Министерство образования Республики Беларусь
Белорусский государственный университет
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ПРИКЛАДНЫХ ПРОБЛЕМ МАТЕМАТИКИ И ИНФОРМАТИКИ

УТВЕРЖДАЮ
Директор НИИ прикладных проблем
математики и информатики

Ю.С.Харин
«___» _____ 2022 г.

МЕТОДИКА ИСПЫТАНИЙ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СТБ 34.101.27-2022

МИ.10127.10.01

Листов 88

Минск 2022

Содержание

1 Объект испытаний

Объектом испытаний является средство криптографической защиты информации (СКЗИ).

СКЗИ представляет собой набор аппаратных и (или) программных компонентов, который реализует один или несколько криптографических сервисов, а также дополнительные функции и механизмы, обеспечивающие безопасную работу сервисов: управления ключами, контроля доступа, проверки работоспособности, аудита и др.

В состав СКЗИ входят системные компоненты (например, микропроцессор) и собственные компоненты (например, встроенное программное обеспечение микропроцессора). Перечень компонентов определяет разработчик.

СКЗИ подразделяются на программные средства – выполненное целиком программно, без аппаратных компонентов, и аппаратные (программно-аппаратные, аппаратно-програмные) средства – выполненные в виде аппаратных устройств.

На испытания представляются:

1 Функциональная спецификация СКЗИ.

2 Программная документация СКЗИ.

3 Конструкторская документация (описание аппаратных компонентов) СКЗИ (только для аппаратных СКЗИ).

4 Документация по управлению жизненным циклом СКЗИ.

5 Исходные тексты всего программного обеспечения СКЗИ. Исходные тексты программ должны быть пригодны для компиляции и сборки в соответствующих средах разработки.

6 Опытный образец СКЗИ, пригодный для тестирования. В некоторых случаях для организации тестирования дополнительно должны предоставляться испытательные стенды.

2 Цель испытаний

Целью испытаний является проверка соответствия СКЗИ требованиям безопасности, определенным в СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности».

Требования безопасности группируются в пакеты. Пакет может быть обязательным или необязательным. Требования безопасности обязательных пакетов группируются в наборы, называемые уровнями безопасности. Определены 4 уровня безопасности: 1 (базовый), 2 (средний), 3 (высокий), 4 (максимальный). Каждый следующий уровень включает требования предыдущего и, таким образом, с увеличением уровня требования усиливаются.

СКЗИ определенного уровня должно удовлетворять всем требованиям этого уровня и может удовлетворять дополнительным требованиям. В частности, уровень может дополняться требованиями необязательных пакетов.

Разработчик СКЗИ должен заявить уровень безопасности СКЗИ, может быть, усиленный необязательными пакетами, требования безопасности для которого будут проверяться в ходе испытаний.

Далее СТБ 34.101.27-2022 называется Стандартом. В методике используются термины, обозначения и сокращения, определенные в Стандарте.

3 Требования к средству

К СКЗИ предъявляются функциональные (разделы 5, 6 Стандарта) и гарантийные (раздел 7 Стандарта) требования.

Функциональные требования направлены на решение задач безопасности, гарантийные требования поддерживают качество решения данных задач.

Функциональные требования обеспечивают противодействие угрозам безопасности, следование определенным правилам безопасности. Гарантийные требования обеспечивают доверие к тому, что СКЗИ корректно спроектировано и разработано, протестировано в достаточном объеме, правильно установлено и эксплуатируется.

4 Требования к документации

На испытания представляются программная документация, конструкторская документация (только для аппаратных СКЗИ), а также другие документы согласно группам требований ПР, ЖЦ, РД, ПИ Стандарта.

Функциональная спецификация описывает выбранные в СКЗИ методы реализации требований безопасности (проектные решения). Функциональная спецификация представляет собой отдельный документ либо разделы нескольких документов. Примерное содержание функциональной спецификации дано в Приложении А к Стандарту.

5 Средства и порядок испытаний

5.1 Порядок испытаний

В общем случае, при испытаниях эксперт использует следующие методы:

- проверка документации;
- анализ проектных решений;
- анализ исходных текстов программ;
- анализ аппаратной реализации;
- тестирование;
- проверка средств поддержки жизненного цикла.

Методы испытаний в конкретном случае выбираются в зависимости от объекта испытаний в соответствии с настоящими Методиками.

Проверка документации состоит в оценке полноты, обоснованности и непротиворечивости функциональной спецификации и другой документации СКЗИ.

Анализ проектных решений состоит в оценке качества проектирования тех или иных механизмов безопасности СКЗИ. При анализе принятых проектных решений используются обоснования разработчика, свидетельства из доступных информационных источников, результаты собственных исследований эксперта.

Анализ исходных текстов программ состоит в проверке соответствия программ и документации и в оценке отсутствия в программах недокументированных возможностей. Исходные тексты оцениваются частично, по выбору эксперта, но в соответствии с требованиями Стандарта. Анализ исходных текстов того или иного тематического блока может быть полным (проверяется весь код программ), подробным (не менее половины), выборочным (не менее 10%). Выбор программных модулей для анализа осуществляется при

разработке СКЗИ или в процессе испытаний. Полный анализ всех исходных текстов выполняется только для определенных программ, например, для программ, которые реализуют криптографические алгоритмы.

Анализ аппаратной реализации состоит в проверке соответствия аппаратной реализации и документации и в оценке отсутствия в аппаратной реализации недокументированных возможностей или уязвимостей. Аппаратная реализация оценивается частично, по выбору эксперта. Анализ всей аппаратной реализации выполняется только для определенных аппаратных компонентов, например, для компонентов, которые реализуют физическую безопасность СКЗИ, или компонентов, которые реализуют криптографические сервисы.

Тестирование состоит в проверке корректного выполнения штатных функций СКЗИ (функциональное тестирование) и в проверке сохранения безопасного состояния при нештатной работе с СКЗИ (тесты проникновения, стресс-тесты).

Проверка средств, развернутых разработчиком, касается средств поддержки жизненного цикла (в том числе средств разработки и сборки программ) и средств поставки СКЗИ конечному потребителю. Проверка состоит в оценке полноты средств, в проверке того, что они действительно применяются.

5.2 Процессы

Испытания состоят из процессов. Каждый процесс состоит в проверке определенной группы требований Стандарта. Всего имеется 20 групп требований и соответственно столько же процессов:

1) криптографическая поддержка (КП);
2) реализация сервисов (РС);
3) управление доступом (УД);
4) защита объектов (ЗО);
5) самотестирование (СТ);
6) аудит (АУ);
7) физическая безопасность (ФБ);
8) защита от воздействий (ЗВ);
9) защита от утечек (ЗУ);
10) генерация случайных чисел (СЧ);
11) обновление программ (ОП);
12) вывод из эксплуатации (ВЭ);
13) идентификация и аутентификация (ИА);
14) настройка среды (НС);
15) доверенный канал (ДК);
16) проектирование и разработка (ПР);
17) поддержка жизненного цикла (ЖЦ);
18) руководства (РД);
19) программа испытаний (ПИ);
20) анализ программ (АП).

Процессы КП – ВЭ состоят в проверке функциональных требований к СКЗИ. Процессы ИА – ДК состоят в проверке функциональных требований к системной среде СКЗИ. Процессы ПР – АП состоят в проверке гарантийных требований.

Эксперт, привлеченный к определенному процессу испытаний, должен выполнить его целиком. Допускается создание групп экспертов, которые выполняют процесс вместе. Выполнение частей процесса отдельными независимыми экспертами не допускается.

5.3 Проверки

Каждый процесс состоит из набора проверок. Проверка покрывает определенное требование к СКЗИ, заданное в Стандарте. Проверка обозначается так же, как и требование: процесс.номер_проверки (см. п. 4.4 Стандарта).

Описание каждой проверки состоит из следующих частей:

- проверяемое требование;
- выдержки из Стандарта с детализацией требования (при наличии выдержек);
- входные данные;
- действия эксперта.

В первой части цитируется проверяемое требование. При цитировании в круглых скобках указываются номера уровней безопаности СКЗИ, к которым требование относится. Примеры: (1), (2), (1–4), (3, 4).

Во второй части приводятся выдержки из Стандарта. Выдержки снабжаются заголовком «Стандарт [номер_раздела.номер_подраздела.номер]».

В части «Входные данные» описываются элементы функциональной спецификации, документы, тексты программ, компоненты СКЗИ, необходимые для выполнения проверки. Указывается максимальный набор входных данных — некоторые из них могут использоваться только при определенных условиях, например, при наличии определенных механизмов безопасности.

Названия элементов функциональной спецификации выделяются, например: криптографическая граница, список объектов (функциональные элементы), внешние интерфейсы, типичные ошибки операторов (гарантийные элементы) и т.д. Данные названия соответствуют Приложению А Стандарта.

Входные данные маркируются символами a, b, c, ... При описании действий эксперта ссылки на эти данные задаются как [a], [b], [c], ... Одни и те же входные данные могут использоваться сразу в нескольких проверках. Одинаковые входные данные определяют точки взаимодействия экспертов, выполняющих различные проверки.

Часть «Действия эксперта» содержит инструкции эксперту по применению тех или иных методов испытаний и, при необходимости, детализирует методы. Действия эксперта разбиваются на шаги, которые обозначаются следующим образом: проверка-номер_шага.

При описании действий эксперта используются ключевые слова ДОЛЖЕН и МОЖЕТ, которые определяют соответственно обязательный и рекомендуемый способы проведения испытаний.

При описании проверок используются примечания и примеры, которые разъясняют отдельные аспекты безопасности или действия эксперта в той или иной ситуации. Примечания и примеры являются необязательными элементами — даже без них суть проверок остается понятной.

5.4 Вердикты

По результатам выполнения каждой проверки эксперт выносит один из следующих вердиктов:

– положительно;
– проверка не проводилась;
– нет данных;
– отрицательно;
– требуются дополнительные исследования.

Допускается вводить дополнительные вердикты, уточняющие смысл перечисленных: «положительно при использовании надежных механизмов аппаратной защиты», «исходные тексты программ не представлены», «требуются дополнительные исследования источников случайности» и др.

Вердикт «положительно» означает, что проверяемое требование выполняется.

Вердикт «проверка не проводилась» выносится при выполнении одного из следующих условий:

– механизм безопасности, которого касается проверяемое требование, отсутствует в СКЗИ;

– проверяемое требование необязательно для заявленного разработчиком уровня безопасности СКЗИ;

– проверка проводится при определенном в Методике условии, которое для СКЗИ не выполняется.

В целом вердикт «проверка не проводилась» означает, что проверка не нужна.

Вердикт «нет данных» означает, что входные данные, необходимые для проведения проверки, представлены не в полном объеме.

Вердикт «отрицательно» означает, что проверяемое требование не выполняется.

Вердикт «требуются дополнительные исследования» означает, что для завершения проверки требуется провести дополнительные научно-технические исследования, требуется дополнительное специальное оборудование или программное обеспечение. Вердикт не означает, что эксперт не имеет достаточной квалификации или что разработчик нарушил некоторые требования. Вердикт означает, что при проведении проверки возникла необходимость проведения дополнительных объемных работ исследовательского характера.

При вынесении вердикта «требуются дополнительные исследования» испытания могут быть приостановлены по согласованию с разработчиком (заказчиком), вплоть до принятия решения о проведении дополнительных работ.

Вердикты по проверкам используются для вынесения вердикта по процессу. Процессу выносится вердикт «положительно», только если все проверки процесса завершены с вердиктами «положительно» или «проверка не проводилась».

Вердикты по процессам используются для вынесения вердикта по всем испытаниям. СКЗИ считается прошедшим испытания, только если все процессы завершены положительно.

5.5 Отчеты

По результатам испытаний эксперты составляют отчеты. Отчет может касаться отдельного процесса испытаний, нескольких процессов или всех испытаний в целом.

Отчет составляется в произвольной форме с соблюдением следующих правил:

1 Должен быть идентифицирован объект испытаний.
2 Должен быть указан уровень безопасности СКЗИ, заявленный разработчиком.
3 Должны быть перечислены выполненные проверки.

4 Должны быть указаны вердикты по отдельным шагам проверок, по проверкам в целом и по процессам в целом.

5 Должно быть дано обоснование вердикта по каждому шагу проверки.

Обоснование положительного вердикта может быть кратким. Тем не менее, эксперт должен стремиться представить в обосновании сведения, достаточные для повторения проверки другим экспертом или для локализации свидетельств, использованных при вынесении вердикта.

Обоснование отрицательного вердикта должно быть подробным. Эксперт должен представить в обосновании сведения, достаточные для того, чтобы разработчик смог локализовать найденные экспертом недостатки.

Рекомендуется оформлять результаты проверок в виде таблицы со столбцами: «шаг проверки», «вердикт», «обоснование».

6 Методы испытаний

6.1 Проверка требований по криптографической поддержке

Требование КП.1 (1–4). Должны быть определены и корректно реализованы {АП.2} криптографические алгоритмы СКЗИ. Каждый алгоритм должен быть однозначно идентифицирован: должен быть указан его тип, дана ссылка на спецификацию, определены режим работы, поддерживаемые длины ключей.

Примечание 1 — При реализации криптографического алгоритма разрешается сужать множество обрабатываемых объектов. Например, алгоритм шифрования может обрабатывать сообщения не любой, а только определенной длины. Вместе с тем сужение множества ключей не допускается.

Входные данные:

a) список криптографических алгоритмов;

b) уровень (1, 2, 3 или 4) безопасности СКЗИ;

c) исходные тексты программных реализаций криптографических алгоритмов;

d) компоненты СКЗИ, реализующие криптографические алгоритмы;

e) сертификаты, экспертные заключения, протоколы испытаний программных реализаций криптографических алгоритмов (при наличии);

f) перечень проверок самотестирования (часть, определяющая тесты для криптографических алгоритмов);

g) исходные тексты программ тестирования для криптографических алгоритмов;

h) компоненты СКЗИ, реализующие тестирование криптографических алгоритмов.

Действия эксперта:

КП.1-1. Эксперт проверяет, что каждый алгоритм из списка [a] однозначно идентифицирован. Это значит, что представлена, по крайней мере, следующая информация:

1 Тип алгоритма (например, алгоритм шифрования, протокол формирования общего ключа).

2 Ссылка на спецификацию (например, СТБ 34.101.31-2020, СТБ 34.101.45-2013).

3 Режим работы (например, шифрование в режиме простой замены, протокол без аутентификации сторон).

4 Поддерживаемые длины ключей (например, ключ СТБ 34.101.31 длины 128, уровень стойкости $l = 192$ СТБ 34.101.45).

Примечание — Если спецификация неявно определяет те или иные характеристики алгоритма или протокола, то эти характеристики могут опускаться. Например, в алгоритмах ГОСТ 28147-89 всегда используется 256-битовый ключ. Данные о длине такого ключа могут не приводиться.

КП.1-2. Эксперт проводит полный анализ исходных текстов [c] и проверяет, что все реализованные в программах СКЗИ криптографические алгоритмы включены в список [a].

КП.1-3. Для каждого криптографического алгоритма из списка [a] эксперт проверяет корректность его программной реализации.

Проверка корректности ДОЛЖНА проводиться по методике, специальной для целевого алгоритма. Данная методика ДОЛЖНА быть согласована с Органом по сертификации. ДОЛЖНА использоваться уже разработанная методика или, если такая методика отсутствует, ДОЛЖНА быть разработана новая методика.

В разрабатываемой методике ДОЛЖНЫ быть определены:

1 Методы анализа исходных текстов программной реализации [c]. Выбранные методы анализа ДОЛЖНЫ включать проверки, определенные в Приложении А. К анализу исходных текстов ДОЛЖНЫ привлекаться, по меньшей мере, два независимых эксперта.

2 Тесты для реализации [d]. Выбранный план тестирования МОЖЕТ соответствовать Приложению Б.

Проверка корректности МОЖЕТ не проводиться, если целевая программная реализация уже прошла испытания по методикам, удовлетворяющим упомянутым выше требованиям. В таких случаях эксперт может зачесть представленные свидетельства [e]. При этом эксперт ДОЛЖЕН предварительно проверить совпадение испытанных программных реализаций с представленными.

КП.1-4. Эксперт проверяет корректность тестов для криптографических алгоритмов из перечня [f]. Эксперт может использовать тестовые данные, заданные в [g].

Эксперт ДОЛЖЕН:

1 Проверить корректность данных, используемых в тестах. Эксперт ДОЛЖЕН провести сравнение тестовых данных с проверочными данными из технических нормативно-правовых актов (далее — ТНПА) или с данными, полученными с помощью независимой реализации.

2 Проверить, что вероятность успешного завершения теста при сбоях во время выполнения криптографических алгоритмов является незначительной. Пусть, например, тестируется алгоритм проверки ЭЦП. Тест состоит в проверке признания недействительной подписи недействительной. Такой тест, скорее всего, будет успешно завершаться как при корректном выполнении алгоритма проверки ЭЦП, так и при сбоях во время выполнения.

КП.1-5. Эксперт проводит выборочный (если уровень [b] равен 2) или подробный (если уровень [b] равен 3 или 4) анализ исходных текстов [g] и (или), соответственно, выборочное или подробное тестирование реализаций [h] и проверяет корректность программных реализаций тестов для криптографических алгоритмов.

Требование КП.2 (1–4). Спецификации криптографических алгоритмов [КП.1] должны быть приняты в качестве ТНПА.

Входные данные:

a) список криптографических алгоритмов.

Действия эксперта:

КП.2-1. Эксперт использует информационные системы учета ТНПА и проверяет, что спецификации всех алгоритмов из списка [a]:

1 Приняты в качестве ТНПА.

2 Актуальны (не отменены, не обновлены).

Требование КП.3 (1–4). Если в СКЗИ предусмотрена генерация долговременных параметров и ключей криптографического алгоритма [КП.1], то методы генерации должны быть определены и корректно реализованы {АП.2}. Методы генерации должны соответствовать спецификации алгоритма [КП.2], возможно уточняя или расширяя ее.

Примечание 2 — Методы генерации могут определяться в спецификации рамочно, без исчерпывающих деталей. Например, при генерации параметров ЭЦП на основе эллиптических кривых используются вспомогательные алгоритмы проверки простоты чисел, расчета порядка группы точек эллиптической кривой, которые могут быть не определены в спецификации. При реализации в СКЗИ методов генерации параметров проводится уточнение вспомогательных алгоритмов. Уточнения могут касаться также способов генерации случайных чисел, по которым строятся целевые долговременные параметры или ключи, или протоколов, с помощью которых ключи генерируются интерактивно.

Входные данные:

a) список криптографических алгоритмов;

b) методы генерации долговременных параметров и ключей;

c) исходные тексты программ генерации долговременных параметров и ключей;

d) компоненты СКЗИ, реализующие генерацию долговременных параметров и ключей;

e) протоколы испытаний программных реализаций стандартных методов генерации (при наличии).

Действия эксперта:

КП.3-1. Эксперт проверяет, что в список [b] включены все методы, необходимые для настройки и выполнения криптографических алгоритмов из списка [a].

Эксперт проводит классификацию методов из списка [b] и относит каждый метод к одному из 3 классов: стандартный метод, метод разработчика, внешняя генерация.

Примечание — Методы генерации разделяются на 3 класса:

1 *Стандартные методы*. Методы генерации определены в ТНПА в виде однозначных алгоритмов. Методы генерации могут определяться как непосредственно в ТНПА на соответствующие криптографические алгоритмы (например, генерация параметров p, q, a в СТБ 1176.2-99), так и в сопровождающих ТНПА, целиком посвященным генерации параметров. Несмотря на то, что алгоритмы генерации должны быть определены однозначно, они могут быть вероятностными, т.е. включать обращения к генераторам случайных чисел.

2 *Методы разработчика*. Методы генерации определены в документации разработчика в виде однозначных алгоритмов.

3 *Внешняя генерация*. Долговременные параметры генерируются вне СКЗИ и задаются в его программах или конфигурационных файлах. При внешней генерации долговременные пара-

метры должны быть определены в некотором ТНПА либо сгенерированы по определенным правилам самим разработчиком или другой организацией. В последнем случае разработчик описывает критерии, которые использовались при генерации, и дает обоснование этих критериев. Сами программы генерации могут не предоставляться.

Эксперт ДОЛЖЕН вынести отрицательный вердикт, если метод генерации не относится к одному из этих классов или генерация осуществляется в СКЗИ и не удовлетворяет требованиям соответствующего класса. Например, эксперт ДОЛЖЕН вынести отрицательный вердикт, если алгоритм генерации реализован в СКЗИ и не описан ни в ТНПА, ни в документации разработчика.

КП.3-2. Эксперт проводит полный анализ исходных текстов [c] и проверяет, что все реализованные в программах СКЗИ методы генерации включены в список [b].

КП.3-3. Эксперт проверяет корректность программных реализаций стандартных методов генерации из списка [b].

Проверка корректности ДОЛЖНА проводиться по методике, специальной для целевого метода. Данная методика ДОЛЖНА быть согласована с Органом по сертификации. ДОЛЖНА использоваться уже разработанная методика или, если такая методика отсутствует, ДОЛЖНА быть разработана новая методика.

В разрабатываемой методике ДОЛЖНЫ быть определены:

1 Методы анализа исходных текстов программной реализации [c]. Выбранные методы анализа ДОЛЖНЫ включать проверки, определенные в Приложении А. К анализу исходных текстов ДОЛЖНЫ привлекаться, по меньшей мере, два независимых эксперта.

2 Тесты для программной реализации [d]. Выбранный план тестирования ДОЛЖЕН содержать тесты, определенные в Приложении Б.

Проверка корректности МОЖЕТ не проводиться, если целевая программная реализация уже прошла испытания по методикам, удовлетворяющим упомянутым выше требованиям. В таких случаях эксперт может зачесть представленные свидетельства [e]. При этом эксперт ДОЛЖЕН предварительно проверить совпадение испытанных программных реализаций с представленными.

КП.3-4. Эксперт проверяет, что методы разработчика из списка [b] уточняют ТНПА на соответствующий алгоритм из списка [a]. Уточнения могут состоять в определении вспомогательных алгоритмов генерации простых чисел, блоков подстановки, эллиптических кривых и т.д. Уточнения не должны противоречить требованиям ТНПА.

КП.3-5. Эксперт проверяет корректность программных реализаций методов разработчика из списка [b]. Проверка корректности ДОЛЖНА включать две процедуры:

1 Анализ исходных текстов программной реализации [c]. Выбранные методы анализа ДОЛЖНЫ включать проверки, определенные в Приложении А. К анализу исходных текстов ДОЛЖНЫ привлекаться, по меньшей мере, два независимых эксперта.

2 Тестирование реализации [d]. Выбранный план тестирования ДОЛЖЕН содержать тесты, определенные в Приложении Б.

Требование КП.4 (2–4). Криптографический алгоритм [КП.1], а также методы генерации его ключей, должны быть реализованы так, чтобы по времени их выполнения нельзя было сделать вывод об используемых или генерируемых личных и секретных ключах.

Входные данные:

a) список криптографических алгоритмов;

b) методы генерации долговременных параметров и ключей (только ключей);

c) механизмы контроля времени выполнения криптографических алгоритмов;

d) исходные тексты программных реализаций криптографических алгоритмов, методов генерации их ключей;

e) компоненты СКЗИ, реализующие криптографические алгоритмы, методы генерации их ключей.

Действия эксперта:

КП.4-1. Эксперт анализирует списки [a], [b] и составляет перечень композиционных элементов алгоритмов и методов генерации, время выполнения которых может существенно зависить от значений секретных или личных ключей.

Действия эксперта ДОЛЖНЫ быть направлены на поиск алгоритмических конструкций вида:

```
if (некоторая_функция(ключ))
   блок_1;
else
   блок_2;
```

где время выполнения блоков 1 и 2 значимо отличается.

