранного производства должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации.

6.3.2 В случае планирования размещения СКЗИ в помещениях, в которых отсутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и не установлены АС и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну:

а) решение о проведении проверок АС СКЗИ иностранного производства, входящих в состав СКЗИ классов КС1, КС2, КС3 и КВ, принимается организацией, обеспечивающей эксплуатацию данных СКЗИ;

б) проверки АС СКЗИ иностранного производства, входящих в состав СКЗИ класса КА, проводятся в обязательном порядке.

6.4 Принципы взаимодействия со средой функционирования СКЗИ

Взаимодействие СКЗИ со средой функционирования основывается на следующих принципах:

6.4.1 Состав СФ определяется разработчиком СКЗИ, а правильность определения состава ПО СФ и АС СФ проверяется в ходе тематических исследований.

6.4.2 Для СКЗИ классов КС1, КС2 и КС3 допускается неполное определение состава СФ. В отношении части СФ, состав которой не определен, разработчиком СКЗИ, совместно с организацией, проводящей тематические исследования, должны быть сформулированы рекомендации, реализация которых необходима для выполнения предъявляемых к СКЗИ требований.

6.4.3 Для СКЗИ классов КВ и КА состав СФ должен быть определен полностью.

6.4.4 ПО СФ для СКЗИ всех классов:

а) должно обеспечивать работоспособность СКЗИ и корректное выполнение криптографических функций, реализуемых СКЗИ;

б) не должно оказывать влияния на результат выполнения криптографических функций, реализуемых СКЗИ;

в) не должно содержать возможностей, приводящих к построению атак, включая построение каналов обхода СКЗИ.

6.4.5 В состав ППО ПО СФ не должны входить средства анализа, разработки и отладки ПО. Включение данных средств в состав СФ должно быть обосновано в ходе тематических исследований СКЗИ.

6.4.6 УПО ПО СФ для СКЗИ классов КС2, КС3, КВ и КА должно иметь описание документированных возможностей. Перечень ПО СФ, относимого к УПО ПО СФ, определяется в ТЗ.

6.4.7 Для СКЗИ классов КВ и КА должны быть выполнены следующие требования:

а) ППО ПО СФ должно иметь исходные тексты;

б) перечень компонентов, входящих в состав ОС ПО СФ и для которых предоставляются исходные тексты, должен быть определен в ТЗ и обоснован в ходе тематических исследований СКЗИ;

в) должны быть реализованы и обоснованы в ходе тематических исследований СКЗИ меры по нейтрализации атак, использующих неопубликованные уязвимости ПО СФ. Меры по нейтрализации атак, использующих неопубликованные уязвимости ПО СФ, определяются в ТЗ и обосновываются в ходе тематических исследований СКЗИ.

6.5 Принципы разработки документации на СКЗИ

Документацию на СКЗИ следует разрабатывать на основании следующих принципов:

6.5.1 В состав документации на СКЗИ входят формуляр на СКЗИ, технические условия на СКЗИ (если в состав СКЗИ входят АС СКЗИ) и правила пользования СКЗИ.

6.5.2 Формуляр оформляют в соответствии с ГОСТ 19.501. Дополнительно в формуляре указывают:

а) назначение и область применения СКЗИ;

б) состав и назначение АС и ПО, обеспечивающих функционирование СКЗИ;

в) средства защиты информации, используемые совместно с СКЗИ и обеспечивающие безопасность защищаемой информации и безопасность использования СКЗИ.

6.5.3 Технические условия оформляют в соответствии с ГОСТ 2.114. В технических условиях дополнительно указывают меры противодействия атакам на СКЗИ на этапе производства.

6.5.4 В правилах пользования, в частности, указывают:

а) класс СКЗИ и реализуемые им криптографические функции;

б) вид и формат защищаемой и защищенной информации;

в) условия эксплуатации СКЗИ и ограничения на использование СКЗИ;

г) порядок учета СКЗИ;

д) инструкцию по вводу СКЗИ в эксплуатацию;

е) инструкцию по встраиванию СКЗИ в ИС (в случае, если такое встраивание предусмотрено ТЗ), содержащую перечень аргументов и возвращаемых значений функций, обеспечивающих возможность использования СКЗИ, с указанием допустимых значений этих параметров;

ж) порядок формирования (изготовления) и работы с ключевой информацией, а также меры защиты ключевой информации от несанкционированного доступа;

з) порядок и форму заказа ключевых документов (в случае их использования) в ФСБ России либо в организациях, имеющих лицензии ФСБ России на изготовление и распределение ключевых документов и/или исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов;

и) меры по обеспечению целостности СКЗИ, АС СФ и ПО СФ и документации на СКЗИ и на АС СФ и ПО СФ после завершения производства, хранения, транспортировки и ввода в эксплуатацию (пусконаладочных работ) СКЗИ и на этапе его эксплуатации;