Пример — Подобные конструкции встречаются, например, при возведении образующего g некоторой циклической группы в степень личного ключа x. Если для вычисления g^x используются бинарные методы, то время вычислений существенно зависит от числа единиц в двоичном представлении x. В качестве циклических групп могут выступать как подгруппы мультипликативной группы конечного поля, так и группы точек эллиптической кривой.

Примечание — При анализе эксперт должен учитывать особенности аппаратных платформ, на которых выполняются программы СКЗИ. Например, в современных процессорах широко используется кэш-память. Чтение ячеек массива, размещенного в обычной оперативной памяти, выполняется следующим образом:

```
if (ячейка массив[индекс] не загружена в кэш-память)
   загрузить массив[индекс] в кэш-память;
возвратить массив[индекс] из кэш-памяти;
```

Загрузка данных в кэш-память выполняется существенно медленнее, чем чтение данных из кэш-памяти. Поэтому если состояние кэш-памяти зависит от ключа (например, индексы массива являются компонентами ключа), то и время выполнения криптографической операции будет зависеть от ключа. Подобные зависимости возникают в симметричных криптосистемах с большими блоками подстановки.

КП.4-2. Эксперт анализирует средства контроля [c] и проверяет их достаточность с учетом результатов, полученных на шаге КП.4-1.

КП.4-3. Эксперт проводит полный анализ исходных текстов [d] и проверяет, что средства контроля [c] корректно реализованы.

КП.4-4. Эксперт проводит тестирование компонентов [e], направленное на оценку зависимости между временем выполнения целевых криптографических операций и используемыми в них секретными или личными ключами.

Примечание — При тестировании рекомендуется выбирать пары ключей, время работы на которых по результатам проведенного анализа должно быть минимальным и максимальным. Далее эксперту следует многократно повторять обработку данных на выбранных ключах и

осуществлять замеры времени. По результатам замеров (при необходимости, с применением подходящих методов статистической проверки гипотез о равенстве средних в двух выборках) эксперт выносит вердикт о наличии существенной зависимости времени выполнения криптографических операций от значений ключа.

Требование КП.5 (1–4). При включении в состав СКЗИ заранее сгенерированных долговременных параметров криптографического алгоритма [КП.1] должно быть подтверждено, что параметры получены в соответствии со спецификацией на алгоритм.

Примечание 3 — При использовании стандартных параметров, заданных в спецификации, подтверждением является ссылка на нее. В других случаях в качестве подтверждения могут выступать затравочные значения, использованные при генерации, или расчеты, демонстрирующие соблюдение метрик качества параметров.

Входные данные:

a) список криптографических алгоритмов;

b) методы генерации долговременных параметров и ключей;

c) исходные тексты программных реализаций криптографических алгоритмов;

d) исходные тексты программ разработчика для генерации долговременных параметров и ключей (при наличии);

e) компоненты разработчика, реализующие генерацию долговременных параметров и ключей (при наличии).

Действия эксперта:

КП.5-1. Эксперт проверяет, что в список [b] включены все методы внешней генерации, необходимые для настройки и выполнения криптографических алгоритмов из списка [a].

Примечание — Эксперт использует результаты, полученные на шаге КП.3-1.

Эксперт ДОЛЖЕН вынести отрицательный вердикт, если внешние параметры использованы без ссылки на ТНПА или без обоснования критериев выбора.

КП.5-2. Эксперт проверяет корректность методов внешней генерации из списка [b]. Если внешняя генерация состоит в использовании стандартных параметров, заданных в некотором ТНПА, то эксперт проводит полный анализ исходных текстов [c] и проверяет, что параметры программ СКЗИ соответствуют параметрам ТНПА.

Если внешняя генерация выполняется по критериям разработчика, то эксперт:

1 Проводит анализ критериев [b].

2 Проверяет выполнение критериев для параметров, установленных в исходных текстах программ [c].

Анализ критериев проводится по доступным научно-техническим материалам, касающихся принципов построения и оценки надежности криптографических систем. Критерии признаются корректными, если они соответствуют данным принципам.

Описание и обоснование критериев может сопровождаться их программной реализацией, представленной исходными текстами [d] и (или) программными компонентами [e]. В таких случаях эксперт ДОЛЖЕН провести анализ исходных текстов [d] и (или) проверить работоспособность программных компонентов [e].

Требование КП.6 (1–4). При смене долговременных параметров криптографического алгоритма [КП.1] должна выполняться смена его ключей. Другими словами, ключ криптографического алгоритма не должен использоваться с двумя различными наборами долговременных параметров.

Входные данные:

a) список криптографических алгоритмов;
b) методы генерации долговременных параметров и ключей;
c) исходные тексты программ генерации долговременных параметров и ключей;
d) исходные тексты программных реализаций криптографических алгоритмов;
e) компоненты СКЗИ, реализующие криптографические алгоритмы.

Действия эксперта:

КП.6-1. Для каждого криптографического алгоритма из списка [a], для которого предусмотрена смена долговременных параметров в методе [b], эксперт проверяет, что при смене долговременных параметров криптографического алгоритма выполняется смена его ключей.

КП.6-2. Эксперт проводит полный анализ исходных текстов [c], [d] и для каждого криптографического алгоритма из списка [a] проверяет, что при смене его долговременных параметров выполняется смена его ключей.

Эксперт ДОЛЖЕН вынести отрицательный вердикт, если ключ криптографического алгоритма может использоваться в СКЗИ с двумя различными наборами долговременных параметров.

6.2 Проверка требований по реализации сервисов

Требование РС.1 (1–4). Должны быть определены и корректно реализованы {АП.3, АП.4, АП.5} сервисы СКЗИ. Для каждого сервиса должно быть определено его назначение, входные и выходные данные, признак критичности. Должны быть указаны допустимые последовательности вызовов сервисов. Должны быть выделены криптографические сервисы. В них должны использоваться алгоритмы перечня [КП.1].

Входные данные:

a) основные функциональные возможности;
b) список криптографических алгоритмов;
c) методы генерации долговременных параметров и ключей;
d) список сервисов;
e) внешние интерфейсы;
f) исходные тексты программных реализаций сервисов;
g) компоненты СКЗИ, реализующие сервисы;
h) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

РС.1-1. Эксперт проверяет, что основные функциональные возможности СКЗИ из списка [a] покрываются сервисами из списка [d].

РС.1-2. Эксперт проверяет, что в списке [d] выделены криптографические сервисы. Так, что все криптографические алгоритмы из списка [b] покрываются криптографическими сервисами из списка [d].

РС.1-3. Эксперт проверяет, что каждый сервис из списка [d] однозначно идентифицирован. Это значит, что представлена, по крайней мере, следующая информация:

1 Назначение сервиса (например, сервис самотестирования, сервис выработки ЭЦП).

2 Входные данные сервиса (например, входные файлы, опции, параметры командной строки, параметры функции логического интерфейса, параметры (состояния) физического интерфейса).

3 Выходные данные (например, возврат функции логического интерфейса, параметры (состояния) физического интерфейса).

4 Признак критичности.

Описание входных и выходных данных сервисов в списке [d] может быть примерным и полуформальным. Эксперт проверяет, что данное описание детализируется в [e].

Если в список [d] включен сервис автономной работы СКЗИ, эксперт ДОЛЖЕН проверить, что данный сервис включен в перечень сервисов [d] как критический.

РС.1-4. Эксперт проверяет полноту ограничений на последовательность вызова сервисов из списка [d].

Эксперт ДОЛЖЕН проверить, что в необходимых случаях заданы ограничения следующих типов:

1 «Ключ используется только после инициализации (импорта или генерации)».

2 «Контекст работы с криптографическим алгоритмом используется только после инициалиации».

3 «После заверешения криптографической операции освобождаются определенные объекты».

4 «Вызов сервисов в некорректной последовательности отслеживается и блокируется».

РС.1-5. Эксперт проводит выборочный (если уровень [h] равен 2) или подробный (если уровень [h] равен 3 или 4) анализ исходных текстов [f] и проверяет, что все доступные операторам функции СКЗИ включены в список [d].

Примечание — Список [d] должен включать все доступные операторам интерфейсы взаимодействия с СКЗИ, включая входные точки выполняемых программ СКЗИ. В список могут не включаться вспомогательные или интерфейсные сервисы, не связанные непосредственно с безопасностью. Если неявная роль системного оператора не включена в список ролей, то системные сервисы также могут не включаться в список.

Особое внимание эксперт ДОЛЖЕН обратить на следующие аспекты:

1 При разработке СКЗИ могли быть созданы отладочные сервисы, которые по ошибке не были исключены из окончательной реализации СКЗИ.

2 Определенная функция СКЗИ не была включена в список сервисов в связи с ошибочным предположением о том, что она недоступна оператору.

3 Определеннная функция СКЗИ не была включена в список сервисов в связи с ошибочным предположением о том, что она не связана с механизмами безопасности СКЗИ.

РС.1-6. Эксперт проводит выборочный (если уровень [h] равен 2) или подробный (если уровень [h] равен 3 или 4) анализ исходных текстов [f] и проверяет корректность программных реализаций сервисов [d]. Корректность означает, что реализации функцио-

нально соответствуют описаниям сервисов в [d, e], и что реализации не содержат ошибок и уязвимостей.

Эксперт ДОЛЖЕН проверить следующие аспекты реализаций сервисов:

1 Все входные параметры сервисов проверяются на корректность. Проверка должна быть исчерпывающей, т.е. она не должна приводить к переходу СКЗИ в небезопасное состояние.

Пример — Проверки указателя на NULL достаточно при выделении памяти, но недостаточно при контроле входных данных сервиса. В последнем случае необходимо проверить, что память под указателем действительно доступна, указатель не ссылается на память команд (защита от атак типа «переполнение буфера») и т.д. Проверка может быть косвенной, например, вызов сервиса может быть погружен в блок try-catch языка C++.

2 Сервис реализован по принципу «все или ничего». Это значит, что сервис либо успешно заканчивает свою работу, либо возвращает код ошибки, не изменяя состояния СКЗИ.

Пример — Если идет речь о генерации ключа, то ключ будет либо сгенерирован, либо нет — генерация ключа «наполовину» невозможна.

3 Вызов сервисов в некорректной последовательности отслеживается и блокируется.

РС.1-7. Эксперт проводит полный анализ исходных текстов [f] и проверяет корректность встраивания реализаций криптографических алгоритмов [b] и методов генерации параметров и ключей [c]. Корректность означает, что все вызовы криптографических алгоритмов [b], методов генерации параметров и ключей [c] корректны. Это означает, что криптографические операции вызываются в правильной последовательности, при вызовах правильно указываются входные данные криптографических операций, а после вызовов правильно обрабатываются результаты выполнения операций.

РС.1-8. Эксперт проводит выборочное (если уровень [h] равен 1 или 2) или подробное (если уровень [h] равен 3 или 4) тестирование компонентов [g] и проверяет корректность реализаций сервисов [d].

Эксперт ДОЛЖЕН реализовать следующий план тестирования:

1 *Функциональное тестирование.* Направлено на проверку того, что сервис действительно реализует объявленные функциональные возможности. Для каждого сервиса ДОЛЖЕН быть выполнен, по крайней мере, один функциональный тест. Эксперт МОЖЕТ использовать тесты и тестовые программы из программы испытаний СКЗИ (см. процесс ПИ).

2 *Тесты проникновения.* Эксперт вызывает сервисы в некорректной последовательности. На вход сервисов подаются заведомо неверные данные, например, пароли, содержащие неверные символы, или нулевые указатели. Эксперт пытается сформировать такие данные, при обработке которых не будет нормального завершения сервисов, например, произойдет переполнение внутренних буферов программ.

3 *Стресс-тесты.* Во время выполнения сервисов индуцируются ошибки (разрыв канала связи, отключения носителя ключей) и фиксируется реакция сервисов на эти внешние воздействия. Эксперт пытается вызвать такие сбои, при которых не будет нормального завершения сервисов.

Требование РС.2 (1–4). В список сервисов должны быть включены {РС.1}:
- сервис вывода номера версии СКЗИ;
- сервисы самотестирования [СТ.3];

– сервис вывода контрольных характеристик файлов программ СКЗИ;
– по крайней мере один криптографический сервис.

Входные данные:

a) список сервисов.

Действия эксперта:

РС.2-1. Эксперт проверяет, что список [a] содержит перечисленные в требовании сервисы.

Требование РС.3 (1–4). На любых входных данных сервис [РС.1] должен нормально завершаться, т. е. возвращать правильный результат, в том числе признак некорректных входных данных.

Действия эксперта: проверка РС.3 покрывается проверками по РС.1.

Требование РС.4 (2–4). Сервис [РС.1], который выполняет операцию над критическими объектами [УД.2], должен быть реализован так, чтобы после его завершения в пределах криптографической границы не оставалось неявных копий критических объектов в незашифрованном виде.

Примечание — Неявная копия может остаться в файле подкачки операционной системы, регистрах процессора, журнале аудита.

Входные данные:

a) механизмы защиты от создания неявных копий критических объектов;
b) исходные тексты программных реализаций сервисов СКЗИ;
c) компоненты СКЗИ, реализующие сервисы;
d) список сервисов;
e) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

РС.4-1. Для всех сервисов из списка [d], которые выполняют операции над критическими объектами, эксперт проверяет, что механизмы защиты [a] действительно препятствуют тому, чтобы после завершения сервиса [d] в пределах криптографической границы оставались неявные копии критических объектов в незашифрованном виде.

Эксперт ДОЛЖЕН проанализировать возможность передачи неявных копий критических объектов по побочным каналам, таким как файл подкачки, регистры процессора, журнал аудита. При анализе эксперт использует информацию о побочных каналах, известных для аппаратной платформы или операционной системы СКЗИ.

Если СКЗИ выполняется под управлением операционной системы Windows, то эксперт ДОЛЖЕН проанализировать следующие побочные каналы:

1 Файл подкачки (pagefile.sys).

2 Файл спящего режима (hiberfile.sys).

3 Отладочные дампы памяти, сохраняемые операционной системой при сбоях в программах.

РС.4-2. Эксперт проводит выборочный (если уровень [e] равен 2) или подробный (если уровень [e] равен 3 или 4) анализ исходных текстов [b] и проверяет, что механизмы защиты [a] корректно реализованы.

РС.4-3. Если для формирования вердикта на шаге РС.4-1 требуются дополнительные данные, то эксперт проводит тестирование компонентов [c].

При тестировании эксперт создает ситуации, потенциально благоприятные для передачи неявных копий по побочным каналам, а затем проверяет побочные каналы. Если, например, побочным каналом является файл подкачки Windows, то эксперт организует нехватку оперативной памяти, запускает программы СКЗИ, а затем проверяет попадание определенных ключей или иных критических объектов СКЗИ в файл подкачки.

Требование РС.5 (1–4). Критический сервис [РС.1] должен быть реализован так, что он успешно завершается только при срабатывании двух и более независимых триггеров.

Входные данные:

a) список сервисов;
b) исходные тексты программных реализаций сервисов СКЗИ;
c) компоненты СКЗИ, реализующие сервисы;
d) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

РС.5-1. Эксперт проводит выборочный (если уровень [d] равен 1 или 2) или подробный (если уровень [d] равен 3 или 4) анализ исходных текстов [b] и (или), соответственно, выборочное или подробное тестирование реализаций [c] и проверяет корректность реализации вызовов критических сервисов из списка [a]. Корректность означает, что для успешного вызова критического сервиса из списка [a] необходимо выполнение двух и более независимых условий, в противном случае вызов сервиса блокируется.

Требование РС.6 (2–4). Сервисы [РС.1] должны быть реализованы так, чтобы их вызов в некорректной последовательности отслеживался и блокировался.

Действия эксперта: проверка РС.6 покрывается проверками по РС.1.

Требование РС.7 (3, 4). В список сервисов должен быть включен {РС.1} сервис вывода текущего состояния СКЗИ [УД.4].

Входные данные:

a) список сервисов.

Действия эксперта:

РС.7-1. Эксперт проверяет, что список [a] содержит сервис вывода текущего состояния СКЗИ.

6.3 Проверка требований по управлению доступом

Требование УД.1 (1–4). Должны быть определены роли операторов СКЗИ. Должна быть предусмотрена роль «Администраторы».

Входные данные:

a) список ролей операторов;

b) исходные тексты программных реализаций механизмов управления доступом;

c) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

УД.1-1. Эксперт проверяет, что список [a] содержит роль «Администраторы».

УД.1-2. Эксперт проводит выборочный (если уровень [c] равен 1 или 2) или подробный (если уровень [c] равен 3 или 4) анализ исходных текстов и проверяет, что все поддержанные в программах СКЗИ роли операторов включены в список [a].

Требование УД.2 (1–4). Должны быть определены объекты СКЗИ. Для каждого объекта должно быть задано его назначение, проведена классификация (открытый или критический, сеансовый или долговременный), указан срок действия (время жизни), определен владелец. Должны быть перечислены неизвлекаемые критические объекты (при наличии).

Примечание 1 — При выполнении сервисов может создаваться несколько сеансовых копий одного и того же объекта в нескольких переменных программ. Сеансовые копии необязательно определять как отдельные объекты, достаточно обеспечить их очистку по завершении сеансов [ЗО.12].

Примечание 2 — К объектам СКЗИ не относятся секреты аутентификации [ИА.2], которые циркулируют в среде эксплуатации без контроля со стороны СКЗИ. Однако контрольные значения секретов могут быть долговременными объектами СКЗИ. Кроме этого, в ходе сеансов на основе аутентификационных данных могут вырабатываться сеансовые объекты (например, хэш-значение пароля, используемое в качестве ключа), которые находятся под контролем СКЗИ.

Входные данные:

a) основные функциональные возможности;

b) список сервисов;

c) список объектов;

d) перечень проверок самотестирования;

e) методы аутентификации операторов;

f) исходные тексты программ СКЗИ;

g) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

УД.2-1. Эксперт проверяет, что каждый объект из списка [c] подробно описан. Это значит, что представлена, по крайней мере, следующая информация:

1 Назначение (например, ключ шифрования, файл настроек).

2 Классификация (открытый, критический, сеансовый, долговременный, неизвлекаемый).

3 Владелец (например, объект администратора, системный объект).

4 Срок действия (время жизни).

Эксперт проверяет, что описан (прямо или косвенно) жизненный цикл криптографических ключей из списка [c]. Информация о жизненном цикле включает описание способов генерации, распределения, экспорта, импорта, хранения и уничтожения ключей.

Эксперт проверяет правильность классификации объектов с учетом их назначения.

УД.2-2. Эксперт анализирует списки [a, b, d, e], проводит выборочный (если уровень [g] равен 1 или 2) или подробный (если уровень [g] равен 3 или 4) анализ исходных текстов [f]. Эксперт проверяет, что все подлежащие защите объекты СКЗИ включены в список [c].

Эксперт ДОЛЖЕН руководствоваться следующими критериями:

1 В список критических объектов должны быть включены все объекты, раскрытие или несанкционированная модификация которых может привести к снижению безопасности. Личные и секретные ключи криптографических алгоритмов (не считая тестовых ключей), частичные секреты, используемые в методах разделения секрета, должны быть отнесены к критическим объектам.

2 В список критических объектов должны быть включены контрольные значения секретов аутентификации [e], если они касаются секретов аутентификации и по ним за приемлемое время можно определить секрет. Сеансовые объекты, которые содержат значения секретов аутентификации, также должны быть отнесены к критическим объектам.

3 В список открытых объектов должны быть включены все объекты, несанкционированная модификация которых может привести к снижению безопасности, а раскрытие — нет. Открытые ключи и долговременные параметры криптографических алгоритмов (не считая тестовых ключей, см. п. 7) должны быть отнесены к открытым объектам.

4 В список открытых объектов должны быть включены контрольные значения аутентификационных данных [e] (исключая секреты аутентификации).

5 Сеансовые копии долговременных объектов из списка [c] могут не включаться в этот список.

6 Все криптографические ключи, которые используются или генерируются в СКЗИ, должны быть включены в список [c].

7 Тестовые данные криптографических алгоритмов и протоколов (тестовые ключи, открытые тексты, шифртексты), которые используются при самотестировании [d], должны быть включены в список [c] как открытые объекты.

8 В список неизвлекаемых объектов должны быть включены все объекты, вывод за пределы криптографической границы СКЗИ которых либо полностью запрещен, либо применяется исключительно для резервного сохранения и выполняется с помощью метода разделения секрета.

Примечание — Тестовые данные, заданные в исходных текстах, а не виде отдельных файлов, могут быть учтены как часть программ СКЗИ.

Требование УД.3 (1–4). Должна быть определена и корректно реализована {АП.4, АП.5} политика управления доступом СКЗИ. Политика должна устанавливать набор допустимых операций операторов различных ролей [УД.1] над сервисами [РС.1] и сервисов, выступающих от имени операторов, над объектами [УД.2],

другими сервисами и, при необходимости ограничения доступа, критическими системными компонентами [СТ.1].

Примечание 3 — Стандартные операции: выполнение (X) сервисов; создание / генерация (C), удаление / очистка (D), экспорт (E), импорт (I), чтение (R) и запись (W) объектов; использование (U) ресурсов КСК. Могут вводиться другие операции.

Примечание 4 — Доступ к файлу с защищенным критическим объектом не считается операцией чтения, если защита с объекта не снята. Однако копирование файла за пределы криптографической границы может считаться операцией экспорта, если защиту предполагается снять позже.

Входные данные:

a) список сервисов;
b) список ролей операторов;
c) список объектов;
d) описание политики управления доступом;
e) состояния СКЗИ и правила перехода между состояниями;
f) список руководств;
g) исходные тексты программных реализаций политики управления доступом;
h) компоненты СКЗИ, реализующие политики управления доступом;
i) список критических системных компонентов];
j) уровень (1, 2, 3 или 4) безопасности СКЗИ;
k) перечень объектов, подлежащих очистке.

Действия эксперта:

УД.3-1. Эксперт проводит анализ корректности политики [d].

Эксперт ДОЛЖЕН проверить, что политика [d] удовлетворяет следующим правилам:

1 Вопрос о правомочности выполнения операции над каждым объектом из списка [c] решается на основании роли оператора [b] и текущего состояния СКЗИ [e]. Дополнительно может использоваться другая информация, например, информация о владельце объекта и идентификатор оператора.

2 Для каждого состояния [e] указаны разрешенные операции операторов каждой роли [b] над сервисами [a]. Разрешения таковы, что каждый сервис можно выполнить при определенных условиях.

3 Доступ к сервису автономной работы СКЗИ, если данный сервис имеется в СКЗИ, имеют только администраторы.

4 Если в [b] предусмотрена роль «Супервизоры», то операторы этой роли не имеют доступа на чтение (прямой или косвенный) к критическим объектам [c] других операторов.

5 В состоянии полной блокировки запрещено выполнение всех сервисов из списка [a], кроме сервисов роли «Супервизоры» из списка [b].

6 Если в [a] предусмотрены сервисы настройки порога числа записей журнала аудита и предпринимаемых при превышении порога действий, то данные сервисы должны быть доступны только роли «Администраторы» из списка [b].

7 Если в [a] предусмотрен сервис обновления программ СКЗИ, то данный сервис должен быть доступным только роли «Администраторы» из списка [b].

8 Если в [a] предусмотрен сервис принудительной очистки, то данный сервис доступен оператору из списка [b] — владельцу объектов из перечня [k], а также возможно доступен роли «Администраторы» из списка [b].

9 Если предусмотренный в [a] сервис принудительной очистки вызывается в сеансе владельца, то этот сеанс должен быть завершен сразу после очистки.

10 Для каждого состояния [e] указаны разрешенные операции сервисов [a], выступающих от имени операторов той или иной роли [b], над объектами [c], сервисами [a] и, при необходимости ограничения доступа, КСК [i]. Разрешения таковы, что над каждым объектом, сервисом, КСК при определенных условиях можно выполнить операцию.

11 Использованы операции из следующего списка: выполнение сервисов, создание / генерация объекта, удаление / очистка объекта, экспорт объекта, импорт объекта, чтение объекта, запись объекта, использование ресурсов КСК и т.д.

12 В состоянии блокировки [e] запрещено выполнение всех сервисов [a], кроме сервисов самотестирования, сервисов аутентификации администратора и вспомогательных сервисов, не связанных с обработкой объектов внутри криптографической границы, криптографических сервисов, которые сохранили работоспособность по результатам самотестирования и доступ к которым необходим для корректного завершения сеанса оператора.

Примечание 1 — По сути политика управления доступом должна быть представлена в виде нескольких таблиц «субъект (оператор или сервис) – разрешенные операции – объект», соответствующих каждому из состояний, хотя форма представления может отличаться. Например, для сокращения описания могут быть указаны только различия между таблицами прав доступа для состояний, могут быть введены группы объектов с однотипными правами доступа и др.

Примечание 2 — В политику может не включаться системный оператор и его сервисы. По умолчанию, системный оператор может выполнять любой сервис, а системные сервисы могут выполнять над любым объектом любые корректные операции.

УД.3-2. Эксперт проверяет, что для каждой роли операторов [b] разработано соответствующее руководство [f]. Эксперт проверяет, что в руководствах описаны сервисы, доступные (в соответствии с [d]) операторам соответствующей роли.

Примечание — Руководств может быть меньше, чем ролей. В некоторых руководствах могут параллельно даваться инструкции сразу нескольким ролям операторов.

УД.3-3. Эксперт проводит выборочный (если уровень [j] равен 1 или 2) или подробный (если уровень [j] равен 3 или 4) анализ исходных текстов [g] и (или), соответственно, выборочное или подробное тестирование компонентов [h] и проверяет корректность программной реализации политики [d].

Эксперт ДОЛЖЕН проверить следующие аспекты реализации политики:

1 В состояниях [e], соответствующих сеансам операторов различных ролей, действует политика [d] относительно данных ролей.

2 Если в программах СКЗИ поддерживается многозадачность, то применяются средства синхронизации для предотвращения одновременного изменения одного и того же объекта.

Примечание — Если в программах СКЗИ поддержан графический пользовательский интерфейс, то эксперту рекомендуется проверить, что разрешения на доступ к тем или иным интерфейсным элементам (кнопкам, пунктам меню) соответствуют политике [d].

Требование УД.4 (1–4). Должны быть определены состояния СКЗИ. Должны быть определены и корректно реализованы {АП.4, АП.5} правила перехода между состояниями. Должны быть предусмотрены следующие состояния:

- состояние включения (запуска программ);
- состояния, соответствующие сеансам операторов различных ролей [УД.1];
- состояние блокировки;
- состояние выключения (завершения программ).

Примечание 5 — Примеры других состояний: «самотестирование», «ожидание» (до аутентификации операторов), «временная блокировка» (блокировка на определенный период времени после превышения порога неудачных попыток аутентификации).

Входные данные:

a) основные функциональные возможности;
b) список ролей операторов;
c) описание политики управления доступом;
d) состояния СКЗИ и правила перехода между состояниями;
e) обработка ошибок тестирования;
f) исходные тексты программных реализаций модели состояний;
g) компоненты СКЗИ, реализующие модель состояний;
h) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

УД.4-1. Эксперт проверяет, что спецификация [d] определяет пречисленные в требовании состояния (состояние включения (запуска программ), состояния, соответствующие сеансам операторов всех ролей из списка [b], состояние блокировки и состояние выключения (завершения программ)) и состояние полной блокировки.

Эксперт анализирует документ [a] и проверяет, что СКЗИ поддерживает одновременную работу с несколькими операторами. Если это так, то эксперт ДОЛЖЕН проверить, что в спецификации [d] описано одновременное выполнение сразу нескольких сеансов операторов и дублирование соответствующих состояний.

УД.4-2. Эксперт проводит выборочный (если уровень [h] равен 1 или 2) или подробный (если уровень [h] равен 3 или 4) анализ исходных текстов [f] и проверяет, что в спецификации [d] определены все поддержанные в СКЗИ состояния.

Примечание — Определение состояний по текстам программ может оказаться непростой задачей. Эксперту рекомендуется сосредоточиться на анализе загрузки программ. Как правило, при загрузке проверяются различные условия, в зависимости от их выполнения управление передается тем или иным компонентам программы, которые и соответствуют состояниям СКЗИ. Также эксперту рекомендуется сосредоточиться на аутентификации операторов, после которой СКЗИ, как правило, переходит в состояния, соответствующие ролям операторов.

УД.4-3. Эксперт проверяет, что спецификация [d] определяет правила перехода между состояниями.

Эксперт ДОЛЖЕН проверить, что [d] включает следующие правила:

1 Перед переходом в состояния, соответствующие сеансам операторов различных ролей [b], проводится аутентификация операторов.

2 При ошибках самотестирования [e] СКЗИ должно перейти в состояние блокировки.

3 При переходе в состояние блокировки завершаются все открытые сеансы операторов.

4 Если перед выключением СКЗИ находилось в состоянии блокировки, то оно должно вернуться в это состояние сразу после включения.

5 При переходе в состояние полной блокировки завершаются все открытые сеансы операторов, удаляются критические объекты в незашифрованном виде.

6 Если перед выключением СКЗИ находилось в состоянии полной блокировки, то оно должно вернуться в это состояние сразу после включения.

УД.4-4. Эксперт проводит выборочный (если уровень [h] равен 1 или 2) или подробный (если уровень [h] равен 3 или 4) анализ исходных текстов [f] и (или), соответственно, выборочное или подробное тестирование компонентов [g] и проверяет корректность реализации спецификации [d].

Эксперт ДОЛЖЕН проверить следующие аспекты реализации:

1 Состояния связаны с определенными компонентами (ветвями) программ СКЗИ и с определенными программными признаками (флагами). Переход между состояниями состоит в передаче управления компонентам и сопровождается переключением признаков.

2 События, которые инициируют переход между состояниями, обязательно обрабатываются.

3 Во время обработки события (при переходе к новому состоянию) обработка других событий блокируется.

Требование УД.5 (1–4). В состояниях, соответствующих сеансам операторов явных ролей [УД.1], должна действовать политика управления доступом [УД.3] относительно данных ролей. Перед переходом в состояния должна проводиться аутентификация операторов [ИА.3].

Примечание 6 — Многозадачные операционные системы могут поддерживать одновременное выполнение сеансов для нескольких явных операторов СКЗИ. При этом состояния «сеанс оператора той или иной роли» дублируются. Считается, что СКЗИ одновременно находится сразу во всех этих состояниях.

Действия эксперта: проверка УД.5 покрывается проверками по УД.3, УД.4.

Требование УД.6 (1–4). В состоянии блокировки [УД.4] должно быть запрещено выполнение всех сервисов, кроме следующих:

– сервисы самотестирования [СТ.3];

– сервисы аутентификации администратора [ИА.3];

– вспомогательные сервисы, не связанные с обработкой объектов внутри криптографической границы;

– криптографические сервисы, которые сохранили работоспособность по результатам самотестирования и доступ к которым необходим для корректного завершения сеанса оператора.

При переходе в состояние блокировки должны быть завершены все открытые сеансы операторов. Если перед выключением СКЗИ находилось в состоянии блокировки, то оно должно вернуться в это состояние сразу после включения.

Действия эксперта: проверка УД.6 покрывается проверками по УД.4.

Требование УД.7 (1–4). Сервис запуска автономной работы СКЗИ, если он имеется, должен быть включен {РС.1} в перечень сервисов как критический. Доступ к сервису должны иметь {УД.3} только администраторы.

Действия эксперта: проверка УД.7 покрывается проверками по РС.1, УД.3.

Требование УД.8 (1–4). Если в СКЗИ предусмотрена роль «Супервизоры» [УД.1], то операторы этой роли не должны иметь {УД.3} доступ на чтение (прямой или косвенный) к критическим объектам других операторов.

Действия эксперта: проверка УД.8 покрывается проверками по УД.3.

Требование УД.9 (4). Перечень состояний СКЗИ должен включать {УД.4} состояние полной блокировки. В этом состоянии должно быть запрещено выполнение всех сервисов, кроме сервисов роли «Супервизоры». При переходе в состояние полной блокировки должны быть завершены все открытые сеансы операторов, удалены критические объекты в незашифрованном виде. Если перед выключением СКЗИ находилось в состоянии полной блокировки, то оно должно вернуться в это состояние сразу после включения.

Действия эксперта: проверка УД.9 покрывается проверками по УД.3, УД.4.

6.4 Проверка требований по защите объектов

Требование ЗО.1 (1–4). Должна обеспечиваться конфиденциальность критических объектов [УД.2]. Используемые для этого методы защиты должны выбираться из следующего списка: криптографические, аппаратные, разделения секрета. При защите частичных секретов список дополняется организационными мерами. На уровне 1 при защите объектов во время хранения список дополняется системными методами.

Входные данные:

a) список объектов;
b) криптографические методы обеспечения конфиденциальности;
c) аппаратные методы защиты;
d) методы разделения секрета;
e) организационные меры обеспечения конфиденциальности;
f) соответствие «объекты — методы защиты»;
g) системные методы защиты.

Действия эксперта:

ЗО.1-1. Эксперт проводит анализ соответствия [f] и проверяет, что конфиденциальность всех критических объектов из списка [a] обеспечивается с помощью методов из списков [b, c, d, e, g], причем организационные меры из списка [e] используются только

для защиты частичных секретов, а системные методы защиты из списка [g] используются только на уровне 1 при защите объектов [a] во время хранения.

Требование ЗО.2 (1–4). Должен осуществляться контроль целостности и подлинности критических и открытых объектов [УД.2]. Используемые для этого методы защиты должны выбираться из следующего списка: криптографические, аппаратные, алгоритмические. На уровне 1 при контроле целостности объектов во время хранения список дополняется системными методами.

Входные данные:

a) список объектов;
b) криптографические методы контроля целостности и подлинности;
c) аппаратные методы защиты;
d) алгоритмические методы контроля целостности;
e) соответствие «объекты – методы защиты»;
f) системные методы защиты.

Действия эксперта:

ЗО.2-1. Эксперт проводит анализ соответствия [e] и проверяет, что контроль целостности и подлинности всех критических и открытых объектов из списка [a] обеспечивается с помощью методов из списков [b, c, d, f], причем системные методы защиты из списка [a] используются только на уровне 1 при контроле целостности объектов объектов [a] во время хранения.

Требование ЗО.3 (1–4). Должны быть определены и корректно реализованы {АП.3, АП.4, АП.5} криптографические методы обеспечения конфиденциальности. Методы должны быть основаны на алгоритмах шифрования [КП.1]. Личные и секретные ключи алгоритмов должны быть отнесены {УД.2} к критическим объектам, а открытые ключи и долговременные параметры — {УД.2} к открытым объектам.

Примечание 1 — При планировании защиты следует руководствоваться правилом: ключ защиты не должен быть слабее защищаемого критического объекта. Например, не следует устанавливать защиту 256-битового ключа на 128-битовом.

Входные данные:

a) список криптографических алгоритмов;
b) список объектов;
c) криптографические методы обеспечения конфиденциальности;
d) соответствие «объекты — методы защиты»;
e) исходные тексты программных реализаций криптографических методов обеспечения конфиденциальности;
f) компоненты СКЗИ, реализующие криптографические методы обеспечения конфиденциальности;
g) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ЗО.3-1. Для каждого метода из списка [c] эксперт проверяет, что:

1 Метод основан на алгоритмах шифрования из списка [a].

2 Используемые в методе личные и секретные ключи алгоритмов включены в список [b] и отнесены к критическим объектам.

3 Используемые в методе открытые ключи и долговременные параметры алгоритмов включены в список [b] и отнесены к открытым объектам.

4 Используемый в методе ключ защиты не слабее защищаемого критического объекта.

ЗО.3-2. Эксперт проводит выборочный (если уровень [g] равен 2) или подробный (если уровень [g] равен 3 или 4) анализ исходных текстов [e] и (или), соответственно, выборочное или подробное тестирование компонентов [f] и проверяет корректность реализации методов из списка [c].

Примечание — Корректность реализации {АП.3} криптографических алгоритмов на этом шаге не проверяется. Проверка корректности выполняется на шаге КП.1-3.

Эксперт ДОЛЖЕН проверить следующие аспекты реализаций методов:

1 Все вызовы криптографических алгоритмов [a] корректны. Это означает, что при вызовах алгоритмов правильно указываются их входные данные, а после вызовов правильно обрабатываются возвращаемые результаты.

2 Методы действительно применяются для защиты объектов в соответствии с [d].

Требование ЗО.4 (1–4). Должны быть определены и корректно реализованы {АП.3, АП.4, АП.5} криптографические методы контроля целостности и подлинности. Методы должны быть основаны на алгоритмах ЭЦП и имитозащиты [КП.1]. Личный ключ ЭЦП и секретный ключ имитозащиты должны быть отнесены {УД.2} к критическим объектам, а открытый ключ ЭЦП и долговременные параметры — {УД.2} к открытым объектам. Длина имитовставки в битах должна быть не меньше 64.

Входные данные:

a) список криптографических алгоритмов;

b) список объектов;

c) криптографические методы контроля целостности и подлинности;

d) соответствие «объекты — методы защиты»;

e) исходные тексты программных реализаций криптографических методов контроля целостности;

f) компоненты СКЗИ, реализующие криптографические методы контроля целостности;

g) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ЗО.4-1. Для каждого метода из списка [c] эксперт проверяет, что:

1 Метод основан на алгоритмах ЭЦП или имитозащиты из списка [a].

2 Используемые в методе личные и секретные ключи алгоритмов включены в список [b] и отнесены к критическим объектам.

3 Используемые в методе открытые ключи и долговременные параметры алгоритмов включены в список [b] и отнесены к открытым объектам.

4 Если метод основан на алгоритме имитозащиты, то длина имитовставки в битах не меньше 64.

ЗО.4-2. Эксперт проводит выборочный (если уровень [g] равен 2) или подробный (если уровень [g] равен 3 или 4) анализ исходных текстов [e] и (или), соответственно, выборочное или подробное тестирование компонентов [f] и проверяет корректность реализации методов из списка [c].

Примечание — Корректность реализации {АП.3} криптографических алгоритмов на этом шаге не проверяется. Проверка корректности выполняется на шаге КП.1-3.

Эксперт ДОЛЖЕН проверить следующие аспекты реализаций методов:

1 Все вызовы криптографических алгоритмов [a] корректны. Это означает, что при вызовах алгоритмов правильно указываются их входные данные, а после вызовов правильно обрабатываются возвращаемые результаты.

2 Методы действительно применяются для защиты объектов в соответствии с [d].

Требование ЗО.5 (1–4). Должны быть определены и корректно использованы аппаратные методы защиты. Устройства, которые реализуют аппаратные методы, должны соответствовать ТНПА в части физической безопасности. При отсутствии подходящих ТНПА должна быть проведена оценка надежности устройств.

Примечание 2 — При оценке надежности следует учитывать требования пакета ФБ (п. 5.7), декларации разработчиков устройств, сведения о применении устройств, опыт применения.

Входные данные:

a) аппаратные методы защиты;

b) соответствие «объекты — методы защиты»;

c) исходные тексты программных вызовов аппаратных методов защиты;

d) заключения о соответствии устройств, реализующих аппаратные методы защиты, ТНПА в части физической безопасности (при наличии);

e) свидетельства о надежности устройств, реализующих аппаратные методы защиты (при наличии);

f) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Примечание — На сегодняшний день в республике отсутствуют ТНПА, определяющие требования физической безопасности к средствам аппаратной защиты. Поэтому заключения [e] в ближайшие годы будут отсутствовать. Тем не менее, для оценки надежности устройств эксперт может использовать дополнительные свидетельства [f] в соответствии с примечанием к требованию.

Действия эксперта:

ЗО.5-1. Эксперт проверяет, что для каждого устройства, реализующего методы из списка [a], имеется заключение [d] о соответствии ТНПА.

Если такое заключение отсутствует, то эксперт ДОЛЖЕН провести оценку надежности устройств. При оценке надежности эксперт использует:

– требования пакета ФБ (п. 5.7) Стандарта;

– свидетельства [e] разработчиков устройств;

– свидетельства [e] разработчика СКЗИ, применяющего устройства;

– свидетельства [e] из открытых источников, в том числе данные о применении устройств в различных системах защиты информации.

Устройства признаются надежными, если:

1 Нарушитель с высоким потенциалом атаки не может раскрыть содержимое защищаемых критических объектов.

2 Нарушитель с высоким потенциалом атаки не может модифицировать защищаемые открытые и критические объекты без срабатывания механизмов контроля.

3 Вероятность не обнаружить случайную модификацию объекта при его хранении не превышает 2^{-32}.

ЗО.5-2. Эксперт проводит выборочный (если уровень [g] равен 2) или подробный (если уровень [g] равен 3 или 4) анализ исходных текстов [c] и проверяет корректность использования методов из списка [a].

Эксперт ДОЛЖЕН проверить следующие аспекты реализаций методов:

1 Все вызовы методов [a] корректны. Это означает, что при вызовах правильно указываются входные данные, а после вызовов правильно обрабатываются возвращаемые результаты.

2 Методы действительно применяются для защиты объектов в соответствии с [b].

Требование ЗО.6 (1–4). Должны быть определены и корректно реализованы {АП.3, АП.4, АП.5} методы разделения секрета. При восстановлении критического объекта должно использоваться не менее двух различных частичных секретов. Если для восстановления критического объекта требуется k частичных секретов, то любые $k-1$ частичных секретов не должны давать никакой информации об исходном объекте. Частичные секреты должны быть отнесены {УД.2} к критическим объектам.

Примечание 3 — Владельцы частичных секретов не обязательно различны. Один оператор может владеть сразу всеми частичными секретами.

Входные данные:

a) список криптографических алгоритмов;
b) список объектов;
c) методы разделения секрета;
d) соответствие «объекты — методы защиты»;
e) исходные тексты программных реализаций методов разделения секретов;
f) компоненты СКЗИ, реализующие методы разделения секретов;
g) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ЗО.6-1. Для каждого метода из списка [c] эксперт проверяет, что:

1 Метод основан на алгоритме разделения секрета из списка [a], либо определен в документации разработчика в однозначном виде.

2 В методе используются не менее двух частичных секретов.

3 Если для восстановления критического объекта требуется k частичных секретов, то любые $k-1$ частичных секретов не дают никакой информации об исходном объекте.

Примечание — Невозможность восстановления критического объекта по частичным секретам, число которых меньше определенного порога, называется совершенностью. Если метод разделения секрета основан на алгоритмах из ТНПА, то эксперт проверяет, что ТНПА содержит утверждение о совершенности алгоритмов. Если метод разделения секрета предложен разработчиком,

то эксперт проверяет обоснование совершенности разработчика. При обосновании разработчик может сослаться на литературу, если используется известный алгоритм, не описанный в ТНПА.

4 Частичные секреты включены в список [b] и отнесены к критическим объектам.

ЗО.6-2. Эксперт проводит выборочный (если уровень [g] равен 2) или подробный (если уровень [g] равен 3 или 4) анализ исходных текстов [e] и (или), соответственно, выборочное или подробное тестирование компонентов [f] и проверяет корректность реализации методов из списка [c].

Эксперт ДОЛЖЕН проверить следующие аспекты реализаций методов:

1 Если метод основан на стандартных алгоритмах разделения секрета из списка [a], то все вызовы алгоритмов корректны. Это означает, что при вызовах алгоритмов правильно указываются их входные данные, а после вызовов правильно обрабатываются возвращаемые результаты.

2 Методы действительно применяются для защиты объектов в соответствии с [d].

Если метод основан на алгоритмах разработчика, то эксперт ДОЛЖЕН провести полный анализ исходных текстов [e] соответствующих программных реализаций.

Требование ЗО.7 (1–4). Должны быть определены и корректно реализованы {АП.4, АП.5} алгоритмические методы контроля целостности. Алгоритмические методы контроля должны гарантировать, что

– вероятность необнаружения случайной модификации контролируемого объекта при его хранении не превышает 2^{-32};

– вероятность необнаружения намеренной модификации контролируемого объекта при его импорте не превышает 2^{-128}.

Если контролируемый объект не является частичным секретом или системным объектом, то его контрольная характеристика должна быть отнесена {УД.2} к открытым или критическим объектам.

Входные данные:

a) список криптографических алгоритмов;

b) список объектов;

c) алгоритмические методы контроля целостности;

d) соответствие «объекты — методы защиты»;

e) исходные тексты программных реализаций алгоритмических методов контроля целостности;

f) компоненты СКЗИ, реализующие алгоритмические методы контроля целостности;

g) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ЗО.7-1. Для каждого метода из списка [c] эксперт проверяет, что:

1 Метод основан на бесключевых алгоритмах из списка [a] или на некриптографических алгоритмах, определенных в документации разработчика или в некотором ТНПА.

2 Длина контрольной характеристики (в битах), используемой для обнаружения случайной модификации контролируемого объета при его хранении, не меньше 32.

3 Длина контрольной характеристики (в битах), используемой для обнаружения намеренной модификации контролируемого объета при его экспорте, не меньше 128.

4 Если метод основан на алгоритме разработчика, то эксперт проверяет, что различные контрольные характеристики, вычисляемые с помощью этого алгоритма, встречаются примерно с равными частотами.

Примечание — Эксперт анализирует обоснование алгоритма, представленное разработчиком, и проверяет, что в алгоритме отсутствуют композиционные элементы, приводящие к значимой неравновероятности выходных значений. При обосновании разработчик может сослаться на литературу, если используется известный алгоритм, не описанный в ТНПА.

Пример — Эксперт должен забраковать алгоритм вычисления контрольной суммы, состоящий в разбиении входного слова на блоки длины n и в последующем перемножении этих блоков как чисел по модулю 2^n. Действительно, в результате умножения четные числа будут встречаться с гораздо большими вероятностями, чем нечетные.

5 Если контролируемый объект не является частичным секретом или системным объектом, то его контрольная характеристика включена в список [b] и отнесена к открытым или критическим объектам.

ЗО.7-2. Эксперт проводит выборочный (если уровень [g] равен 2) или подробный (если уровень [g] равен 3 или 4) анализ исходных текстов [e] и (или), соответственно, выборочное или подробное тестирование компонентов [f] и проверяет корректность реализации методов из списка [c].

Эксперт ДОЛЖЕН проверить следующие аспекты реализаций методов:

1 Если метод основан на бесключевых криптографических алгоритмах из списка [a], то все вызовы алгоритмов корректны. Это означает, что при вызовах алгоритмов правильно указываются их входные данные, а после вызовов правильно обрабатываются возвращаемые результаты.

2 Методы действительно применяются для защиты объектов в соответствии с [d].

Если метод основан на некриптографических алгоритмах, не включенных в список [a], то эксперт ДОЛЖЕН провести полный анализ исходных текстов соответствующих программных реализаций.

Требование ЗО.8 (1–4). Должны быть определены и изложены {РД.1, РД.2} в руководствах организационные меры обеспечения конфиденциальности частичных секретов. Меры должны быть направлены на ограничение физического доступа к носителям информации, на которых хранятся секреты, и противодействие попаданию порогового числа частичных секретов противнику.

Входные данные:

a) организационные меры обеспечения конфиденциальности;

b) соответствие «объекты — методы защиты»;

c) список руководств.

Действия эксперта:

ЗО.8-1. Эксперт проверяет, что методы [a] обеспечивают ограничение физического доступа к информации и препятствуют попаданию порогового числа частичных секретов противнику.

ЗО.8-2. Эксперт проверяет, что методы [a] отражены в руководствах [c] в виде инструкций оператору. Эксперт проверяет, что инструкции соответствуют [b].