к) инструкцию по восстановлению СКЗИ и СФ в случае нарушения целостности, а также порядок периодического контроля целостности эталонного ПО, используемого для восстановления СКЗИ и СФ;

л) меры по защите от атак на СФ и через нее на СКЗИ из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц (при необходимости);

м) меры по защите от несанкционированного доступа к информации в ИС, в которых используются СКЗИ, в том числе административный регламент и порядок проверки выполнения требований по защите от несанкционированного доступа к информации, СКЗИ и СФ;

н) порядок действий в нештатных ситуациях, связанных с использованием СКЗИ;

п) инструкцию по контролю технических характеристик СКЗИ при эксплуатации и хранении СКЗИ;

р) перечень ситуаций, в которых следует производить аварийное (экстренное) уничтожение ключевой и криптографически опасной информации,

с) порядок выполнения технического обслуживания, регламентных работ, ремонта, вывода из эксплуатации и утилизации СКЗИ;

т) организационные меры по обеспечению безопасности СКЗИ.

6.5.5. Оценка полноты и корректности сведений, изложенных в документации на СКЗИ, выполняется в ходе тематических исследований СКЗИ.

6.5.6. Формуляр на СКЗИ, технические условия на СКЗИ и правила пользования СКЗИ подлежат согласованию с ФСБ России.

Приложение А
(обязательное)

Базовая совокупность возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак

Настоящая совокупность возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак, сформирована с учетом возможностей, содержащихся в Приказе [8], а также в Приказе [9].

Каждая атака, проводимая с целью нарушения безопасности защищаемой информации или создания условий для этого, может быть задана следующими характеристиками:

а) объектом проведения атаки, безопасность которого должна обеспечиваться в течение определенного периода времени и/или определенного этапа жизненного цикла СКЗИ;

б) возможностями, которые могут быть использованы при создании способов, подготовке и проведении атак. Каждая возможность определяется:

– сведениями, а также

– техническими средствами, используемыми при создании способов, подготовке и проведении атак,

в) местом проведения атаки.

Для определения класса СКЗИ заказчик должен сформировать перечень подлежащих защите объектов ИС (см. А.1) и совокупность возможностей, состоящую из:

а) перечня сведений, которые могут быть использованы при проведении атак (на основе перечней из А.2);

б) перечня технических средств, которые могут быть использованы при проведении атак (на основе перечней А.3);

в) места проведения атак (на основе перечня из А.4).

В качестве класса СКЗИ заказчику СКЗИ следует выбирать младший класс, способный противостоять атакам на все указанные в сформированном заказчиком перечне объекты атак, с учетом ограничений, накладываемых на класс СКЗИ совокупностью возможностей, содержащейся в сформированных заказчиком перечнях сведений и технических средств, которые могут быть использованы при проведении атак.

А.1 Объекты атак

А.1.1 Класс СКЗИ определяется исходя из возможности СКЗИ противостоять атакам, для которых заказчиком определены подлежащие защите объекты атак.

А.1.2 СКЗИ всех классов должны противостоять атакам на следующие объекты:

а) защищаемую информацию с момента ее обработки в СКЗИ в течение периода времени, определяемого в ТЗ;

б) защищенную СКЗИ информацию в процессе ее передачи по каналам связи на этапе эксплуатации жизненного цикла СКЗИ и/или хранения в течение периода времени, определяемого в ТЗ;

в) ключевую, исходную ключевую и парольную информацию СКЗИ в течение периода времени, определяемого в ТЗ;

г) ЭП в течение периода времени, определяемого в ТЗ;

д) имитовставку в течение периода времени, определяемого в ТЗ;

е) криптографически опасную информацию на этапе эксплуатации жизненного цикла СКЗИ;

ж) СКЗИ на всех этапах жизненного цикла СКЗИ;

з) СФ на всех этапах жизненного цикла СКЗИ;

и) незащищенные данные, передаваемые по каналам связи, по которым передается защищенная СКЗИ информация, на этапе эксплуатации жизненного цикла СКЗИ;

к) документацию на СКЗИ, СФ и ИС на этапах разработки (модернизации), производства, хранения, транспортировки и ввода в эксплуатацию жизненного цикла СКЗИ;

л) иные объекты атак, которые при необходимости указываются в ТЗ на разработку (модернизацию) СКЗИ с учетом используемых в ИС информационных технологий, АС и ПО.

А.1.3 СКЗИ классов КС2, КС3, КВ и КА должны противостоять атакам на следующие объекты:

а) документацию на СКЗИ, СФ и ИС на этапе эксплуатации жизненного цикла СКЗИ.

б) объекты информатизации, в которых размещены штатные средства, на этапе эксплуатации жизненного цикла СКЗИ.