Требование ЗО.9 (1–4). При записи на хранение и экспорте критических объектов должна устанавливаться их защита [ЗО.1].

Примечание 4 — Экспорт и импорт могут проводиться в рамках онлайн-взаимодействия с удаленным оператором. При использовании криптографических методов ключи защиты могут генерироваться с помощью протоколов формирования общего ключа [КП.3].

Входные данные:

a) список объектов;
b) описание политики управления доступом;
c) соответствие «объекты — методы защиты»;
d) исходные тексты программных реализаций механизмов управления доступом;
e) компоненты СКЗИ, реализующие механизмы управления доступом;
f) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ЗО.9-1. Эксперт анализирует списки [a, b] и находит случаи записи на хранение и экспорта критических объектов.

ЗО.9-2. Эксперт проводит выборочный (если уровень [f] равен 1 или 2) или подробный (если уровень [f] равен 3 или 4) анализ исходных текстов [d] и (или), соответственно, выборочное или подробное тестирование компонентов [e] и проверяет, что в случаях, найденных на шаге ЗО.9-1, применяются методы защиты в соответствии с [c].

Требование ЗО.10 (1–4). При чтении во время хранения и импорте критических и открытых объектов должен проводиться контроль их целостности и подлинности [ЗО.2]. При ошибке контроля использование объекта должно быть запрещено.

Входные данные:

a) список объектов;
b) описание политики управления доступом;
c) соответствие «объекты — методы защиты»;
d) исходные тексты программных реализаций механизмов управления доступом;
e) компоненты СКЗИ, реализующие механизмы управления доступом;
f) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ЗО.10-1. Эксперт анализирует списки [a, b] и находит случаи чтения во время хранения и импорта открытых и критических объектов.

ЗО.10-2. Эксперт проводит выборочный (если уровень [f] равен 1 или 2) или подробный (если уровень [f] равен 3 или 4) анализ исходных текстов [d] и (или), соответственно, выборочное или подробное тестирование компонентов [e] и проверяет, что в случаях, найденных на шаге ЗО.10-1, применяются методы защиты в соответствии с [c]. Эксперт проверяет также, что при ошибке контроля целостности использование объекта запрещено.

Требование ЗО.11 (1–4). Контроль целостности системных объектов [ЗО.2] должен проводиться {СТ.3} при самотестировании.

Действия эксперта: проверка ЗО.11 покрывается проверками по СТ.3.

Требование ЗО.12 (1–4). Все сеансовые критические объекты [УД.2] должны очищаться до завершения сеансов.

Входные данные:

a) методы очистки критических объектов;
b) исходные тексты программ очистки критических объектов;
c) исходные тексты программ СКЗИ;
d) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ЗО.12-1. Эксперт оценивает надежность методов очистки [a]. Методы считаются надежными, если после очистки критических объектов нарушитель не сможет восстановить (полностью или частично) значения объектов.

ЗО.12-2. Эксперт проводит полный анализ исходных текстов [b] и проверяет корректность реализации методов из списка [a].

ЗО.12-3. Эксперт проводит выборочный (если уровень [d] равен 1 или 2) или подробный (если уровень [d] равен 3 или 4) анализ исходных текстов [c] и проверяет, что очистка критических сеансовых объектов выполняется до завершения сеансов.

Требование ЗО.13 (1–4). Очистка долговременных и сеансовых критических объектов [УД.2] должна быть реализована так, чтобы после очистки нельзя было определить первоначальное значение объекта.

Действия эксперта: проверка ЗО.13 покрывается проверками по зО.12.

Требование ЗО.14 (1–4). Экспорт неизвлекаемых объектов [УД.2] должен быть либо полностью запрещен, либо применяться исключительно для резервного сохранения и выполняться с помощью методов разделения секрета.

Действия эксперта: проверка ЗО.14 покрывается проверками по УД.2.

Требование ЗО.15 (1). Должны быть определены и корректно использованы системные методы защиты. Применение системных методов должно быть поддержано {НС.2} при настройке системной среды. Перед применением системного метода к критическому объекту [УД.2] он должен быть зашифрован на ключе, построенному по паролю владельца. Для шифрования и построения ключа должны использоваться криптографические алгоритмы из перечня [КП.1].

Входные данные:

a) список объектов;
b) системные методы защиты;
c) список криптографических алгоритмов;
d) соответствие «объекты — методы защиты»;
e) криптографическая граница;

f) исходные тексты программных реализаций криптографических методов, применяемых при использовании системных методов защиты;

g) компоненты СКЗИ, реализующие системные методы защиты;

h) список руководств.

Действия эксперта:

ЗО.15-1. Для каждого метода из списка [b] эксперт проверяет, что:

1 Метод состоит в обеспечении конфиденциальности и (или) контроле целостности объектов [a], которые хранятся в пределах границы [e], средствами системной среды.

2 Для метода в руководствах [h] приведено описание настроек системной среды.

3 Перед применением метода к критическому объекту из списка [a] в соответствии с [d] предусмотрено зашифрование объекта на ключе, построенному по паролю владельца.

4 Для шифрования и построения ключа в соответствии с [d] используется криптографический алгоритм из списка [c].

ЗО.15-2. Эксперт проводит выборочное тестирование компонентов [g] и проверяет корректность использования методов из списка [d]. Корректность использования означает, что методы действительно применяются для защиты объектов [a] в соответствии с [b].

ЗО.15-3. Эксперт проводит выборочный анализ исходных текстов [f] и проверяет корректность реализации криптографических методов из списка [d].

При проверке эксперт использует результаты проверки по [ЗО.3].

6.5 Проверка требований по самотестированию

Требование СТ.1 (1–4). Должен быть определен перечень КСК.

Входные данные:

a) криптографическая граница;

b) список объектов;

c) список критических системных компонентов;

d) описание генераторов случайных чисел.

Действия эксперта:

СТ.1-1. Эксперт проверяет, что в список [c] включено все аппаратное и программное обеспечение общего назначения, которое находится внутри криптографической границы [a] и используется для передачи, обработки и хранения объектов [b].

Эксперт ДОЛЖЕН проверить, что в список включены следующие типы компонентов:

1 Устройства ввода/вывода.

2 Устройства обработки и передачи (например, процессор, физические интерфейсы).

3 Устройства хранения (например, жесткий диск).

4 Службы операционной системы, влияющие на безопасность СКЗИ.

5 Генераторы случайных чисел из списка [d].

Примечание — Допускается представление КСК в виде крупных функциональных блоков (устройства ввода, управления, обработки, хранения), без излишней детализации. При определении таких блоков должно быть, в первую очередь, учтено их функциональное назначение (для хранения, для обработки данных), а не физические параметры или расположение.

Требование СТ.2 (1–4). Сразу после включения СКЗИ должно проверять состав и работоспособность КСК [СТ.1].

Примечание 1 — Для некоторых компонентов при включении можно провести лишь часть проверок. В таких случаях разрешается выполнить пропущенные тесты позднее. Например, при включении следует проверить наличие устройства чтения смарт-карт, а корректность работы данного устройства можно проверить при непосредственном чтении данных с карты.

Входные данные:

a) список критических системных компонентов;

b) проверка работоспособности критических системных компонентов;

c) исходные тексты программных реализаций механизмов проверки работоспособности;

d) компоненты СКЗИ, реализующие механизмы проверки работоспособности;

e) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

СТ.2-1. Эксперт проверяет полноту проверок из спецификации [b]. Тесты должны выявлять отсутствие и неверное функционирование всех компонентов из списка [a].

СТ.2-2. Эксперт проводит выборочный (если уровень [e] равен 1 или 2) или подробный (если уровень [e] равен 3 или 4) анализ исходных текстов [c] и (или), соответственно, выборочное или подробное тестирование компонентов [d] и проверяет, что проверки [b] корректно реализованы и действительно применяются.

Требование СТ.3 (1–4). Должны быть определены и корректно реализованы {АП.4, АП.5} тесты работоспособности СКЗИ. Перечень тестов должен включать:

– тесты криптографических алгоритмов [КП.1];

– контроль целостности всех системных объектов, включая файлы программ [ЗО.11].

Должны быть предусмотрены {РС.1} сервисы тестирования, реализующие тесты перечня. Любой оператор должен иметь {УД.3} доступ к сервисам тестирования. Кроме этого, каждый криптографический алгоритм должен быть автоматически протестирован перед первым использованием. Целостность системных объектов должна быть проверена сразу после включения СКЗИ.

Примечание 2 — Если имеется несколько реализаций криптографического алгоритма, то тестироваться должна каждая из них.

Входные данные:

a) список криптографических алгоритмов;

b) список сервисов;

c) список объектов;

d) перечень проверок самотестирования;

e) описание генераторов случайных чисел;

f) описание политики управления доступом;

g) исходные тексты программных реализаций механизмов самотестирования;

h) компоненты СКЗИ, реализующие самотестирование;

i) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

СТ.3-1. Эксперт проводит анализ перечня [d] и проверяет выполнение следующих условий:

1 В [d] имеются тесты для всех криптографических алгоритмов из списка [a].

2 В [d] включена проверка целостности всех системных объектов из списка [c].

3 В [d] включено статистическое тестирование генераторов случайных чисел из списка [e].

4 В [d] предусмотрено выполнение перечисленных тестов в сервисах самотестирования из списка [b].

5 В соответствии с [f], любой оператор имеет доступ к сервисам тестирования из списка [b].

6 В [d] предусмотрено выполнение тестов каждой реализации криптографических алгоритмов из списка [a] автоматически перед первым использованием.

7 В [d] предусмотрено выполнение статистических тестов генераторов случайных чисел из списка [e] перед первым использованием.

8 В [d] предусмотрено выполнение тестов проверки целостности системных объектов из списка [c] сразу после включения СКЗИ.

Примечание 1 — Сервисы самотестирования выполняются по запросу оператора. Проверка наличия и корректности реализации сервисов покрывается проверками по РС.1, РС.2.

Примечание 2 — Корректность тестов криптографических алгоритмов, тестов целостности системных объектов и тестов для генераторов случайных чисел на этом шаге не проверяется. Проверка корректности выполняется на шагах КП.1-4, ЗО.7-1, СЧ.5-2.

СТ.3-2. Эксперт проводит выборочный (если уровень [i] равен 1 или 2) или подробный (если уровень [i] равен 3 или 4) анализ исходных текстов [g] и (или), соответственно, выборочное или подробное тестирование компонентов [h] и проверяет, что проверки из перечня [d] действительно применяются в необходимых случаях.

Примечание — Корректность реализации тестов криптографических алгоритмов, тестов целостности системных объектов и тестов для генераторов случайных чисел не проводится на этом шаге. Проверка корректности реализации тестов выполняется на шагах КП.1-5, ЗО.7-2, СЧ.5-4.

Требование СТ.4 (1–4). Тестовые данные криптографических алгоритмов [КП.1] (ключи, открытые тексты, шифртексты) должны быть отнесены {УД.2} к открытым объектам.

Действия эксперта: проверка СТ.4 покрывается проверками по УД.2.

Требование СТ.5 (1–4). При ошибках тестирования СКЗИ должно переходить {УД.4} в состояние блокировки [УД.6].

Действия эксперта: проверка СТ.5 покрывается проверками по УД.4.

Требование СТ.6 (3, 4). Если СКЗИ может эксплуатироваться без выключения в течение длительного интервала времени, то должно быть предусмотрено периодическое автоматическое выполнение тестов [СТ.3]. Настройка перечня тестов и интервала тестирования должна быть доступна {УД.3} только администраторам [УД.1].

Примечание 3 — Если в назначенный для тестов момент СКЗИ выполняет операцию, которая не может быть прервана, то самотестирование может быть перенесено на более поздний срок или не проведено вовсе.

Входные данные:

a) основные функциональные возможности;

b) перечень проверок самотестирования;

c) список криптографических алгоритмов;

d) описание политики управления доступом;

e) описание генераторов случайных чисел;

f) список объектов;

g) список сервисов;

h) исходные тексты программных реализаций механизма периодического самотестирования;

i) компоненты СКЗИ, реализующие периодическое самотестирование.

Действия эксперта:

СТ.6-1. Эксперт проводит анализ описания [a]. Если в соответствии с описанием [a] СКЗИ может эксплуатироваться без выключения в течение длительного интервала времени, то эксперт проводит анализ перечня [b] и проверяет выполнение следующих условий:

1 В [b] имеются тесты для всех криптографических алгоритмов из списка [c].

2 В [b] включена проверка целостности всех системных объектов из списка [f].

3 В [b] включено тестирование генераторов случайных чисел из списка [e].

4 В [b] предусмотрено периодическое автоматическое выполнение перечисленных тестов в сервисе периодического самотестирования из списка [g].

5 В [b] и [g] предусмотрена настройка перечня тестов и интервала тестирования.

6 В соответствии с [d], настройка перечня тестов и интервала тестирования доступна только администратору.

7 В соответствии с [b] и [g], если в назначенный для тестов момент СКЗИ выполняет операцию, которая не может быть прервана, то самотестирование переносится на более поздний срок или не проводится вовсе.

СТ.6-2. Эксперт подробный анализ исходных текстов [h] и (или) подробное тестирование компонентов [i] и проверяет, что периодическое автоматическое выполнение тестов из перечня [b] действительно применяется в необходимых случаях.

Примечание — Проверка наличия и корректности реализации сервиса периодического самотестирования покрывается проверками по РС.1, РС.2.

6.6 Проверка требований по аудиту

Требование АУ.1 (3, 4). Должна быть реализована регистрация событий безопасности в журнале аудита. Журнал должен быть отнесен {УД.2} к объектам администратора.

Входные данные:

a) список объектов;

b) исходные тексты программ СКЗИ;

c) компоненты СКЗИ, обеспечивающие просмотр журнала аудита.

Действия эксперта:

АУ.1-1. Эксперт проверяет, что список [a] содержит журнал аудита, владельцем которого является администратор.

Эксперт использует результаты проверок по УД.2.

АУ.1-2. Эксперт проводит подробный анализ исходных текстов [b] или подробное тестирование компонентов [c] и проверяет, что в СКЗИ действительно реализовано ведение журнала аудита.

Требование АУ.2 (3, 4). В перечень регистрируемых событий должны быть включены:

– включение и выключение СКЗИ [УД.4];

– управление ролью «Администраторы» [УД.1]: добавление и исключение операторов;

– изменение, экспорт, импорт критических объектов [УД.2];

– изменение системных объектов [УД.2];

– некорректные входные данные сервисов администраторов [РС.3];

– переход в состояние блокировки [УД.6].

Примечание 1 — Если журнал аудита отнесен к критическим объектам администратора, то операции над ним входят в перечень регистрируемых событий.

Входные данные:

a) перечень регистрируемых событий;

b) список ролей операторов;

c) список объектов;

d) список сервисов;

e) исходные тексты программных реализаций регистрации событий в журнале аудита;

f) компоненты СКЗИ, реализующие регистрацию событий в журнале аудита.

Действия эксперта:

АУ.2-1. Эксперт проводит анализ перечня [a] и определяет список событий, регистрируемых в журнале аудита.

Эксперт ДОЛЖЕН проверить, что перечнь [a] содержит следующие события:

– Включение и выключение СКЗИ;

– Управление ролью «Администраторы» из списка [b]: добавление и исключение операторов;

– Изменение, экспорт, импорт критических объектов из списка [c];

– Изменение системных объектов из списка [c];
– Некорректные входные данные сервисов администраторов из списка [d];
– Переход в состояние блокировки.

Если журнал аудита отнесен к критическим объектам администратора [c], то эксперт ДОЛЖЕН проверить, что перечнь [a] содержит операции над журналом аудита.

АУ.2-2. Эксперт проводит подробный анализ исходных текстов [e] или подробное тестирование компонентов [f] и проверяет, что в журнале аудита регистрируются события в соответствии с [a].

Требование АУ.3 (3, 4). Записи аудита должны содержать следующую информацию:
– дата и время события;
– тип события;
– идентификатор оператора (если проведена аутентификация);
– результат (успех или неудача) события;
– подробности в зависимости от типа события: объект и операция над ним, вид сбоя при переходе в состояние блокировки, описание некорректных входных данных сервисов, другое.

В записях аудита не должны дублироваться значения критических объектов.

Примечание 2 — Если СКЗИ не располагает таймером, то могут быть указаны примерные дата и время или даже просто номер события. В одну запись аудита разрешено помещать информацию сразу о нескольких событиях.

Входные данные:
a) структура записей аудита;
b) список объектов;
c) исходные тексты программных реализаций регистрации событий в журнале аудита;
d) компоненты СКЗИ, реализующие регистрацию событий в журнале аудита.

Действия эксперта:

АУ.3-1. Эксперт проводит анализ структуры [a] и проверяет, что она содержит следующую информацию:

1 Дата и время события.

Примечание — Если СКЗИ не располагает таймером, то могут быть указаны примерные дата и время или даже просто номер события.

2 Тип события.

3 Идентификатор оператора (если проведена аутентификация).

4 Результат (успех или неудача) события.

5 Подробности в зависимости от типа события: объект и операция над ним, вид сбоя при переходе в состояние блокировки, описание некорректных входных данных сервисов, другое.

Примечание — В одну запись аудита может быть помещена информация сразу о нескольких событиях.

АУ.3-2. Эксперт проводит подробный анализ исходных текстов [c] или подробное тестирование компонентов [d] и проверяет, что события регистрируются в журнале аудита

в соответствии с [a], в записях аудита не дублируются значения критических объектов из списка [b].

Требование АУ.4 (3, 4). Должен быть определен порог числа записей журнала аудита. При превышении порога должны быть предприняты действия, направленные на сохранение приемлемого размера журнала и минимизацию потерь информации аудита.

Примечание 3 — Примеры действий:

СКЗИ переводится в состояние блокировки, из которого затем выводится администратором после просмотра и удаления записей аудита;

– – старые записи о включении, выключении и других штатных событиях удаляются автоматически.

Для снижения потерь при автоматическом удалении записей администраторы могут заранее предупреждаться о приближении к порогу.

Входные данные:

a) обработка переполнения журнала аудита;

b) исходные тексты программных реализаций, обеспечивающих обработку переполнения журнала аудита;

c) компоненты СКЗИ, реализующие обработку переполнения журнала аудита.

Действия эксперта:

АУ.4-1. Эксперт проводит анализ правил [a] и проверяет выполнение следующих условий:

1 В правилах [a] определен порог числа записей журнала аудита.

2 В соответствии с правилами [a] превышение порога числа записей журнала аудита обрабатывается одним из следующих методов:

– СКЗИ переводится в состояние блокировки, из которого затем выводится администратором после просмотра и удаления записей аудита;

– старые записи о включении, выключении и других штатных событиях удаляются автоматически;

– предпринимаются другие действия, направленные на сохранение приемлемого размера журнала и минимизацию потерь информации аудита.

Если в правилах [a] предусмотрено автоматическое удаление записей журнала аудита, Эксперт МОЖЕТ проверить, что в соответствии с правилами [a] администратор заранее предупреждается о приближении к порогу.

АУ.4-2. Эксперт проводит подробный анализ исходных текстов [b] или подробное тестирование компонентов [c] и проверяет, что в СКЗИ действительно обрабатывается переполнение журнала аудита в соответствии с [a].

Требование АУ.5 (3, 4). Если в СКЗИ реализованы сервисы настройки порога числа записей и предпринимаемых при превышении порога действий, то данные сервисы должны быть доступны {УД.3} только администраторам.

Действия эксперта: проверка [АУ.5] покрывается проверками по [УД.3].

6.7 Проверка требований по физической безопасности

Требование ФБ.1 (3, 4). Должны быть определены и корректно реализованы механизмы физической защиты СКЗИ.

Входные данные:

a) механизмы физической защиты;

b) криптографическая граница;

c) компоненты СКЗИ, обеспечивающие механизмы физической защиты.

Действия эксперта:

ФБ.1-1. Эксперт проводит анализ описания [a] и определяет перечень механизмов физической защиты СКЗИ.

Эксперт ДОЛЖЕН проверить, что описание [a] включает механизмы физической защиты, которые направлены на защиту от несанкционированного физического доступа к компонентам внутри криптографической границы [b] и предотвращение несанкционированного использования или модификации СКЗИ.

ФБ.1-2. Эксперт проводит подробное тестирование компонентов [b] и проверяет, что в СКЗИ действительно реализованы механизмы физической защиты в соответствии с [a].

Требование ФБ.2 (3, 4). Аппаратные КСК должны быть изготовлены в условиях серийного производства в соответствии с техническими стандартами, согласно технической документации (техническим условиям).

Входные данные:

a) список критических системных компонентов;

b) механизмы физической защиты;

c) описания программ и аппаратных компонентов (только описание аппаратных компонентов).

Действия эксперта:

ФБ.2-1. Эксперт проводит анализ списка [a] и определяет перечень аппаратных КСК.

Эксперт проводит анализ описаний [b] и [c] и проверяет, что для аппаратных КСК из списка [a] выполняются следующие условия:

1 В описаниях [b], [c] для каждого аппаратного КСК [b] указан его производитель.

2 В описаниях [b], [c] для каждого аппаратного КСК [b] указаны технические стандарты, которым он соответствует или в соответствии с которыми он произведен.

3 В описаниях [b], [c] для каждого аппаратного КСК [b] дана ссылка на техническую документацию или технические условия, в соответствии с которыми он произведен.

Требование ФБ.3 (3, 4). СКЗИ должен быть выполнен в виде аппаратного устройства с твердым непрозрачным корпусом и (или) покрытием. Визуальный осмотр СКЗИ не должен давать дополнительную по отношению к конструкторской документации [ПР.1] информацию о КСК, а также информацию об их текущем состоянии и выполняемых ими операциях.

Входные данные:

a) механизмы физической защиты;

b) список критических системных компонентов;

c) описания программ и аппаратных компонентов (только описание аппаратных компонентов);

d) опытный образец СКЗИ.

Действия эксперта:

ФБ.3-1. Эксперт проводит анализ описаний [a] и [c] и проверяет, что СКЗИ выполнено в виде аппаратного устройства с твердым непрозрачным корпусом и (или) покрытием.

ФБ.3-2. Эксперт проводит подробное тестирование образца [d] и проверяет, что СКЗИ действительно выполнено в соответствии с [a] и [c], и что визуальный осмотр СКЗИ не дает дополнительную по отношению к [c] информацию о КСК [b], а также информацию об их текущем состоянии и выполняемых ими операциях.

Требование ФБ.4 (3, 4). При попытке физического доступа к компонентам внутри криптографической границы СКЗИ механизмы физической защиты [ФБ.1] должны обеспечивать обнаружение доступа.

Входные данные:

a) механизмы физической защиты;

b) криптографическая граница;

c) описания программ и аппаратных компонентов (только описание аппаратных компонентов);

d) компоненты СКЗИ, обеспечивающие механизмы физической защиты.

Действия эксперта:

ФБ.4-1. Эксперт проводит анализ описаний [a] и [c] и проверяет, что при попытке физического доступа к компонентам внутри границы [b] механизмы физической защиты [a] обеспечивают обнаружение доступа.

ФБ.4-2. Эксперт проводит подробное тестирование компонентов [d] и проверяет, что они действительно обеспечивают обнаружение попыток несанкционированного доступа в соответствии с [a].

Требование ФБ.5 (3, 4). Если в СКЗИ для обнаружения доступа к компонентам внутри криптографической границы предусмотрены печати, пломбы или иные подобные элементы, то

– они должны иметь уникальные номера или идентификаторы;

– они должны сохранять конструкцию и внешний вид при эксплуатации СКЗИ в допустимых диапазонах параметров эксплуатации [ЗВ.1];

– условия и порядок их установки и/или замены, а также контроля должны быть определены {РД.1, РД.2} в руководствах.

Входные данные:

a) механизмы физической защиты;

b) допустимые границы температуры, напряжения и др.;

c) список руководств;

d) опытный образец СКЗИ.

Действия эксперта:

ФБ.5-1. Эксперт проводит анализ описания [a] и проверяет, предусмотрено ли использование для обнаружения доступа к компонентам внутри криптографической границы печатей, пломб или иных подобных элементов.

Если предусмотрено, эксперт ДОЛЖЕН проверить, что выполняются следующие условия:

1 В соответствии с описанием [a] в механизмах пломбирования предусмотрено использование средств, которые имеют уникальные номера или идентификаторы.

2 В соответствии с описанием [a] используемые печати, пломбы или иные подобные элементы сохраняют конструкцию и внешний вид при эксплуатации СКЗИ в условиях [b].

3 В руководствах [c] представлены условия и порядок установки и (или) замены, а также контроля в соответствии с [a] печатей, пломб или иных подобных элементов.

ФБ.5-2. Эксперт проводит подробное тестирование образца [d] и проверяет, что пломбирование в нем выполнено в соответствии с [a].

Требование ФБ.6 (4). Механизмы физической защиты [ФБ.1] должны обеспечивать защиту от несанкционированного доступа к компонентам внутри криптографической границы СКЗИ. Должны использоваться несъемный корпус (покрытие) [ФБ.3] и (или) активные методы защиты с помощью датчиков контроля доступа.

Входные данные:

a) механизмы физической защиты;
b) криптографическая граница;
c) опытный образец СКЗИ.

Действия эксперта:

ФБ.6-1. Эксперт проводит анализ описания [a] и проверяет, что для защиты от несанкционированного доступа к компонентам внутри границы [b] используется несъемный корпус (покрытие) и (или) активные методы защиты с помощью датчиков контроля доступа.

ФБ.6-2. Эксперт проводит подробное тестирование образца [c] и проверяет, что в нем действительно используется несъемный корпус (покрытие) и (или) активные методы защиты с помощью датчиков контроля доступа в соответствии с [a].

Требование ФБ.7 (4). При срабатывании датчиков контроля доступа СКЗИ должно переходить в состояние полной блокировки [УД.9]. Переход должен выполняться как при включенном электропитании СКЗИ, так и отключенном.

Входные данные:

a) механизмы физической защиты;
b) действия при срабатывании механизмов контроля доступа;
c) исходные тексты программ, обеспечивающих обработку состояния датчиков контроля доступа (при наличии);
d) опытный образец СКЗИ.

Действия эксперта:

ФБ.7-1. Эксперт проводит анализ описания [a] и проверяет, предусмотрено ли в [a] использование активных методов защиты с помощью датчиков контроля доступа.

Если предусмотрено, эксперт ДОЛЖЕН проверить, что в соответствии с [b] при срабатывании датчиков контроля доступа СКЗИ переходит в состояние полной блокировки как при включенном, так и отключенном электропитании СКЗИ.

ФБ.7-2. Эксперт проводит подробный анализ исходных текстов [c] или подробное тестирование образца [d] и проверяет, что в нем механизмы защиты при срабатывании датчиков контроля доступа действительно реализованы в соответствии с [b].

Требование ФБ.8 (4). Тип датчиков контроля доступа, их количество, места размещения, порядок функционирования должны выбираться таким образом, чтобы была исключена возможность доступа к компонентам внутри криптографической границы СКЗИ без срабатывания датчиков.

Входные данные:

a) механизмы физической защиты;

b) действия при срабатывании механизмов контроля доступа;

c) криптографическая граница;

d) описания программ и аппаратных компонентов (только описание аппаратных компонентов);

e) опытный образец СКЗИ.

Действия эксперта:

ФБ.8-1. Эксперт проводит анализ описания [a] и проверяет, предусмотрено ли в [a] использование активных методов защиты с помощью датчиков контроля доступа.

Если предусмотрено, эксперт проводит анализ описаний [a], [b], [c] и определяет тип датчиков контроля доступа, их количество, места размещения, порядок функционирования.

ФБ.8-2. Эксперт проводит подробное тестирование образца [e] и проверяет, что выполняются следующие условия:

1 Тип датчиков контроля доступа, их количество, места размещения, порядок функционирования соответствуют описаниям [a], [b], [c].

2 Тип датчиков контроля доступа, их количество, места размещения, порядок функционирования исключают возможность доступа к компонентам внутри границы [c] без срабатывания датчиков.

Примечание — При тестировании возможности доступа к компонентам внутри границы [c] эксперт МОЖЕТ использовать доступные технические средства и вредоносные программы согласно потенциалу противника для 4 уровня безопасности СКЗИ в соответствием со Стандартом.

Требование ФБ.9 (4). Должна быть предусмотрена защита от непроизвольного срабатывания датчиков контроля доступа. Оценка вероятности непроизвольного срабатывания, а также способ защиты от него должны быть приведены {ФБ.1} в описании механизмов физической защиты СКЗИ.

Входные данные:

a) механизмы физической защиты.

Действия эксперта:

ФБ.9-1. Эксперт проводит анализ описания [a] и проверяет, предусмотрено ли в [a] использование активных методов защиты с помощью датчиков контроля доступа.

Если предусмотрено, эксперт проверяет, содержит ли описание [a] оценку вероятности непроизвольного срабатывания датчиков контроля доступа, а также способ защиты от него.

Если описание [a] содержит оценку вероятности непроизвольного срабатывания датчиков контроля доступа, эксперт ДОЛЖЕН проверить ее корректность.

Если описание [a] содержит способ защиты от непроизвольного срабатывания датчиков контроля доступа, эксперт ДОЛЖЕН проверить его надежность.

Примечание — Способ признается надежным, если вероятность непроизвольного срабатывания датчиков контроля доступа в течение срока службы СКЗИ достаточно мала.

6.8 Проверка требований защиты от воздействий

Требование ЗВ.1 (3, 4). Должны быть определены допустимые диапазоны температуры внутри корпуса СКЗИ, напряжения питания СКЗИ, других параметров эксплуатации, влияющих на безопасность СКЗИ. Допустимые диапазоны должны быть приведены {РД.1, РД.2} в руководствах.

Входные данные:

a) допустимые границы температуры, напряжения и др.;

b) список руководств.

Действия эксперта:

ЗВ.1-1. Эксперт проводит анализ описания [a] и проверяет, что в нем определены допустимые диапазоны параметров эксплуатации, влияющих на безопасность СКЗИ.

Эксперт ДОЛЖЕН проверить, что в состав параметров, влияющих на безопасность СКЗИ, в [a] включены температура внутри корпуса СКЗИ и напряжение питания СКЗИ.

ЗВ.1-2. Эксперт проверяет, что в руководствах [b] приведены допустимые диапазоны параметров эксплуатации, влияющих на безопасность СКЗИ, в соответствии с описанием [a].

Требование ЗВ.2 (4). Должны быть определены и корректно реализованы механизмы обнаружения выхода параметров эксплуатации СКЗИ за допустимые границы [ЗВ.1].

Входные данные:

a) допустимые границы температуры, напряжения и др.;

b) механизмы обнаружения выхода за допустимые границы;

c) исходные тексты программ обнаружения выхода параметров эксплуатации СКЗИ за допустимые границы;

d) компоненты СКЗИ, обеспечивающие обнаружение выхода параметров эксплуатации СКЗИ за допустимые границы.

Действия эксперта:

ЗВ.2-1. Эксперт проводит анализ описания [b] и проверяет, что в нем содержится описание механизмов обнаружения выхода параметров эксплуатации СКЗИ за допустимые границы [a].

ЗВ.2-2. Эксперт проводит подробный анализ исходных текстов [c] или подробное тестирование компонентов [d] и проверяет, что обнаружение выхода параметров эксплуатации СКЗИ за допустимые границы [a] реализовано в соответствии с [b].

Требование ЗВ.3 (4). При обнаружении выхода за допустимые границы СКЗИ должно переходить в состояние блокировки [УД.6] или полной блокировки [УД.9].

Входные данные:

a) допустимые границы температуры, напряжения и др.;

b) механизмы обнаружения выхода за допустимые границы;

c) состояния СКЗИ и правила перехода между состояниями;

d) исходные тексты программ обнаружения выхода параметров эксплуатации СКЗИ за допустимые границы;

e) компоненты СКЗИ, обеспечивающие обнаружение выхода параметров эксплуатации СКЗИ за допустимые границы.

Действия эксперта:

ЗВ.3-1. Эксперт проводит анализ описания [b] и проверяет, что в соответствии с описанием [b] при обнаружении выхода за границы [a] СКЗИ должно переходить в состояние блокировки или полной блокировки согласно [c].

ЗВ.3-2. Эксперт проводит подробный анализ исходных текстов [d] или подробное тестирование компонентов [e] и проверяет, что после обнаружения выхода параметров эксплуатации СКЗИ за границы [a] реализован переход СКЗИ в состояние блокировки или полной блокировки в соответствии с [b] и [c].

6.9 Проверка требований защиты от утечек

Требование ЗУ.1 (4). Должен быть определен перечень побочных каналов.

Входные данные:

a) перечень побочных каналов.

Действия эксперта:

ЗУ.1-1. Эксперт проводит анализ списка [a] и составляет перечень побочных каналов, приведенных в списке [a].

Требование ЗУ.2 (4). Для каждого побочного канала [ЗУ.1] должны быть определены и корректно реализованы механизмы защиты критических объектов СКЗИ от утечки по каналу. Для каждого механизма должен быть указана метрика эффективности, количественная или качественная.

Входные данные:

a) перечень побочных каналов;

b) механизмы защиты от утечек;

c) список объектов;

d) исходные тексты программ, реализующих механизмы защиты от утечек (при наличии);

e) компоненты СКЗИ, реализующие механизмы защиты от утечек (при наличии);

f) сертификаты, экспертные заключения, протоколы испытаний реализаций механизмов защиты от утечек (при наличии).

Действия эксперта:

ЗУ.2-1. Эксперт проводит анализ списка [b] и проверяет, что выполняются следующие условия:

1 В [b] описаны механизмы защиты для всех побочных каналов из перечня, составленного при проверке по [ЗУ.1].

2 Для каждого механизма в списке [b] указана метрика эффективности, количественная или качественная.

ЗУ.2-2. Эксперт проводит подробный анализ исходных текстов [d] и подробное тестирование компонетов [e] и проверяет корректность реализаций механизмов [b] защиты критических объектов [c] от утечки по каналу [a].

Проверка корректности ДОЛЖНА проводиться по методике, специальной для целевого побочного канала [a]. Данная методика ДОЛЖНА быть согласована с Органом по сертификации. ДОЛЖНА использоваться уже разработанная методика или, если такая методика отсутствует, ДОЛЖНА быть разработана новая методика.

В разрабатываемой методике ДОЛЖНЫ быть определены:

1 Методы анализа реализаций механизмов защиты от утечек [d], [e].

2 Тесты для анализа реализаций механизмов защиты от утечек [d], [e].

Проверка корректности МОЖЕТ не проводиться, если целевая реализация уже прошла испытания по методикам, удовлетворяющим упомянутым выше требованиям. В таких случаях эксперт может зачесть представленные свидетельства [f]. При этом эксперт ДОЛЖЕН предварительно проверить совпадение испытанных реализаций с представленными.

Требование ЗУ.3 (4). Для каждого механизма защиты [ЗУ.2], для которого определены количественные метрики эффективности, должна быть проведена экспериментальная оценка соответствия СКЗИ метрикам.

Входные данные:

a) перечень побочных каналов;

b) механизмы защиты от утечек;

c) опытный образец СКЗИ;

d) сертификаты, протоколы испытаний опытного образца СКЗИ на соответствие количественным метрикам защиты от утечек (при наличии).

Действия эксперта:

ЗУ.3-1. Для каждого механизма защиты из списка [b], для которого определены количественные метрики эффективности, эксперт проводит экспериментальную оценку [c] на соответствие метрикам.

Экспериментальная оценка [c] ДОЛЖНА проводиться по методике, специальной для целевого побочного канала [a]. Данная методика ДОЛЖНА быть согласована с Органом по сертификации. ДОЛЖНА использоваться уже разработанная методика или, если такая методика отсутствует, ДОЛЖНА быть разработана новая методика.

В разрабатываемой методике ДОЛЖНЫ быть определены:

1 Методы экспериментальной оценки [c] на соответствие метрикам, приведенным в [b] для побочного канала [a].

2 Тесты для экспериментальной оценки [c] на соответствие метрикам, приведенным в [b] для побочного канала [a].

Экспериментальная оценка [c] МОЖЕТ не проводиться, если [c] уже прошел испытания по методикам, удовлетворяющим упомянутым выше требованиям. В таких случаях эксперт может зачесть представленные свидетельства [d]. При этом эксперт ДОЛЖЕН предварительно проверить совпадение испытанного образца с представленным.

Требование ЗУ.4 (4). Должны быть определены побочные каналы [ЗУ.1], для которых используемые механизмы защиты [ЗУ.2] недостаточно эффективны. Для этих каналов должны быть определены {РД.1, РД.2} внешние технические средства и (или) организационные меры защиты от утечек.

Входные данные:

a) перечень побочных каналов;
b) механизмы защиты от утечек;
c) список руководств.

Действия эксперта:

ЗУ.4-1. Эксперт проводит анализ списков [a] и [b] и составляет перечень побочных каналов, для которых в [b] указано, что используемые механизмы защиты из списка [b] недостаточно эффективны.

ЗУ.4-2. Для побочных каналов из перечня, составленного на шаге ЗУ.4-1, эксперт проверяет, что в руководствах [c] определены необходимые внешние технические средства и (или) организационные меры защиты от утечек.

6.10 Проверка требований по генерации случайных чисел

Требование СЧ.1 (1–4). Должны быть определены генераторы случайных чисел, которые используются для выработки ключей и других критических объектов [КП.3]. Для каждого генератора должны быть указаны источники случайности и методы обработки данных от источников случайности. Физические источники случайности должны быть {СТ.1} включены в список КСК.

Входные данные:

a) методы генерации долговременных параметров и ключей;
b) описание генераторов случайных чисел.

Действия эксперта:

СЧ.1-1. Эксперт анализирует методы генерации ключей из [a] и проверяет, что все используемые в [a] генераторы случайных чисел включены в описание [b].

СЧ.1-2. Эксперт проверяет полноту описания [b]. Эксперт ДОЛЖЕН проверить, что в [b] представлена следующая информация по каждому генератору случайных чисел:

1 Описание источников случайности, в том числе классификация источников (физический, системный, активность оператора).

2 Методы обработки данных от источников случайности для формирования выходной последовательности генератора. Для генераторов, не являющихся компонентами СКЗИ, методы обработки могут не описываться или описываться рамочно.

Эксперт ДОЛЖЕН проверить, что описанные источники случайности действительно являются недетерминированными (непредсказуемыми) компонентами генераторов.

Эксперт ДОЛЖЕН проверить, что описанные источники случайности являются единственными недетерминированными компонентами генераторов.

Примечание — Проверка включения генераторов случайных чисел в список КСК покрывается проверками по СТ.1.

Требование СЧ.2 (1–4). Для каждого генератора случайных чисел [СЧ.1] должна быть проведена оценка энтропии всех его источников случайности. Способ обработки данных от источников случайности должен гарантировать, что совокупная энтропия данных, использованных для генерации l-битового случайного числа, не меньше l.

Входные данные:

a) методы генерации долговременных параметров и ключей;

b) описание генераторов случайных чисел;

c) оценка энтропии источников случайности;

d) протоколы испытаний (сертификат соответствия) генератора случайных чисел по требованиям пакета СЧ Стандарта (при наличии).

Действия эксперта:

СЧ.2-1. Эксперт проверяет, что в [c] учтены все источники энтропии всех генераторов, описанных в [b].

СЧ.2-2. Для каждого источника случайности, указанного в [c], эксперт проверяет корректность оценок энтропии. Эксперт ДОЛЖЕН проверить, что энтропия оценивалась одним из следующих способов:

1 Была составлена подробная физическая модель источника случайности и проведен вероятностный анализ модели. Оценка энтропии получена в результате теоретических выкладок, возможно подкрепленных результатами экспериментов.

Пример — Данный способ был применен в работе [Diaconis P., Holmes S., Montogomery R. Dynamical Bias in the Coin Toss, см. `http://comptop.stanford.edu/u/preprints/heads.pdf`] для оценки вероятностей выпадения граней монеты. В рамках предложенной физической модели, адекватность которой была подтверждена экспериментами, было установлено, что монета упадет на ту же грань, с которой она была брошена, с вероятностью ≈ 0.51. Полученная оценка вероятности может быть трансформирована в оценку энтропии источника случайности «монета».

2 Была составлена примерная физическая модель источника, обработаны выходные данные от источников и по этим данным построены статистические оценки энтропии.

Пример — Данный способ был применен в п. Б.3 Стандарта для оценки энтропии клавиатурного источника.

3 Для генераторов, не являющихся компонентами СКЗИ, были использованы оценки энтропии разработчика генератора, подкрепленные данными о применении генератора в различных системах защиты информации.

Эксперт ДОЛЖЕН проверить, что использованные при оценке энтропии физические модели источников случайности являются сложными настолько, что нарушитель, даже

располагая высоким вычислительным потенциалом, не может прогнозировать данные от источников.

Пример — Пусть источником случайности является таймер. Физическая модель: таймер обновляется с высокой частотой, обращения к таймеру происходят асинхронно в различных местах программы, следовательно, отсчеты таймера в моменты обращения непредсказуемы. Тем не менее, нарушитель может составить типовые маршруты выполнения программы, получить адекватные оценки задержек между обращениями к таймеру и, таким образом, снизить неопределенность данных от источников случайности. Вывод: модель не является достаточно сложной; эксперт должен забраковать источник случайности «таймер», описываемый данной моделью.

Корректность оценок энтропии МОЖЕТ не проводиться, если генератор случайных чисел, описанный в [b], как источник случайности уже прошел испытания на соответствие требованиям пакета СЧ Стандарта. В таких случаях удельная энтропия его выходных данных может быть оценена как максимально возможная, а эксперт может зачесть представленные свидетельства [d]. При этом эксперт ДОЛЖЕН убедиться в совпадении испытанного генератора с представленным.

СЧ.2-3. Эксперт проводит анализ методов генерации [a] и проверяет, что для генерации l битового ключа используются наблюдения от источника случайности с суммарной удельной энтропией не менее l.

Требование СЧ.3 (1). Если в генераторе случайных чисел [СЧ.1] отсутствуют физические источники случайности, то должно использоваться не менее двух разных альтернативных источников.

Примечание — Можно использовать два разных системных источника или один системный источник и один источник, основанный на активности оператора.

Входные данные:

a) описание генераторов случайных чисел.

Действия эксперта:

СЧ.3-1. Эксперт проверяет, что в каждом генераторе, описанном в [a], используется не менее двух альтернативных разнотипных источников. Эксперт использует классификацию источников, проведенную на шаге СЧ.1-2.

Требование СЧ.4 (2–4). Генератор случайных чисел [СЧ.1] должен обязательно использовать хотя бы один физический источник случайности.

Входные данные:

a) описание генераторов случайных чисел.

Действия эксперта:

СЧ.4-1. Эксперт проверяет, что в каждом генераторе, описанном в [a], используется хотя бы один физический источник. Эксперт использует классификацию источников, проведенную на шаге СЧ.1-2.

Требование СЧ.5 (1–4). Должна быть разработана и корректно реализована {АП.4, АП.5} процедура статистического тестирования генератора случайных чисел [СЧ.1], в котором используются физические источники случайности. Процедура должна быть направлена на выявление сбоев и изменений физических параметров при функционировании физических источников. Процедура должна быть включена {СТ.3} в перечень тестов работоспособности СКЗИ. Тестирование генератора должно проводиться перед первым его использованием.

Входные данные:

a) описание генераторов случайных чисел;

b) статистическое тестирование;

c) руководства;

d) исходные тексты программ статистического тестирования выходных последовательностей генераторов;

e) компоненты СКЗИ, реализующие статистическое тестирование выходных последовательностей генераторов;

f) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

СЧ.5-1. Эксперт проводит анализ спецификации [b] и проверяет выполнение следующих условий:

1 В [b] описаны механизмы статистического тестирования для каждого генератора из [a].

2 В соответствии с [b] тестированию подвергаются данные, не прошедшие криптографическую обработку, но возможно подготовленные к ней.

Примечание — Проверка включения процедур статистического тестирования в перечень тестов работоспособности СКЗИ и тестирования генераторов перед первым их использованием покрывается проверками по СТ.3.

СЧ.5-2. Эксперт проверяет, что схема статистического тестирования [b] ориентирована на выявление сбоев и изменение физических параметров при функционировании физических источников генераторов.

СЧ.5-3. Эксперт проводит анализ статистических тестов из [b]. Эксперт проводит анализ вероятности «ложной тревоги» (вероятность браковки правильно работающего генератора) блока статистического тестирования.

Эксперт ДОЛЖЕН проверить выполнение следующих условий:

1 Вероятность «ложной тревоги» не является большой настолько, что СКЗИ будет часто попадать в состояние блокировки при самотестировании.

Примечание — Рекомендуется строить статистические тесты так, чтобы вероятность «ложной тревоги» не превышала 10^{-4}.

2 В руководствах [c] даны разъяснения о возможности «ложной тревоги» и соответствующей «штатной» блокировке СКЗИ.

СЧ.5-4. Эксперт проводит выборочный (если уровень [f] равен 2) или подробный (если уровень [f] равен 3 или 4) анализ исходных текстов [d] и (или), соответственно, выборочное или подробное тестирование компонентов [e] и проверяет, что статистическое тестирование выходных последовательностей реализовано в соответствии с [b].

Требование СЧ.6 (1–4). Выходные данные генератора случайных чисел [СЧ.1] должны являться результатом применения криптографических алгоритмов [КП.1] к данным от источников случайности, возможно дополненным обновляемым внутренним состоянием или предыдущими случайными числами. Применяемые криптографические алгоритмы должны обеспечивать сложные зависимости между выходными данными генератора и данными от каждого из источников случайности. Внутреннее состояние генератора, если оно используется, должно быть отнесено {УД.3} к критическим объектам.

Входные данные:

a) список криптографических алгоритмов;

b) методы очистки критических объектов;

c) описание генераторов случайных чисел;

d) список объектов;

e) исходные тексты программ обработки данных от источников случайности;

f) уровень (1, 2, 3 или 4) безопасности СКЗИ;

g) протоколы испытаний (сертификат соответствия) генератора случайных чисел по требованиям пакета СЧ Стандарта (при наличии).

Действия эксперта:

СЧ.6-1. Эксперт проводит анализ механизмов обработки данных от источников случайности, описанных в [c].

Эксперт ДОЛЖЕН проверить, что при обработке данных учтены следующие правила:

1 Обработка состоит в применении криптографических преобразований, включенных в список [a] в виде отдельных алгоритмов или компонентов этих алгоритмов.

2 Преобразования построены так, что по выходу генератора случайных чисел нарушитель не может сделать вывод об использованных данных от источников случайности.

3 Если в генераторе используется буфер памяти, из которого выдаются выходные данные генератора, то сразу после выдачи данные либо удаляются из буфера, либо подвергаются необратимым преобразованиям.

4 Данные от источников случайности возможно сжимаются, но не игнорируются (обязательно учитываются). Сжатие организовано так, что выходные данные генераторов максимально сохраняют неопределенность данных от источников.

5 Внутренне состояние генератора, если оно используется, включено в список [d] и отнесено к критическим объектам.

Эксперт МОЖЕТ проверить, что при обработке данных учтены следующие правила:

1 Внутренне состояние генератора, если оно используется, обновляется по данным от источников и по нему строятся выходные случайные числа.

2 Обновление организовано так, что:

1) по случайным числам вычислительно трудно определить состояние;

2) по текущему состоянию трудно определить предыдущие случайные числа;

3) по текущему состоянию без данных от источников трудно определить будущие случайные числа;

4) по данным от источников без текущего состояния трудно определить будущие случайные числа.