Примечание – Возможность СКЗИ противостоять атакам, на перечисленные в А.1 объекты атак, иллюстрируется таблицей 1, в которой знак «+» означает, что СКЗИ противостоит атакам на рассматриваемый в п. А.1 объект атаки, а знак «-» — не противостоит.

Подпункт	Класс				
	КС1	КС2	КС3	КВ	КА
А.1.2	+	+	+	+	+
А.1.3	-	+	+	+	+

таблица 1

А.2 Сведения, используемые при создании способов, подготовке и проведении атак

А.2.1 Класс СКЗИ определяется исходя из возможности СКЗИ противостоять атакам, использующим сведения о защищаемой информации.

А.2.2 СКЗИ всех классов должны противостоять атакам, использующим следующие сведения:

а) общие сведения об информации, используемой в процессе эксплуатации СКЗИ;

б) защищенную СКЗИ информацию;

в) все данные, передаваемые по каналам связи, не защищенным от несанкционированного доступа к информации организационно-техническими мерами.

А.2.3 СКЗИ всех классов должны противостоять атакам, использующим следующие сведения о СКЗИ:

а) содержание документации на СКЗИ (см. п. 6.5.1);

б) документированные и опубликованные возможности ПО СКЗИ, ПО АС СКЗИ и АС СКЗИ;

в) исходные коды ПО СКЗИ и ПО АС СКЗИ;

г) содержание конструкторской документации на СКЗИ;

д) сведения обо всех нарушениях правил пользования СКЗИ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами;

е) ведения обо всех неисправностях и сбоях АС СКЗИ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами.

А.2.4 Класс СКЗИ определяется исходя из возможности СКЗИ противостоять атакам, использующим сведения о СФ.

А.2.5 СКЗИ всех классов должны противостоять атакам, использующим следующие сведения:

а) содержание документации на СФ;

б) опубликованные возможности и уязвимости ПО СФ, ПО АС СФ и АС СФ;

в) сведения обо всех нарушениях правил эксплуатации СФ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами;

г) сведения обо всех неисправностях и сбоях АС СФ, проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами.

А.2.6 СКЗИ классов КВ и КА должны противостоять атакам, использующим сведения, содержащиеся в исходных текстах ПО СФ и ПО АС СФ.

А.2.7 СКЗИ класса КА должны противостоять атакам, использующим сведения, содержащиеся в конструкторской документации на АС СФ и ПО АС СФ.

Примечание – Возможность СКЗИ противостоять атакам, использующим сведения о СФ, перечисленные в А.2.5, А.2.6 и А.2.7, иллюстрируется таблицей 2, в которой знак «+» означает,

что СКЗИ противостоит атакам, использующим соответствующие сведения, а знак «-» — не противостоит.

Подпункт	Класс				
	КС1	КС2	КС3	КВ	КА
А.2.5	+	+	+	+	+
А.2.6	-	-	-	+	+
А.2.7	-	-	-	-	+

таблица 2

А.2.8 Класс СКЗИ определяется исходя из возможности СКЗИ противостоять атакам, использующим сведения об ИС.

А.2.9 СКЗИ всех классов должны противостоять атакам, использующим следующие сведения:

а) общие сведения об ИС, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы ИС;

б) Документированные и опубликованные сведения об информационных технологиях, базах данных, АС, ПО, используемых в ИС совместно с СКЗИ;

в) сведения о каналах связи.

А.2.10 СКЗИ классов КС3, КВ и КА должны противостоять атакам, использующим сведения обо всех сетях связи в составе ИС, работающих на едином криптографическом ключе.

А.2.11 СКЗИ классов КВ и КА должны противостоять атакам, использующим сведения, содержащиеся в конструкторской документации на информационные технологии, базы данных, ПО, используемые в ИС совместно с СКЗИ.

А.2.12 СКЗИ класса КА должны противостоять атакам, использующим сведения, содержащиеся в конструкторской документации на АС, используемые в ИС совместно с СКЗИ.

Примечание – Возможность СКЗИ противостоять атакам, использующим сведения о ИС, иллюстрируется таблицей 3, в которой знак «+» означает, что СКЗИ противостоит атакам, использующим соответствующие сведения, а знак «-» — не противостоит.

Подпункт	Класс				
	КС1	КС2	КС3	КВ	КА
А.2.9	+	+	+	+	+
А.2.10	-	-	+	+	+
А.2.11	-	-	-	+	+
А.2.12	-	-	-	-	+

таблица 3

А.2.13 СКЗИ классов КС2, КС3, КВ и КА должны противостоять атакам, использующим следующие сведения об организационных мерах:

а) сведения о физических мерах защиты объектов информатизации, в которых размещены штатные средства;

б) сведения о мерах по обеспечению контролируемой зоны объектов информатизации, в которых размещены штатные средства;

в) сведения о мерах по разграничению доступа на объекты информатизации, в которых размещены штатные средства.