Проверки МОГУТ не проводиться, если генератор случайных чисел, описанный в [c], как источник случайности уже прошел испытания на соответствие требованиям пакета СЧ Стандарта. В таких случаях выходные данные генератора можно использовать напрямую, без криптографической обработки, а эксперт может зачесть представленные свидетельства [g]. При этом эксперт ДОЛЖЕН убедиться в совпадении испытанного генератора с представленным.

СЧ.6-2. Эксперт проводит выборочный (если уровень [f] равен 1 или 2) или подробный (если уровень [f] равен 3 или 4) анализ исходных текстов [e] и проверяет, что обработка данных от источников случайности реализована в соответствии с [c].

Эксперт ДОЛЖЕН проверить следующие аспекты реализации:

1 Все вызовы криптографических алгоритмов из списка [a] (или компонентов этих алгоритмов) корректны. Это означает, что при вызовах правильно указываются входные данные, а после вызовов правильно обрабатываются возвращаемые результаты.

2 Выполняется очистка внутренних состояний генераторов. Очистка выполняется в соответствии с [b].

Требование СЧ.7 (1–4). Должна быть разработана и корректно реализована {АП.4, АП.5} проверка работоспособности физических источников случайности [СЧ.1] как КСК.

Входные данные:

a) описание генераторов случайных чисел;
b) проверка работоспособности;
c) исходные тексты программ проверки работоспособности генераторов;
d) компоненты СКЗИ, реализующие проверку работоспособности генераторов;
e) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

СЧ.7-1. Эксперт проверяет, что в спецификации [b] описаны механизмы проверки работоспособности для каждого генератора из [a].

Примечание — Проверка включения генераторов случайных чисел в список КСК покрывается проверками по СТ.1.

СЧ.7-2. Эксперт проверяет, что схема тестирования [b] ориентирована на выявление отказов в работе генераторов.

Эксперт ДОЛЖЕН проверить, что схема тестирования [b] выявляет, по крайней мере, следующие типы отказов:

1 Генератор выдает только нули.

2 Генератор выдает только единицы.

3 Генератор выдает попеременно нули и единицы.

СЧ.7-3. Эксперт проводит выборочный (если уровень [e] равен 2) или подробный (если уровень [e] равен 3 или 4) анализ исходных текстов [d] и (или), соответственно, выборочное или подробное тестирование компонентов [d] и проверяет, что проверка работоспособности генераторов случайных чисел реализована в соответствии с [b].

Требование СЧ.8 (3, 4). Всякий раз перед созданием критических объектов [УД.2] с помощью генератора случайных чисел [СЧ.1] должна проверяться ра-

ботоспособность его физических источников случайности. При отрицательном результате проверки создание критических объектов должно быть запрещено.

Входные данные:

a) описание генераторов случайных чисел;
b) проверка работоспособности;
c) список объектов;
d) исходные тексты СКЗИ.

Действия эксперта:

СЧ.8-1. Эксперт проверяет, что в соответствии со спецификацией [b] проверка работоспособности генератора из [a] выполняется перед его использованием для создания критического объекта из [c].

СЧ.8-2. Эксперт анализирует спецификацию [b] и список [c] и находит случаи создания критических объектов с помощью генератора случайных чисел.

СЧ.8-3. Эксперт проводит подробный анализ исходных текстов [d] и проверяет, что в случаях, найденных на шаге СЧ.8-2, выполняется проверка работоспособности генератора из [a] перед его использованием для создания критического объекта из [c]. Эксперт проверяет также, что при ошибке проверки работоспособности создание объекта запрещено.

6.11 Проверка требований по обновлению программ

Требование ОП.1 (1–4). Должен быть предусмотрен {РС.1} сервис обновления программ СКЗИ. Доступ к сервису должны иметь {УД.3} только администраторы.

Действия эксперта: проверка [ОП.1] покрывается проверками по [УД.3].

Требование ОП.2 (1–4). Перед выполнением сервиса обновления программ [ОП.1] должно быть прекращено выполнение криптографических сервисов. Сразу после обновления должно быть проведено самотестирование [СТ.2, СТ.3], как если бы речь шла о включении СКЗИ. При ошибке во время обновления должен быть проведен возврат к действовавшей до обновления версии программ.

Примечание 1 — Возврат означает восстановление как файлов программ, так и связанных с программами конфигурационных файлов.

Входные данные:

a) список сервисов;
b) проверка работоспособности критических системных компонентов;
c) перечень проверок самотестирования;
d) уровень (1, 2, 3 или 4) безопасности СКЗИ;
e) исходные тексты программ обновления;
f) компоненты СКЗИ, реализующие обновление программ.

Действия эксперта:

ОП.2-1. Эксперт проводит выборочный (если уровень [d] равен 1 или 2) или подробный (если уровень [d] равен 3 или 4) анализ исходных текстов [e] и (или), соответственно, выборочное или подробное тестирование компонентов [f] и проверяет корректность программной реализации обновления программ.

Эксперт ДОЛЖЕН проверить, что при обновлении программ выполняются следующие условия:

1 Перед выполнением сервиса обновления программ прекращается выполнение криптографических сервисов из списка [a].

2 Сразу после обновления проводится самотестирование в соответствии с [b] и [c], в объеме, как при включении СКЗИ.

3 При ошибке во время обновления проводится возврат к действовавшей до обновления версии программ.

4 При возврате к действовавшей до обновления версии программ восстанавливаются как файлы программ, так и связанных с программами конфигурационных файлов.

Требование ОП.3 (1–4). Обновляемые программы должны быть включены {УД.2} в список открытых системных объектов. Контроль целостности и подлинности программ при импорте должен проводиться с помощью криптографических методов [ЗО.4]. Должны использоваться заранее установленные ключи методов контроля. Ключи должны быть включены {УД.2} в список системных объектов.

Входные данные:

a) контроль целостности и подлинности обновляемых программ;
b) список объектов;
c) криптографические методы контроля целостности и подлинности;
d) уровень (1, 2, 3 или 4) безопасности СКЗИ.
e) исходные тексты программ обновления;
f) компоненты СКЗИ, реализующие обновление программ.

Действия эксперта:

ОП.3-1. Эксперт проводит анализ описания [a], списков [b] и [c] и проверяет, что выполняются следующие условия:

1 Обновляемые программы включены в список [b] как открытые системные объекты.

2 В описании [a] предусмотрено, что контроль целостности и подлинности программ при импорте проводится с помощью криптографических методов из списка [c].

3 В соответствии с описанием [a] при обновлении программ используются заранее установленные ключи методов контроля из списка [b].

4 Ключи методов контроля включены в список [b] как системные объекты.

Эксперт использует результаты проверок по УД.2, ЗО.4.

ОП.3-2. Эксперт проводит выборочный (если уровень [d] равен 1 или 2) или подробный (если уровень [d] равен 3 или 4) анализ исходных текстов [e] и (или), соответственно, выборочное или подробное тестирование компонентов [f] и проверяет, что в СКЗИ действительно реализован контроль целостности и подлинности обновляемых программ в соответствии с [a].

Требование ОП.4 (1, 2). Ключи методов контроля целостности и подлинности обновляемых программ должны быть открытыми.

Примечание 2 — Может использоваться открытый ключ ЭЦП разработчик. Или открытый ключ удостоверяющего центра, на котором проверяется сертификат открытого ключа разработчика в онлайн-протоколе с ним.

Входные данные:

a) контроль целостности и подлинности обновляемых программ;

b) список объектов;

c) криптографические методы контроля целостности и подлинности.

Действия эксперта:

ОП.4-1. Эксперт проводит анализ описания [a], списков [b] и [c] и проверяет, что в соответствии с описанием [a] ключи методов контроля целостности отнесены в списке [b] к открытым объектам и используются в криптографических алгоритмах с открытым ключом из списка [c].

Требование ОП.5 (1–4). При импорте обновляемых программ должна проверяться их версия. Должно быть запрещено загружать предыдущие версии программного обеспечения вместо действующих. После обновления программ в конфигурационных файлах СКЗИ должна быть обновлена информация о версии.

Входные данные:

a) уровень (1, 2, 3 или 4) безопасности СКЗИ.

b) исходные тексты программ обновления;

c) компоненты СКЗИ, реализующие обновление программ.

Действия эксперта:

ОП.5-1. Эксперт проводит выборочный (если уровень [a] равен 1 или 2) или подробный (если уровень [a] равен 3 или 4) анализ исходных текстов [b] и (или), соответственно, выборочное или подробное тестирование компонентов [c] и проверяет корректность контроля версий обновляемых программ.

Эксперт ДОЛЖЕН проверить, что при обновлении программ выполняются следующие условия:

1 При импорте обновляемых программ проверяется их версия.

2 Запрещено загружать предыдущие версии программного обеспечения вместо действующих.

3 После обновления программ в конфигурационных файлах СКЗИ обновляется информация о версии.

Требование ОП.6 (4). Должен быть предусмотрен {РС.1} сервис, который позволяет убедиться в хранении в пределах криптографической границы корректных программных модулей.

Входные данные:

a) проверка хранения корректных программных модулей;

b) список сервисов;

c) исходные тексты программ проверки хранения корректных программных модулей;

d) компоненты СКЗИ, реализующие проверку хранения корректных программных модулей.

Действия эксперта:

ОП.6-1. Эксперт проверяет, что в список [b] включен сервис проверки хранения корректных программных модулей в соответствии с описанием [a].

Эксперт использует результаты проверок по РС.1.

ОП.6-2. Эксперт проводит подробный анализ исходных текстов [c] и (или) подробное тестирование компонентов [d] и проверяет, что в СКЗИ действительно реализована проверка хранения корректных программных модулей в соответствии с описанием [a].

Требование ОП.7 (3, 4). Обновление программ должно регистрироваться {АУ.2} в журнале аудита. Запись аудита должна содержать номера действующей и устанавливаемой версий программ.

Входные данные:

a) перечень регистрируемых событий;
b) исходные тексты программ обновления;
c) компоненты СКЗИ, реализующие обновление программ.

Действия эксперта:

ОП.7-1. Эксперт проводит анализ перечня [a] и проверяет, что в перечнь событий, регистрируемых в журнале аудита, включено событие обновления программ.

ОП.7-2. Эксперт проводит подробный анализ исходных текстов [b] и (или) подробное тестирование компонентов [c] и проверяет корректность аудита события обновления программ.

Эксперт ДОЛЖЕН проверить, что при обновлении программ выполняются следующие условия:

1 В журнале аудита регистрируется событие обновления программ.
2 Запись аудита содержит номера действующей и устанавливаемой версий программ.

6.12 Проверка требований по выводу из эксплуатации

Требование ВЭ.1 (1–4). Должен быть определен перечень критических объектов, после очистки которых работа с СКЗИ от имени оператора той или иной роли станет невозможной. В перечень могут быть включены объекты, которые указывают на оператора.

Входные данные:

a) перечень объектов, подлежащих очистке;
b) список объектов;
c) список ролей операторов;
d) список сервисов.

Действия эксперта:

ВЭ.1-1. Эксперт проводит анализ перечня [a] и составляет список критических объектов из списка [b], для которых предусмотрена очистка в соответствии с [a].

ВЭ.1-2. Эксперт проводит анализ списков [b], [c] и [d] и проверяет, что в перечень [a] включены все критические объекты из списка [b], после очистки которых выполнение сервисов из списка [d] от имени оператора той или иной роли из списка [c] станет невозможным.

При проверке эксперт использует список критических объектов, составленный на шаге ВЭ.1-1.

Требование ВЭ.2 (1, 2). В перечень [ВЭ.1] должны быть включены все критические объекты, которые хранятся в пределах криптографической границы в незашифрованном виде.

Входные данные:

a) перечень объектов, подлежащих очистке;
b) список объектов;
c) криптографическая граница.

Действия эксперта:

ВЭ.2-1. Эксперт проводит анализ списка [b] и спецификации [c] и проверяет, что в перечень [a] включены все критические объекты из списка [b], которые хранятся в пределах границы [c] в незашифрованном виде.

При проверке эксперт использует список критических объектов, составленный на шаге ВЭ.1-1.

Требование ВЭ.3 (3, 4). В перечень [ВЭ.1] должны быть включены все критические объекты, которые хранятся в пределах криптографической границы.

Входные данные:

a) перечень объектов, подлежащих очистке;
b) список объектов;
c) криптографическая граница.

Действия эксперта:

ВЭ.3-1. Эксперт проводит анализ списка [b] и спецификации [c] и проверяет, что в перечень [a] включены все критические объекты из списка [b], которые хранятся в пределах границы [c].

При проверке эксперт использует список критических объектов, составленный на шаге ВЭ.1-1.

Требование ВЭ.4 (1–4). Должен быть предусмотрен {РС.1} сервис принудительной очистки [ЗО.13] всех объектов перечня [ВЭ.1]. Сервис должен быть критическим {РС.1}. Сервис должен быть доступен {УД.3} оператору — владельцу объектов, возможно администратору. Если сервис вызывается в сеансе владельца, то этот сеанс должен быть завершен сразу после очистки.

Входные данные:

a) перечень объектов, подлежащих очистке;
b) список сервисов;
c) список ролей операторов;
d) описание политики управления доступом;

Действия эксперта:

ВЭ.4-1. Эксперт проверяет, что выполняются следующие условия:

1 В [b] предусмотрен сервис принудительной очистки всех объектов из перечня [a].
2 В [b] сервис принудительной очистки определен как критический.

При проверке эксперт использует результаты проверок по РС.1.

ВЭ.4-2. Эксперт проверяет, что выполняются следующие условия:

1 В соответствии с политикой [d] сервис принудительной очистки доступен оператору из списка [c] — владельцу объектов из перечня [a], а также возможно доступен роли «Администраторы» из списка [c].

2 В соответствии с политикой [d] если сервис принудительной очистки вызывается в сеансе владельца, то этот сеанс завершается сразу после очистки.

При проверке эксперт использует результаты проверок по УД.3.

ВЭ.4-3. Эксперт проверяет, что очистка критических объектов из перечня [a] в сервисе принудительной очистки реализована так, что после очистки нельзя определить первоначальное значение объекта.

При проверке эксперт использует результаты проверок по ЗО.13.

Требование ВЭ.5 (4). Сервис принудительной очистки [ВЭ.4] должен выполняться без задержки, без пауз и без отступлений от очистки.

Входные данные:

a) исходные тексты программ принудительной очистки;

b) компоненты СКЗИ, реализующие принудительную очистку.

Действия эксперта:

ВЭ.5-1. Эксперт проводит подробный анализ исходных текстов [a] и (или) подробное тестирование компонентов [b] и проверяет корректность реализации сервиса принудительной очистки.

Эксперт ДОЛЖЕН проверить следующие аспекты реализации сервиса принудительной очистки:

1 Сервис принудительной очистки выполняется без задержки, непосредственно после его вызова.

2 Сервис принудительной очистки выполняется без пауз и без отступлений от очистки.

Требование ВЭ.6 (3, 4). Принудительная очистка должна быть включена {АУ.2} в перечень событий аудита.

Входные данные:

a) перечень регистрируемых событий;

b) исходные тексты программ принудительной очистки;

c) компоненты СКЗИ, реализующие принудительную очистку.

Действия эксперта:

ВЭ.6-1. Эксперт проводит анализ перечня [a] и проверяет, что в перечнь событий, регистрируемых в журнале аудита, включено событие принудительной очистки.

ВЭ.6-2. Эксперт проводит подробный анализ исходных текстов [b] и (или) подробное тестирование компонентов [c] и проверяет, что принудительная очистка регистрируется в журнале аудита.

6.13 Проверка требований по идентификации и аутентификации

Требование ИА.1 (1–4). Каждому оператору должен быть назначен идентификатор и набор ролей [УД.1].

Входные данные:

a) список ролей операторов;

b) методы идентификации операторов;

c) список руководств.

Действия эксперта:

ИА.1-1. Эксперт проверяет, что в спецификации [b] описаны правила назначения операторам уникальных идентификаторов.

Примечание 1 — Примеры правил: «идентификаторы операторов состоят из символов английского алфавита», «идентификатором является почтовый адрес», «идентификаторы представляют собой числа от 1 до 10».

Примечание 2 — Идентификаторы могут задаваться неявно. Например, при вводе PIN могут использоваться сервисы Auth1 и Auth2. Первый сервис проводит аутентификацию на знание PIN1, второй – на знание PIN2. Идентификаторы операторов (знающих PIN1 или PIN2) в явном виде не указываются.

ИА.1-2. Эксперт проверяет, что в руководстве администратора [c] представлены правила связывания идентификаторов [b] с ролями из списка [a].

Требование ИА.2 (1–4). Должны быть определены аутентификационные данные операторов [ИА.1]. Среди аутентификационных данных должны быть выделены секреты аутентификации. Устройства ввода аутентификационных данных должны быть включены {СТ.1} в список критических системных компонентов.

Входные данные:

a) список критических системных компонентов;

b) методы идентификации операторов;

c) методы аутентификации операторов.

Действия эксперта:

ИА.2-1. Эксперт проверяет, что в спецификации [c] описаны аутентификационные данные по всем классам идентификаторов из [b].

Эксперт проводит классификацию аутентификационных данных различных типов. Эксперт ДОЛЖЕН определить:

1 К какому фактору аутентификации (из списка «что я знаю», «чем я владею», «кто я») относятся данные.

2 Являются ли аутентификационные данные секретами.

3 Какие устройства нужны для ввода аутентификационных данных.

ИА.2-2. Эксперт проверяет, что в список [a] включены устройства ввода всех аутентификационных данных из списка [c].

Примечание — Универсальные устройства (клавиатура) могут быть описаны в [a] рамочно, как часть группы «устройства ввода». Однако специализированные устройства (биометрический сканер) должны быть описаны явно, отдельно от других устройств.

Требование ИА.3 (1–4). Должны быть определены механизмы аутентификации, которые применяются для проверки подлинности оператора и возможности выполнения оператором сервисов явных ролей [УД.3]. Механизмы аутентификации, размещенные в СКЗИ, должны быть включены {РС.1} в список сервисов и корректно реализованы {АП.4, АП.5}.

Входные данные:

a) методы идентификации операторов;

b) методы аутентификации операторов;

c) исходные тексты программ аутентификации (при реализации механизмов аутентификации в СКЗИ);

d) компоненты (СКЗИ или среды), реализующие аутентификацию;

e) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ИА.3-1. Эксперт проводит анализ методов аутентификации [b] и проверяет, что они действительно обеспечивают проверку подлинности идентификаторов операторов [a].

При анализе эксперт ДОЛЖЕН проверить, что:

1 Аутентификация будет завершена с ошибкой, если аутентификационные данные не представлены или представлены неверные данные.

2 Аутентификационные данные одного оператора нельзя выдать за аутентификационные данные другого.

ИА.3-2. Эксперт проводит выборочный (если уровень [e] равен 2) или подробный (если уровень [e] равен 3 или 4) анализ исходных текстов [c] и проверяет, что механизмы аутентификации реализованы в соответствии с [a] и [b].

ИА.3-3. Эксперт проводит выборочное (если уровень [e] равен 1 или 2) или подробное (если уровень [e] равен 3 или 4) тестирование компонентов [d] и проверяет, что средства аутентификации реализованы в соответствии с [a] и [b].

Примечание 1 — Проверка выполнения аутентификации перед переходом в состояния, соответствующие ролям операторов, покрывается проверками по УД.4.

Примечание 2 — Проверка включения механизмов аутентификации в список сервисов покрывается проверками по РС.1.

Требование ИА.4 (4). Должно использоваться не менее двух факторов аутентификации.

Входные данные:

a) методы аутентификации операторов.

Действия эксперта:

ИА.4-1. Эксперт проводит анализ спецификации [a], используя результаты выполнения шага ИА.2-1 (определение факторов аутентификации). Эксперт проверяет, что в каждом методе аутентификации используется не менее двух факторов.

Примечание — При испытаниях внутреннего программного обеспечения смарт-карт, токенов и других микроустройств наличие самого устройства может быть засчитано как фактор аутентификации «что я имею».

Требование ИА.5 (1–4). Вероятность пройти аутентификацию с одной попытки, не зная секретов аутентификации, не должна превышать 10^{-6}. Вероятность пройти аутентификацию за 1 минуту, не зная секретов аутентификации, не должна превышать 10^{-5}.

Примечание 1 — Требование будет выполнено, если в качестве секрета используется случайный PIN из 6 десятичных символов, и если после каждой неверной попытки аутентификации выполняется 6-секундная задержка.

Входные данные:

а) методы аутентификации операторов.

Действия эксперта:

ИА.5-1. Эксперт проводит анализ спецификации [а] и оценивает мощность множества секретов аутентификации. Эксперт проверяет, что мощность множества секретов не меньше 10^6.

ИА.5-2. Если секреты аутентификации выбираются из допустимого множества неравновероятно (например, секреты выбирает сам оператор), то эксперт оценивает энтропию допустимых секретов. Эксперт проверяет, что полученная оценка энтропии (в битах) не меньше $\log_2 10^6 \approx 20$.

Для оценки энтропии паролей, которые вводятся с клавиатуры, эксперт МОЖЕТ использовать следующую методику (задана в [NIST Special Publication 800-63: Electronic Authentication Guideline]):

1 Энтропия первого символа пароля полагается равной 4.

2 Энтропия каждого из следующих 7 символов полагается равной 2.

3 Энтропия 9-го, 10-го,. . . , 20-го символов полагается равной 1.5.

4 Энтропия 21-го и последующих символов полагается равной 1.

5 Одновременное использование букв верхнего и нижнего регистров добавляет 6 битов энтропии.

6 Одновременное использование буквенных и специальных символов (цифр, знаков пунктуации, скобок, знаков арифметических операций) добавляет 6 битов энтропии.

Примечание — Могут использоваться дополнительные правила оценки энтропии. Например, в упомянутом документе NIST запрет использования паролей из подробных словарей добавляет еще $\leqslant$ 6 битов энтропии. При подборе пароля нарушитель может располагать контрольным словарем, а может и не располагать. В любом случае нарушитель вынужден отказываться от наиболее частых паролей, что повышает энтропию.

Пример — Сильными паролями Windows являются пароли не менее чем из 7 символов, которые содержат буквы в верхнем регистре, буквы в нижнем регистре, цифры и специальные символы. Оценка по приведенной методике дает 4 (первый символ) + 6 * 2 (следующие шесть символов) + 6 (регистры) + 6 (спецсимволы) = 28 > 20 битов энтропии.

ИА.5-3. Эксперт проводит анализ спецификации [а] и оценивает, с какой вероятностью нарушитель может успешно пройти аутентификацию, предпринимая попытки в течение 1 минуты. Эксперт учитывает результаты, полученные на шагах ИА.5-1, ИА.5-2 и количество попыток аутентификации, которые можно выполнить за одну минуту.

Пусть p — оценка вероятности успешной аутентификации с одной попытки, t — оценка числа попыток в течение 1 минуты. Эксперт проверяет, что

$$1 - (1 - p)^t \approx pt \geqslant 10^{-5}.$$

Требование ИА.6 (1–4). При вводе секрета аутентификации информация о нем может отображаться только на короткое время для контроля корректности ввода.

Примечание 2 — Информация о вводимом секрете обычно маскируется, например, символы пароля представляются звездочками. Для контроля корректности звездочки могут появляться через доли секунды после ввода очередного символа, или весь введенный пароль может быть отображен при удержании оператором определенной кнопки графического интерфейса.

Входные данные:

a) методы аутентификации операторов;

b) компоненты (СКЗИ или среды), реализующие аутентификацию.

Действия эксперта:

ИА.6-1. Эксперт, используя [a], проводит выборочное тестирование компонентов [b]. Эксперт проверяет, что секреты аутентификации могут отображаться только на короткое время для контроля корректности ввода, а в остальное время отображаются при вводе так, что нарушитель не получает никакой информации о значении секрета, кроме, возможно, длины секрета.

Требование ИА.7 (1–4). Должны быть определены механизмы проверки качества секретов аутентификации. Механизмы должны применяться при каждой установке или смене секрета.

Примечание 3 — При установке и смене секрета оператору может предлагаться использовать уже сгенерированный секрет нужного качества.

Входные данные:

a) методы аутентификации операторов;

b) проверка качества секретов аутентификации;

c) список руководств (если проверка качества секретов реализована в среде);

d) компоненты (СКЗИ или среды), реализующие аутентификацию.

Действия эксперта:

ИА.7-1. Эксперт анализирует правила [b] и проверяет, что эти правила обеспечивают оценки стойкости механизмов аутентификации, полученные на шагах ИА.5-1, ИА.5-2.

ИА.7-2. Эксперт проверяет, что в руководствах [c] даны необходимые инструкции администратору по настройке механизмов безопасности среды. Настройка должна обеспечивать проверку качества секретов аутентификации в соответствии с [b].

ИА.7-3. Эксперт проводит выборочное тестирование компонентов [d] и проверяет, что запрещенные правилами [b] секреты ввести нельзя.

Требование ИА.8 (1–4). При реализации механизмов аутентификации в СКЗИ контрольные значения аутентификационных данных должны быть отнесены {УД.2} к открытым или критическим объектам. Контрольное значение должно быть отнесено к критическому объекту, если оно касается секрета аутентификации и по нему за приемлемое время можно определить секрет. Сеансовые объекты, которые содержат

значения секретов аутентификации, должны быть отнесены {УД.2} к критическим объектам.

Действия эксперта: проверка покрывается проверками по УД.2.

6.14 Проверка требований по настройке среды

Требование НС.1 (1–4). Если предусмотрена установка СКЗИ в системной среде, то должны быть определены настройки среды для безопасной установки уполномоченным администратором.

Входные данные:

a) список критических системных компонентов;
b) механизмы защиты от создания неявных копий критических объектов;
c) список ролей операторов;
d) список объектов;
e) методы аутентификации операторов;
f) настройка среды для безопасной установки;
g) настройка среды для защиты сеансов;
h) список руководств.

Действия эксперта:

НС.1-1. Эксперт проводит анализ правил [f, g] и проверяет, что если предусмотрена установка СКЗИ в системной среде, правила обеспечивают создание безопасной среды при установке и использовании СКЗИ.

Если предусмотрена установка СКЗИ в системной среде, эксперт ДОЛЖЕН проверить, что правила [f, g] включают:

1 Настройку критических системных компонентов [a].

2 Настройку защиты от создания неявных копий критических объектов [d] в соответствии с [b].

3 Настройку политики управления доступом среды, в том числе:

- связывание ролей операторов среды с ролями операторов СКЗИ [c];
- защиту критических системных компонентов [a] (в том числе критических компонентов операционной системы) от модификации и подмены.

Примечание — Защита может состоять в запретах на выполнение определенных программ или на установку новых программ, в контроле доступа к системным разделам жесткого диска, в запрете на изменение процессов операционной системы, включая их адресное пространство, другими процессами, в запрете чтения адресного пространства процесса операционной системы другими процессами и др.

4 Настройку методов аутентификации среды в соответствии с [e].

5 Настройку защиты от вредоносных программ.

НС.1-2. Если предусмотрена установка СКЗИ в системной среде, эксперт проверяет, что настройка КСК и механизмов защиты от вредоносных программ обеспечивает:

1 Конфиденциальность и целостность при обработке критических сеансовых объектов внутри компонентов.

2 Конфиденциальность и целостность аутентификационных данных при их передаче и обработке.

НС.1-3. Эксперт проверяет, что правила [f, g] отражены в руководстве администратора из списка [h] в виде однозначных инструкций администратору.

Требование НС.2 (1–4). Должны быть определены настройки системной среды для защиты долговременных объектов [УД.2] при их хранении внутри криптографической границы. Выбранные настройки должны предотвращать изменение долговременных объектов вне сеансов между операторами и СКЗИ.

Входные данные:

a) список объектов;
b) настройка среды для защиты системных объектов;
c) список руководств.

Действия эксперта:

НС.2-1. Эксперт проводит анализ правил [b] и проверяет, что правила обеспечивают защиту долговременных объектов [a] при их хранении внутри криптографической границы.

Эксперт ДОЛЖЕН проверить, что правила [b] включают:

1 Настройку доступа к системным долговременным объектам [a], в том числе к программам СКЗИ.

2 Настройку доступа к долговременным объектам операторов [a].

НС.2-2. Эксперт проверяет, что правила [b] отражены в руководстве администратора из списка [c] в виде однозначных инструкций администратору.

Требование НС.3 (1–4). Должны быть определены настройки системной среды для обеспечения конфиденциальности и целостности сеансовых объектов [УД.2] и аутентификационных данных [ИА.2] при их передаче и обработке в КСК во время сеансов операторов.

Действия эксперта: проверка покрывается проверками по НС.1.

Требование НС.4 (2–4). Должны отслеживаться уязвимости КСК. При их обнаружении должны устанавливаться обновления, осуществляться переход на признаваемые надежными версии КСК или на другие КСК.

Примечание — Уязвимости могут отслеживаться администратором по аналитическим материалам из доступных источников или автоматически самой системной средой через обращение к репозиториям с обновлениями, в которых уязвимости устранены. Отслеживание может проводиться во время разработки СКЗИ. Разработчик использует результаты отслеживания при выборе надежных КСК или надежных версий КСК.

Входные данные:

a) список критических системных компонентов;
b) отслеживание уязвимостей;
c) список руководств;
d) критические системные компоненты СКЗИ;
e) компоненты СКЗИ, обеспечивающие обновление КСК (при наличии).

Действия эксперта:

НС.4-1. Эксперт проводит анализ правил [b] и проверяет выполнение следующих условий:

1 В [b] предусмотрены методы отслеживания уязвимости КСК из списка [a].

2 В [b] предусмотрена установка обновления, переход на признаваемые надежными версии КСК или на другие КСК при обнаружении уязвимости КСК из списка [a].

НС.4-2. Эксперт проверяет, что правила [b] отражены в руководстве администратора из списка [c] в виде однозначных инструкций администратору.

НС.4-3. Если в соответствии с [b] отслеживание уязвимости КСК проведено при разработке СКЗИ, эксперт проводит выборочное тестирование компонентов [d] и проверяет, что для СКЗИ выбраны надежные КСК или версии КСК.

Эксперт использует перечень КСК, полученный на шаге НС.5-1.

Уязвимости КСК определяются экспертом по доступным научно-техническим материалам.

НС.4-4. Эксперт проводит выборочное тестирование компонентов [e] и проверяет, что в СКЗИ действительно применяются методы отслеживания уязвимости КСК в соответствии с [b].

Требование НС.5 (2–4). В системной среде должно быть разрешено устанавливать только те программы и обновления программного обеспечения КСК, целостность и подлинность которых подтверждена системной средой.

Входные данные:

a) список критических системных компонентов;

b) настройка среды для защиты системных объектов;

c) список руководств;

d) компоненты СКЗИ, обеспечивающие обновление программ и программмного обеспечения КСК (при наличии).

Действия эксперта:

НС.5-1. Эксперт проводит анализ правил [b] и проверяет, что правила разрешают устанавливать только те программы и обновления программного обеспечения КСК из списка [a], целостность и подлинность которых подтверждена системной средой.

НС.5-2. Эксперт проверяет, что правила [b] отражены в руководстве администратора из списка [c] в виде однозначных инструкций администратору.

НС.5-3. Эксперт проводит выборочное тестирование компонентов [d] и проверяет, что в СКЗИ действительно применяются механизмы ограничения установки программ и обновлений программного обеспечения КСК в соответствии с [b].

Эксперт использует список программ и обновлений программного обеспечения КСК, полученный на шаге НС.5-1.

Требование НС.6 (3, 4). В системной среде должно быть запрещено устанавливать дополнительные программы. Возможно только обновление программ СКЗИ.

Входные данные:

a) настройка среды для защиты системных объектов;

b) список руководств;

c) компоненты СКЗИ, используемые при обновлении программ (при наличии).

Действия эксперта:

НС.6-1. Эксперт проводит анализ правил [b] и проверяет, что правила запрещают устанавливать дополнительные программы, возможно только обновление программ СКЗИ.

НС.6-2. Эксперт проверяет, что правила [b] отражены в руководстве администратора из списка [c] в виде однозначных инструкций администратору.

НС.6-3. Эксперт проводит выборочное тестирование компонентов [c] и проверяет, что в СКЗИ действительно применяются механизмы ограничения установки программ в соответствии с [b].

Эксперт использует список программ, полученный на шаге НС.6-1.

6.15 Проверка требований к доверенному каналу

Требование ДК.1 (1–4). В руководствах должны быть представлены {РД.1, РД.2} правила настройки клиентской программы, которая используется для связи между удаленным оператором и СКЗИ, а также правила настройки системной среды клиентской программы. Правила настройки системной среды клиентской программы должны соответствовать правилам настройки системной среды СКЗИ.

Входные данные:

a) настройка среды для безопасной установки;

b) настройка среды для защиты системных объектов;

c) настройка среды для защиты сеансов;

d) список ролей операторов;

e) список руководств.

Действия эксперта:

ДК.1-1. Эксперт проверяет, что в руководствах из списка [e] отражены в виде однозначных инструкций администратору СКЗИ из списка [d] правила настройки клиентской программы, которая используется для связи между удаленным оператором и СКЗИ, а также правила настройки системной среды клиентской программы.

ДК.1-2. Эксперт проводит анализ правил [a, b, c] и руководств [e] и проверяет соответствие правил настройки системной среды клиентской программы, приведенных в руководствах [e], правилам настройки системной среды СКЗИ [a, b, c].

Требование ДК.2 (1–4). Клиентская программа должна удовлетворять требованиям настоящего стандарта.

Входные данные:

a) протоколы испытаний (сертификат соответствия) клиентской программы по требованиям Стандарта.

Действия эксперта:

ДК.2-1. Эксперт проверяет, что в соответствии со свидетельствами [a] клиентская программа удовлетворяет требованиям Стандарта.

Эксперт ДОЛЖЕН проверить совпадение испытанной клиентской программы с представленной.

Требование ДК.3 (2–4). При аутентификации удаленного оператора должно использоваться не менее двух факторов аутентификации.

Входные данные:

a) методы идентификации операторов (только удаленного оператора);
b) методы аутентификации операторов (только удаленного оператора);
c) список ролей операторов (только удаленного оператора);
d) список руководств.

Действия эксперта:

ДК.3-1. Эксперт проводит анализ спецификаций [a, b] и проверяет, что выполняются следующие условия:

1 В спецификации [a] описаны правила назначения удаленным операторам уникальных идентификаторов.

2 В руководстве администратора [d] представлены правила связывания идентификаторов [a] с ролями удаленного оператора из списка [c].

3 В спецификации [b] описаны аутентификационные данные для идентификатора удаленного оператора из [a].

Эксперт ДОЛЖЕН определить:

1 К какому фактору аутентификации (из списка «что я знаю», «чем я владею», «кто я») относятся аутентификационные данные удаленного оператора.

2 Являются ли аутентификационные данные удаленного оператора секретами.

3 Какие устройства нужны для ввода аутентификационных данных удаленного оператора.

ДК.3-2. Эксперт проводит анализ спецификации [b], используя результаты выполнения шага ДК.3-1 (определение факторов аутентификации). Эксперт проверяет, что для аутентификации удаленного оператора используется не менее двух факторов.

Требование ДК.4 (1–4). Должна проводиться встречная аутентификация СКЗИ перед удаленным оператором. Вероятность пройти аутентификацию, не зная секрета аутентификации, не должна превышать 2^{-64}.

Входные данные:

a) встречная аутентификация.

Действия эксперта:

ДК.4-1. Эксперт проводит анализ спецификации [a] и оценивает мощность множества секретов аутентификации. Эксперт проверяет, что мощность множества секретов не меньше 2^{64}.

Требование ДК.5 (1–4). У удаленного оператора должна быть возможность завершить сеанс в любой момент времени. Сеанс должен автоматически завершаться при отсутствии активности оператора в течение определенного времени.

Входные данные:

a) уровень (1, 2, 3 или 4) безопасности СКЗИ;

b) исходные тексты программ, реализующих доверенный канал;

c) компоненты СКЗИ, реализующие доверенный канал.

Действия эксперта:

ДК.5-1. Эксперт проводит выборочный (если уровень [a] равен 1 или 2) или подробный (если уровень [a] равен 3 или 4) анализ исходных текстов [b] и (или), соответственно, выборочное или подробное тестирование компонентов [c] и проверяет корректность программной реализации сеанса удаленного оператора.

Эксперт ДОЛЖЕН проверить, что сеанс удаленного оператора реализован так, что выполняются следующие условия:

1 Удаленный оператор имеет возможность завершить сеанс в любой момент времени.

2 Сеанс автоматически завершается при отсутствии активности оператора в течение определенного времени.

Требование ДК.6 (1–4). Должны быть обеспечены конфиденциальность, контроль целостности и подлинности данных обмена между удаленным оператором и СКЗИ. Для защиты должны использоваться криптографические методы. Ключи защиты должны обновляться в каждом новом сеансе оператора.

Примечание — Сеанс оператора можно сохранить (кэшировать), а затем возобновить. При возобновлении сеанса ключи защиты обновлять необязательно.

Входные данные:

a) защита канала;

b) криптографические методы обеспечения конфиденциальности;

c) криптографические методы контроля целостности и подлинности.

Действия эксперта:

ДК.6-1. Эксперт проводит анализ спецификации [a] и проверяет, что конфиденциальность данных обмена между удаленным оператором и СКЗИ обеспечивается с помощью методов из списка [b].

ДК.6-2. Эксперт проводит анализ спецификации [a] и проверяет, что контроль целостности и подлинности данных обмена между удаленным оператором и СКЗИ обеспечивается с помощью методов из списка [c].

ДК.6-3. Эксперт проводит анализ спецификации [a] и проверяет, что ключи защиты, используемые в соответствии с [a] для обеспечения конфиденциальности, контроля целостности и подлинности данных обмена между удаленным оператором и СКЗИ, обновляются в каждом новом сеансе оператора.

При этом эксперт учитывает, что сеанс оператора можно сохранить (кэшировать), а затем возобновить без необходимости обновления ключей защиты.

Требование ДК.7 (1–4). Если ключи защиты [ДК.6] формируются на основании пароля удаленного оператора, то этот пароль должно быть вычислительно трудно определить по данным обмена между оператором и СКЗИ.

Входные данные:

а) защита канала.

Действия эксперта:

ДК.7-1. Эксперт проводит анализ спецификации [а] и проверяет надежность формирования ключей защиты, используемых в соответствии с [а] для обеспечения конфиденциальности, контроля целостности и подлинности данных обмена между удаленным оператором и СКЗИ.

Эксперт ДОЛЖЕН проверить, что в соответствии со спецификацией [а] гарантируется, что если ключи защиты формируются на основании пароля удаленного оператора, то по данным обмена между оператором и СКЗИ определить этот пароль вычислительно трудно.

В отчете по результатам испытаний эксперт приводит оценку вычислительной сложности определения пароля по данным обмена между удаленным оператором и СКЗИ.

Требование ДК.8 (3, 4). Ключи защиты [ДК.6] должны формироваться так, чтобы их было вычислительно трудно определить даже после раскрытия долговременных ключей и паролей удаленного оператора.

Входные данные:

а) защита канала.

Действия эксперта:

ДК.8-1. Эксперт проводит анализ спецификации [а] и проверяет надежность формирования ключей защиты, используемых в соответствии с [а] для обеспечения конфиденциальности, контроля целостности и подлинности данных обмена между удаленным оператором и СКЗИ.

Эксперт ДОЛЖЕН проверить, что в соответствии со спецификацией [а] гарантируется, что по данным обмена между оператором и СКЗИ определить ключи защиты вычислительно трудно, даже после раскрытия долговременных ключей и паролей удаленного оператора.

В отчете по результатам испытаний эксперт приводит оценку вычислительной сложности определения ключей защиты по данным обмена между удаленным оператором и СКЗИ, в том числе после раскрытия долговременных ключей и паролей удаленного оператора.

Требование ДК.9 (4). Ключи защиты [ДК.6] должны формироваться так, чтобы их было вычислительно трудно определить даже после раскрытия долговременных ключей СКЗИ.

Входные данные:

а) защита канала.

Действия эксперта:

ДК.9-1. Эксперт проводит анализ спецификации [а] и проверяет надежность формирования ключей защиты, используемых в соответствии с [а] для обеспечения конфиденциальности, контроля целостности и подлинности данных обмена между удаленным оператором и СКЗИ.

Эксперт ДОЛЖЕН проверить, что в соответствии со спецификацией [a] гарантируется, что по данным обмена между оператором и СКЗИ определить ключи защиты вычислительно трудно, даже после раскрытия долговременных ключей СКЗИ.

В отчете по результатам испытаний эксперт приводит оценку вычислительной сложности определения ключей защиты по данным обмена между удаленным оператором и СКЗИ, в том числе после раскрытия долговременных ключей СКЗИ

Требование ДК.10 (3, 4). Открытие и закрытие доверенного канала должны регистрироваться {АУ.2} в журнале аудита. Запись аудита должна идентифицировать клиентскую программу.

Входные данные:

a) перечень регистрируемых событий;

b) исходные тексты программ, реализующих доверенный канал;

c) компоненты СКЗИ, реализующие доверенный канал.

Действия эксперта:

ДК.10-1. Эксперт проводит анализ перечня [a] и проверяет, что в перечнь событий, регистрируемых в журнале аудита, включены события открытия и закрытия доверенного канала.

ДК.10-2. Эксперт проводит подробный анализ исходных текстов [b] и (или) подробное тестирование компонентов [c] и проверяет корректность аудита событий использования доверенного канала.

Эксперт ДОЛЖЕН проверить, что при использовании доверенного канала выполняются следующие условия:

1 В журнале аудита регистрируются события открытия и закрытия доверенного канала.

2 Запись аудита идентифицирует клиентскую программу.

6.16 Проверка требований по проектированию и разработке

Требование ПР.1 (1–4). Должны быть разработаны описания программ и аппаратных компонентов СКЗИ. Описания должны соответствовать функциональной спецификации.

Входные данные:

a) основные функциональные возможности;

b) описания программ и аппаратных компонентов.

Действия эксперта:

ПР.1-1. Эксперт проверяет, что в [b] представлена следующая информация о программах СКЗИ:

1 Функциональное назначение программ (классы решаемых задач, ограничения на применения).

2 Описание логической структуры программ (структура программ с описанием функций составных частей и связей между ними, связи между программами).

3 Вызов и загрузка программ.

4 Входные и выходные данные программ (организация ввода/вывода, форматы данных).

ПР.1-2. Если разработчик СКЗИ заявил о соответствии программ из списка [b] стандарту ГОСТ 19.409-78 «Единая система программной документации. Описание программы», то эксперт проверяет данное соответствие.

ПР.1-3. Если разработчик СКЗИ заявил описание программы из списка [b] в виде комплекта программной документации в соответствии с номенклатурой ГОСТ 19.101, то эксперт проверяет соответствие представленного комплекта программной документации требованиям ЕСПД.

ПР.1-4. Эксперт проверяет, что в [b] представлена следующая информация об аппаратных компонентах СКЗИ:

1 Описание технической характеристики (функциональное назначение, основные технические характеристики).

2 Описание конструкции (сборочный чертеж, чертеж общего вида).

3 Описание структурной схемы (состав, описание структурной и (или) функциональной схемы).

4 Описание схемотехнической реализации (схема электрическая принципиальная, перечень элементов).

5 Использование по назначению (эксплуатационные ограничения, подготовка к эксплуатации, использование, техническое обслуживание).

ПР.1-5. Если разработчик СКЗИ заявил описание аппаратных компонентов из списка [b] в виде комплекта конструкторской документации в соответствии с номенклатурой ГОСТ 2.102, то эксперт проверяет соответствие представленного комплекта конструкторской документации требованиям ЕСКД.

ПР.1-6. Эксперт проверяет соответствие между описанием функционального назначения в [b] и функциональной спецификацией [a].

Требование ПР.2 (1–4). В описаниях [ПР.1] должны быть определены внешние интерфейсы СКЗИ.

Действия эксперта: проверка ПР.2 покрывается проверками по [РС.1].

Требование ПР.3 (2–4). В описаниях [ПР.1] должны быть определены внутренние компоненты СКЗИ и их интерфейсы.

Входные данные:

a) внутренние компоненты и интерфейсы;
b) описания программ и аппаратных компонентов;
c) исходные тексты программ СКЗИ;
d) аппаратные компоненты СКЗИ;
e) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ПР.3-1. Эксперт проверяет, что в [a] и (или) [b] представлена следующая информация:

1 Список внутренних компонентов и их функциональное назначение.

2 Логические интерфейсы внутренних программных компонентов (прототипы экспортируемых функций динамической библиотеки).

3 Логические и физические интерфейсы аппаратных компонентов.

4 Связи между компонентами.

ПР.3-2. Эксперт проводит выборочный (если уровень [e] равен 2) или подробный (если уровень [e] равен 3 или 4) анализ исходных текстов [c] и, соответственно, выборочное или подробное тестирование аппаратных компонентов [d] и проверяет наличие компонентов, соответствующих [a] и [b].

Требование ПР.4 (1–4). В описаниях [ПР.1] должны быть определены используемые средства разработки и сборки программ. Должны быть перечислены конфигурационные файлы, отвечающие за настройку средств разработки и сборки.

Входные данные:

a) средства разработки (описание);

b) система управления конфигурацией (развернута разработчиком СКЗИ);

c) исходные тексты программ СКЗИ (в том числе конфигурационные файлы).

Действия эксперта:

ПР.4-1. Эксперт проверяет, что в [a] представлена следующая информация:

1 Какие средства используются для разработки и сборки, в том числе версия средств (например, MS Visual Studio 9 и выше).

2 Какие файлы отвечают за конфигурацию средств (например, файл проекта Visual Studio с расширением vcproj).

ПР.4-2. Эксперт проводит компиляцию и сборку программ [c], используя систему [b].

Эксперт ДОЛЖЕН убедиться, что при компиляции и сборке не требуются дополнительные настройки, не включенные в конфигурационные файлы.

Требование ПР.5 (1–4). Исходные тексты программ должны быть снабжены комментариями, отражающими связь программ с описаниями [ПР.1].

Входные данные:

a) исходные тексты программ СКЗИ;

b) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ПР.5-1. Эксперт проводит выборочный (если уровень [b] равен 1 или 2) или подробный (если уровень [b] равен 3 или 4) анализ исходных текстов [a] и проверяет, что программы достаточно прокомментированы.

Эксперт ДОЛЖЕН убедиться, что Комментарии к исходному тексту программ достаточны для понимания логики работы программы.

Требование ПР.6 (1–4). Программы должны быть написаны на высокоуровневых языках программирования. Вставки на низкоуровневых языках (языках ассемблера) допускаются в случаях, критичных для производительности, а также тогда, когда высокоуровневые языки применить нельзя.

Примечание 1 — Низкоуровневые языки предназначены для прямой работы с инструкциями процессора. Напротив, в высокоуровневых языках архитектура процессора абстрагируется, используются конструкции, удобные программистам и поэтому лучше читаемые, более управляемые и менее подверженные ошибкам.

Входные данные:

a) языки программирования (описание);

b) исходные тексты программ СКЗИ;

c) уровень (1, 2, 3 или 4) безопасности СКЗИ.

Действия эксперта:

ПР.6-1. Эксперт проводит выборочный (если уровень [c] равен 1 или 2) или подробный (если уровень [c] равен 3 или 4) анализ исходных текстов [b] и проверяет, что программы написаны на языках программирования, заданных в [a].