А.2.14 Класс СКЗИ определяется исходя из возможности СКЗИ противостоять атакам, использующим сведения о недекларированных возможностях и уязвимостях.

А.2.15 СКЗИ всех классов должны противостоять атакам, использующим сведения об опубликованных методах использования уязвимостей ПО СФ и АС СФ.

А.2.16 СКЗИ классов КВ и КА должны противостоять атакам, использующим сведения о недекларированных возможностях ПО СФ и неопубликованных уязвимостях ПО СФ.

А.2.17 СКЗИ класса КА должны противостоять атакам, использующим сведения о недекларированных возможностях АС СФ, ПО АС СФ и неопубликованных уязвимостях АС СФ и ПО АС СФ.

Примечание – Возможность СКЗИ противостоять атакам, использующим сведения о недекларированных возможностях и уязвимостях, иллюстрируется таблицей 4, в которой знак «+» означает, что СКЗИ противостоит атакам, использующим соответствующие сведения, а знак «-» — не противостоит.

Подпункт	Класс				
	КС1	КС2	КС3	КВ	КА
А.2.15	+	+	+	+	+
А.2.16	-	-	-	+	+
А.2.17	-	-	-	-	+

таблица 4

А.3 Технические средства, используемые при создании способов, подготовке и проведении атак

А.3.1 Класс СКЗИ определяется исходя из возможности СКЗИ противостоять атакам, использующим технические средства.

А.3.2 СКЗИ всех классов должны противостоять атакам, использующим следующие средства:

а) штатные средства;

б) специально разработанные АС и ПО.

А.3.3 СКЗИ классов КВ и КА должны противостоять атакам, использующим следующие средства:

а) средства проведения лабораторных исследований штатных средств;

б) средства проведения исследований недекларированных возможностей и уязвимостей ПО.

А.3.4 СКЗИ класса КА должны противостоять атакам, использующим средства проведения исследований недекларированных возможностей и уязвимостей АС.

Примечание – Возможность СКЗИ противостоять атакам, использующим технические средства, иллюстрируется таблицей 5, в которой знак «+» означает, что СКЗИ противостоит атакам, использующим соответствующие средства, а знак «-» — не противостоит.

Подпункт	Класс				
	КС1	КС2	КС3	КВ	КА
А.3.2	+	+	+	+	+
А.3.3	-	-	-	+	+
А.3.4	-	-	-	-	+

таблица 5

А.3.5 СКЗИ должны противостоять атакам, использующим следующие технические каналы:

а) каналы связи – для СКЗИ всех классов;

б) иные каналы распространения информативных сигналов – для СКЗИ классов КВ и КА.

А.4 Место проведения атак

А.4.1 Класс СКЗИ определяется исходя из места проведения атаки.

А.4.2 СКЗИ всех классов должны противостоять атакам, проводящимся из-за пределов контролируемой зоны.

А.4.3 СКЗИ классов КС2, КС3, КВ и КА должны противостоять атакам, проводящимся из пределов контролируемой зоны.

Библиография

[1] Приказ ФСБ России от 09 февраля 2005 г. № 66 (в редакции приказа ФСБ России от 12 апреля 2010 г. № 173). Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ — 2005).

[2] Р 50.1.053 – 2005 Рекомендации по стандартизации. Информационная технология. Основные термины и определения в области технической защиты информации

[3] Федеральный закон Российской Федерации от 06 апреля 2011 г. № 63. Об электронной подписи.

[4] Р 50.1.056 – 2005 Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения

[5] Словарь криптографических терминов / Под. ред. Б.А. Погорелова и В.Н. Сачкова. — М.: МЦМНО, 2006. — 94 с.

[6] Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313. Об утверждении Положения о лицензировании деятельности по разработке, производству,

распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

[7] Приказ ФСБ России от 27 декабря 2011 г. № 795. Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи.

[8] Приказ ФСБ России от 27 декабря 2011 г. № 796. Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра.

[9] Приказ ФСБ России от 10 июля 2014 г. № 378. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности.

УДК 681.3.06:006.354 ОКС 35. 040

Ключевые слова: информационная технология, криптографическая защита информации, принципы разработки и модернизации, шифровальные (криптографические) средства защиты информации, СКЗИ

Руководитель организации-разработчика

наименование организации		
должность	личная подпись	инициалы, фамилия

Руководитель разработки	должность	личная подпись	инициалы, фамилия
Исполнитель	должность	личная подпись	инициалы, фамилия
Исполнитель	должность	личная подпись	инициалы, фамилия
Исполнитель	должность	личная подпись	инициалы, фамилия
Исполнитель	должность	личная подпись	инициалы, фамилия
Исполнитель	должность	личная подпись	инициалы, фамилия