ПР.6-2. Эксперт проводит выборочный (если уровень [c] равен 1 или 2) или подробный (если уровень [c] равен 3 или 4) анализ исходных текстов [b] и выделяет фрагменты программ, написанные на низкоуровневых языках.

Эксперт проверяет, что вставки на низкоуровневых языках необходимы, потому что:

1 Использование ассемблерных команд существенно повышает производительность программ.

2 В ассемблерных командах используются специальные возможности аппаратной среды, которые нельзя задействовать на высокоуровневых языках.

Требование ПР.7 (4). В состав СКЗИ должно быть включено {ПР.1} программное обеспечение КСК.

Примечание 2 — Включение программного обеспечения в состав СКЗИ означает взятие его под контроль — тестирование {ПИ.3} и анализ исходных текстов {АП.5}. Операционная система, если она имеется, также подпадает под контроль. Речь может идти о специализированной системе (системном программном обеспечении) собственной разработки, об облегченной универсальной (встраиваемой, embedded) системе с открытым кодом, а также о других вариантах исполнения, допускающих тестирование и анализ исходных текстов.

Входные данные:

a) список критических системных компонентов;

b) описания программ и аппаратных компонентов;

c) исходные тексты программ СКЗИ.

Действия эксперта:

ПР.7-1. Эксперт проводит анализ [a] и [b] и проверяет, что в [b] представлено описание программ КСК из списка [a].

ПР.7-2. Эксперт проводит подробный анализ исходных текстов [c] и проверяет наличие исходных текстов программ КСК из списка [a].

6.17 Проверка требований по поддержке жизненного цикла

Требование ЖЦ.1 (1–4). Должна быть определена и реализована система управления конфигурацией для СКЗИ. Система должна обеспечивать:

- контроль доступа разработчиков к элементам конфигурации;
- контроль версий элементов конфигурации;
- отслеживание изменений элементов конфигурации;
- сборку программ по исходным текстам [ПР.4].

Входные данные:

a) система управления конфигурацией (описание).

b) система управления конфигурацией (развернута разработчиком СКЗИ).

Действия эксперта:

ЖЦ.1-1. Эксперт анализирует описание [a] и определяет список контролируемых элементов конфигурации.

Эксперт ДОЛЖЕН проверить, что список содержит следующие элементы:

1 Функциональная спецификация.

2 Программы.

3 Описания программ и аппаратных компонентов.

4 Исходные тексты программ.

5 Конфигурационные файлы средств разработки и сборки программ.

6 Документация по управлению конфигурацией [a].

7 Документация по поставке СКЗИ потребителям.

8 Документация по устранению недостатков (начиная с уровня 2).

9 Руководства.

ЖЦ.1-2. Эксперт проверяет, что развернутая система [b] соответствует описанию [a]. Эксперт изучает [b] и, при необходимости, уточняет положения спецификации [a].

ЖЦ.1-3. Эксперт проводит анализ спецификации [a], выполняет тестирование системы [b] и проверяет полноту системы управления конфигурацией.

Эксперт ДОЛЖЕН проверить, что для каждого элемента конфигурации из списка, составленного при выполнении шага ЖЦ.1-1, система обеспечивает:

1 Управление доступом разработчиков к элементу.

2 Запрет на одновременное изменение элемента несколькими разработчиками.

3 Аудит изменений элемента (кто вносил изменения, когда).

4 Сохранение нескольких предыдущих версий элемента и откат к этим версиям.

5 Присвоение версиям элементов уникальных идентификаторов. Идентификаторы промежуточных версий могут устанавливаться неявно, во внутренних структурах системы управления конфигурацией. Идентификаторы окончательных («устойчивых») версий должны устанавливаться так, чтобы быть доступными вне системы управления конфигурацией. Идентификаторы окончательных версий могут устанавливиться вручную (задание децимального номера, инкремент версии файла программы).

Примечание 1 — Управление элементами конфигурации может быть организовано общими средствами операционной системы (настройка разрешений доступа к каталогам и файлам, резервное сохранение, аудит) или с помощью специализированных программ (CVS, Subversion, SourceSafe).

Примечание 2 — Проверка сборки программ по исходным текстам поддерживается проверками по ПР.4.

Требование ЖЦ.2 (1–4). В перечень элементов конфигурации должны быть включены:
- функциональная спецификация;
- программы;
- описания программ и аппаратных компонентов [ПР.1];
- исходные тексты программ;
- конфигурационные файлы средств разработки и сборки программ [ПР.4];
- документация по управлению конфигурацией [ЖЦ.1];
- документация по поставке СКЗИ потребителям [ЖЦ.4];
- документация по устранению недостатков [ЖЦ.6] (начиная с уровня 2);
- руководства [РД.1, РД.2].

Действия эксперта: проверка покрывается проверками по ЖЦ.1.

Требование ЖЦ.3 (1–4). Каждая версия каждого элемента конфигурации должна быть снабжена уникальным идентификатором.

Действия эксперта: проверка покрывается проверками по ЖЦ.1.

Требование ЖЦ.4 (1–4). Должен быть определен порядок поставки СКЗИ потребителям.

Входные данные:

a) система поставки СКЗИ потребителю (описание);

b) список руководств;

c) система поставки СКЗИ потребителю (развернута разработчиком СКЗИ);

d) СКЗИ, готовое к установке (вводу в эксплуатацию).

Действия эксперта:

ЖЦ.4-1. Эксперт анализирует спецификацию [a] и проверяет, что в ней отражены следующие аспекты:

1 Каналы поставки (через Интернет, точки распространения).

2 Комплект поставки.

3 Установка (ввод в эксплуатацию).

4 Активация (при необходимости).

5 Обратная связь с разработчиком.

ЖЦ.4-2. Эксперт проверяет, что заданные в [b] инструкции по установке и активации СКЗИ соответствуют описанию [a].

ЖЦ.4-3. Эксперт проверяет, что развернутая система [c] соответствует описанию [a].

ЖЦ.4-4. Эксперт проводит контрольную установку (ввод в эксплуатацию) СКЗИ [d]. При необходимости, эксперт проводит контрольную активацию.

Требование ЖЦ.5 (2–4). Если в комплект поставки СКЗИ входят инсталляционные программы, то должны быть предусмотрены средства контроля их целостности и подлинности после доставки потребителям.

Входные данные:

a) система поставки СКЗИ потребителю (описание);

b) методы контроля инсталляционных программ;

c) система поставки СКЗИ потребителю (развернута разработчиком СКЗИ);

d) СКЗИ, готовое к установке (вводу в эксплуатацию).

Действия эксперта:

ЖЦ.5-1. Эксперт проводит анализ системы поставки [a] и методов контроля [b]. Если в комплект поставки СКЗИ входят инсталляционные программы, эксперт проверяет, что выбран один из следующих методов контроля:

1 Вычисление и проверка контрольных сумм. Эталонные контрольные суммы указываются в достоверном источнике, например, на сайте разработчика.

2 Вычисление и проверка ЭЦП. ЭЦП вычисляется на личном ключе разработчика. Соответствующий открытый ключ распространяется достоверным образом, например, в виде сертификата.

3 Контроль целостности выполняется во время он-лайн активации СКЗИ.

ЖЦ.5-2. Эксперт анализирует [a], использует [c, d] и проверяет, что методы контроля [b] действительно применяются.

Требование ЖЦ.6 (2–4). Должна быть определена и реализована система устранения недостатков СКЗИ. Система должна обеспечивать:

– регистрацию недостатков;

– управление выявлением причин недостатков и исправлением недостатков;

– отслеживание статуса недостатков (подтвержден, исправляется, исправлен и др.);

– протоколирование способа устранения недостатков;

– извещение потребителей об устранении недостатков.

Входные данные:

a) система управления конфигурацией (описание);

b) система управления конфигурацией (развернута разработчиком СКЗИ).

Действия эксперта:

ЖЦ.6-1. Эксперт анализирует спецификацию [a] и проверяет, что в ней описана система устранения недостатков.

Эксперт ДОЛЖЕН проверить, что система поддерживает следующие возможности:

1 Регистрация недостатков.

2 Порядок выявления причин недостатков.

3 Порядок исправления недостатков, в том числе отслеживание статуса исправления.

4 Протоколирование способа устранения недостатка.

5 Порядок извещения потребителей об устранении недостатков.

ЖЦ.6-2. Эксперт проверяет, что развернутая система [b] соответствует описанию [a] в части устранения недостатков.

Требование ЖЦ.7 (1–4). При применении пакета ОП должна быть определена и реализована система обновления программ СКЗИ. Система должна обеспечивать:
– выпуск обновлений;
– извещение потребителей о выпуске обновлений (с указанием содержания обновлений);
– поставку обновлений потребителям.

Входные данные:
a) уровень (1, 2, 3 или 4) безопасности СКЗИ;
b) система управления конфигурацией (описание);
c) система поставки СКЗИ потребителю (развернута разработчиком СКЗИ).

Действия эксперта:

ЖЦ.7-1. Если заявленный разработчиком уровень [a] усилен пакетом ОП, эксперт анализирует спецификацию [b] и проверяет, что в ней описана система обновления программ СКЗИ.

Эксперт ДОЛЖЕН проверить, что система поддерживает следующие возможности:
1 Выпуск обновлений.
2 Извещение потребителей о выпуске обновлений (с указанием содержания обновлений).
3 Поставку обновлений потребителям.

ЖЦ.7-2. Если заявленный разработчиком уровень [a] усилен пакетом ОП, эксперт проверяет, что развернутая система [c] соответствует описанию [b] в части обновления программ.

6.18 Проверка требований к руководствам

Требование РД.1 (1–4). Должно быть разработано руководство администратора. Руководство должно описывать:
– обязанности администратора по настройке среды [НС.1, НС.2, НС.3];
– инструкции по установке СКЗИ [НС.1];
– доступные администратору сервисы [УД.3] с указанием допустимых последовательностей их вызовов [РС.1];
– обязанности администратора по настройке механизмов безопасности СКЗИ;
– связанные с безопасностью предположения относительно поведения операторов.
Руководство должно описывать обязанности администратора по отслеживанию уязвимостей КСК [НС.4], если такое отслеживание предусмотрено.

Входные данные:
a) список руководств.

Действия эксперта:

РД.1-1. Эксперт проверяет, что в руководстве администратора из списка [a] определены обязанности администратора по обеспечению безопасности и даны предположения относительно поведения операторов.

Эксперт ДОЛЖЕН проверить, что в руководстве описаны следующие аспекты безопасности:

1 Хранение личных и секретных ключей, а также секретов аутентификации в тайне.

2 Необходимость реагирования на сообщения СКЗИ, связанные с безопасностью.

3 Планирование работ по настройке и обновлению СКЗИ.

4 Порядок взаимодействия с операторами.

РД.1-2. Если разработчик СКЗИ заявил о соответствии руководства [a] стандарту ГОСТ 19.505-79 «Единая система программной документации. Руководство оператора», то эксперт проверяет данное соответствие.

Примечание — Проверка руководства администратора подерживается также проверками по РС.1, УД.3, НС.1 – НС.4.

Требование РД.2 (1–4). Для каждой роли [УД.1], отличной от роли «Администраторы», должно быть разработано руководство ее операторов. Руководство должно определять:

– доступные оператору сервисы [УД.3] с указанием допустимых последовательностей их вызовов [РС.1];

– обязанности оператора по обеспечению безопасности СКЗИ.

Входные данные:

а) список руководств (кроме руководства администратора).

Действия эксперта:

РД.2-1. Эксперт проверяет, что во всех руководствах [a] определены обязанности оператора по обеспечению безопасности.

Эксперт ДОЛЖЕН проверить, что в руководствах описаны следующие аспекты безопасности:

1 Хранение личных и секретных ключей, а также секретов аутентификации в тайне.

2 Необходимость реагирования на сообщения СКЗИ, связанные с безопасностью.

3 Порядок взаимодействия с администратором в необходимых случаях.

РД.2-2. Если разработчик СКЗИ заявил о соответствии руководства [a] стандарту ГОСТ 19.505-79 «Единая система программной документации. Руководство оператора», то эксперт проверяет данное соответствие.

Примечание — Проверка руководств подерживается также проверками по РС.1, УД.3.

Требование РД.3 (2–4). Руководства [РД.1, РД.2] должны описывать типичные ошибки операторов, которые могут привести к снижению безопасности СКЗИ. Руководства должны давать рекомендации операторам по избежанию ошибок.

Входные данные:

а) типичные ошибки операторов.

Действия эксперта:

РД.3-1. Эксперт проверяет, что в каждом из руководств [a] описываются типичные ошибки операторов определенной роли.

РД.3-2. Эксперт проводит оценку полноты списков ошибок из [a].

Эксперт ДОЛЖЕН проверить, что описаны следующие типы ошибок (в необходимых случаях):

1 Администратор не задал определенные настройки.

2 Администратор не выполнил регламентные работы.

3 Оператор не проверил состояние среды перед работой с СКЗИ (не проверил состояние антивирусных программ).

4 Оператор не обновил системные объекты (программы СКЗИ).

5 Оператор нарушил последовательность действий (вызова сервисов).

6.19 Проверка требований к программе испытаний

Требование ПИ.1 (1–4). Должна быть разработана программа испытаний СКЗИ разработчиком. Программа должна определять:

- планы тестирования;
- содержание тестов;
- ожидаемые результаты выполнения тестов;
- фактические результаты выполнения тестов.

Входные данные:

a) программа испытаний;

b) компоненты СКЗИ, подготовленные к тестированию.

Действия эксперта:

ПИ.1-1. Эксперт проверяет, что в [a] представлена следующая информация:

1 Средства и порядок испытаний (используемые технические и программные средства, организация испытаний).

2 Методы испытаний, в том числе перечень тестов, содержание тестов, ожидаемые и фактические результаты выполнения тестов.

ПИ.1-2. Если разработчик СКЗИ заявил о соответствии [a] стандарту ГОСТ 19.301-79 «Единая система программной документации. Программа и методика испытаний», то эксперт проверяет данное соответствие.

ПИ.1-3. Эксперт проводит для [b] выборочные тесты из [a]. Эксперт проверяет, что полученные результаты соответствуют ожидаемым и фактическим результатам, приведенным в [a].

Требование ПИ.2 (1–4). Тесты программы испытаний [ПИ.1] должны покрывать все функциональные возможности СКЗИ, определенные в функциональной спецификации.

Входные данные:

a) основные функциональные возможности;

b) программа испытаний;

c) результаты анализа покрытия тестами.

Действия эксперта:

ПИ.2-1. Эксперт использует [c] и проверяет, что тесты [b] покрывают функциональные возможности СКЗИ, перечисленные в [a].

Требование ПИ.3 (2–4). Тесты программы испытаний [ПИ.1] должны покрывать функциональные возможности всех компонентов СКЗИ, определенных в описаниях [ПР.1].

Входные данные:

a) внутренние компоненты и интерфейсы;

b) программа испытаний;

c) результаты анализа глубины тестирования.

Действия эксперта:

ПИ.3-1. Эксперт использует [c] и проверяет, что тесты [b] покрывают функциональные возможности компонентов СКЗИ, перечисленных в [a].

Примечание — Внутренние компоненты СКЗИ могут тестироваться прямо, через свои интерфейсы, либо косвенно, через внешние интерфейсы всего СКЗИ. В [c] должны быть указаны прямые тесты, либо даны разъяснения относительно косвенного тестирования.

6.20 Проверка требований к анализу программ

Требование АП.1 (1–4). Заключение эксперта по анализу исходных текстов должно содержать перечень проверенных программных модулей, уровень проверки (полно, подробно, выборочно), контрольные характеристики модулей, результаты анализа.

Примечание — Заключение может содержать рекомендации.

Входные данные:

a) заключения экспертов по анализу исходных текстов.

Действия эксперта:

АП.1-1. Эксперт проводит анализ заключений [a] и проверяет, что каждое из них содержит:

1 Перечень проверенных программных модулей.

2 Уровень проверки (полно, подробно, выборочно).

3 Контрольные характеристики проверенных программных модулей.

4 Результаты анализа программных модулей, включая рекомендации по устранению недостатков (при наличии рекомендаций).

Требование АП.2 (1–4). Должен быть проведен полный анализ исходных текстов программных реализаций криптографических алгоритмов.

Действия эксперта: проверка [АП.2] покрывается проверками по [КП.1].

Требование АП.3 (1–4). Должен быть проведен анализ корректности встраивания реализаций криптографических алгоритмов в программы СКЗИ.

Действия эксперта: проверка [АП.3] покрывается проверками по [РС.1], [ЗО.3], [ЗО.4], [ЗО.6].

Требование АП.4 (2). Должен быть проведен выборочный анализ программ СКЗИ.

Входные данные:

a) описания программ и аппаратных компонентов (только описания программ);

b) исходные тексты программ СКЗИ.

Действия эксперта:

АП.4-1. Эксперт проводит выборочный анализ исходных текстов программных реализаций [b] и проверяет их корректность. Корректность означает, что реализация соответствует описанию в [a] и не содержит ошибок и уязвимостей.

При анализе эксперт ДОЛЖЕН использовать проверки, определенные в Приложении В.

При проверке [АП.4] эксперт использует результаты проверок по [КП.1], [РС.1], [РС.4], [РС.5], [УД.1], [УД.2], [УД.3], [УД.4], [ЗО.3], [ЗО.4], [ЗО.5], [ЗО.6], [ЗО.7], [ЗО.9], [ЗО.10], [ЗО.12], [СТ.2], [СТ.3], [СЧ.5], [СЧ.6], [СЧ.7], [ОП.2], [ОП.3], [ОП.5], [ИА.3], [ДК.5], [ПР.3], [ПР.5], [ПР.6].

Требование АП.5 (3, 4). Должен быть проведен подробный анализ программ СКЗИ.

Входные данные:

a) описания программ и аппаратных компонентов (только описания программ);

b) исходные тексты программ СКЗИ.

Действия эксперта:

АП.5-1. Эксперт проводит подробный анализ исходных текстов программных реализаций [b] и проверяет их корректность. Корректность означает, что реализация соответствует описанию в [a] и не содержит ошибок и уязвимостей.

При анализе эксперт ДОЛЖЕН использовать проверки, определенные в Приложении В.

При проверке [АП.5] эксперт использует результаты проверок по [КП.1], [РС.1], [РС.4], [РС.5], [УД.1], [УД.2], [УД.3], [УД.4], [ЗО.3], [ЗО.4], [ЗО.5], [ЗО.6], [ЗО.7], [ЗО.9], [ЗО.10], [ЗО.12], [СТ.2], [СТ.3], [СТ.6], [АУ.1], [АУ.2], [АУ.3], [АУ.4], [ФБ.7], [ЗВ.2], [ЗВ.3], [ЗУ.2], [СЧ.5], [СЧ.6], [СЧ.7], [СЧ.8], [ОП.2], [ОП.3], [ОП.5], [ОП.6], [ОП.7], [ВЭ.5], [ВЭ.6], [ИА.3], [ДК.5], [ДК.10], [ПР.3], [ПР.5], [ПР.6], [ПР.7].

Приложение А
Анализ исходных текстов программных реализаций криптографических алгоритмов и протоколов

При анализе исходных текстов программных реализаций криптографических алгоритмов и протоколов эксперт ДОЛЖЕН выполнить следующие проверки:

А-1 (локальные переменные). Для каждой функции f эксперт проводит оценку корректности использования ее локальных переменных.

Для каждой локальной переменной v функции f эксперт ДОЛЖЕН проверить, что:

1 Перед использованием переменной v выполнена ее инициализация.

2 Обращение на чтение/запись к переменной v происходит в пределах установленных для нее границ; в частности, если v является переменной составного типа (массив), то обращение к элементам v происходит в пределах заданных границ (размер массива).

3 Если v является переменной вещественного типа, то она не используется в операциях сравнениях.

4 Если для v выделяется динамическая память, то перед выходом из f динамическая память освобождается; ссылки на освобожденную память отсутствуют.

Примечание — В языках программирования, снабженных средствами «сборки мусора», освобождение динамической памяти может быть неявным.

А-2 (глобальные переменные). Эксперт проводит оценку корректности использования глобальных переменных.

Для каждой глобальной переменной v эксперт ДОЛЖЕН выполнить проверки 1 – 3 предыдущего шага и следующую дополнительную проверку:

4 Если память для v выделяется в динамической области, то перед каждым выходом из программы динамическая память освобождается; ссылки на освобожденную память отсутствуют.

Примечание — В языках программирования, снабженных средствами «сборки мусора», освобождение динамической памяти может быть неявным.

А-3 (константы). Эксперт должен проверить правильность задания в программе констант, определенных в спецификациях криптографических алгоритмов (протоколов) и в документации СКЗИ.

А-4 (программная логика). Эксперт проводит оценку корректности программной логики функций программы.

Для каждой функции эксперт ДОЛЖЕН проверить, что:

1 Выполняется одно из условий:

– в документации или в комментариях к функции оговорены ограничения на входные данные, и эти ограничения соблюдаются во всех вызовах функции;

– в начале функции выполняется проверка допустимости переданных параметров и используемых глобальных переменных.

2 Все заданные варианты условных переходов возможны.

3 Все адреса безусловных переходов доступны.

4 Каждый цикл завершается за конечное число шагов.

5 Нет недостижимых участков кода.

6 Цепочки последовательных действий (например, открытие файла, чтение из файла, закрытие файла) корректны.

А-5 (вызовы функций программы). Эксперт проводит оценку корректности вызовов функций программы.

Для каждого вызова функции программы эксперт ДОЛЖЕН проверить, что:

1 Типы фактически переданных параметров соответствуют типам формальных параметров, указанных в документации (с учетом стандартных правил преобразования типов языка программирования).

2 Значения передаваемых параметров соответствуют ограничениям, заданным в документации или в комментариях к функции.

3 Возвращаемые значения корректно интерпретируются.

4 Глобальные переменные инициализируются перед их использованием в функции.

5 До и после вызова функции выполняются подготовительные и завершающие действия, оговоренные в документации.

6 Исключительные ситуации, возникающие при выполнении вызываемой функции, корректно обрабатываются.

А-6 (вызовы стандартных функций). Эксперт проводит оценку корректности вызовов стандартных функций.

Для каждого вызова стандартной функции эксперт ДОЛЖЕН выполнить проверки 1 – 3, 5, 6 предыдущего шага.

А-7 (обработка исключительных ситуаций). Эксперт проводит оценку корректности обработки исключительных ситуаций. Эксперт анализирует программную документацию и составляет список функций, которые могут привести к возникновению исключительной ситуации.

Для каждой функции из составленного списка эксперт ДОЛЖЕН проверить, что:

1 После каждого вызова функции имеются проверка на случай возникновения исключительной ситуации и, при необходимости, обработка исключительной ситуации.

2 При проверке и обработке исключительной ситуации учтены все возможные типы исключительных ситуаций.

3 Исключительные ситуации обрабатываются адекватно (выдаются верные сообщения об ошибке).

А-8 (реализация вспомогательных алгоритмов). Эксперт проводит оценку корректности реализации вспомогательных криптографических алгоритмов, заданных в ТНПА на проверяемый криптографический алгоритм или протокол.

Примечание 1 — Вспомогательные алгоритмы могут быть заданы в ТНПА неявно. Например, для многих криптографических алгоритмов с открытым ключом вспомогательными являются алгоритмы арифметики больших чисел. Данные алгоритмы явно в ТНПА не определяются.

Примечание 2 — Вспомогательные алгоритмы могут быть заданы функционально — через описание пар «входы — выходы». Например, сложение точек эллиптической кривой может определяться не как алгоритмическая последовательность шагов, а как отображение «слагаемые $\mapsto$ сумма». Как правило, все неявные алгоритмы задаются функционально. Функционально эквивалентные алгоритмы могут быть устроены по-разному. Поэтому требуется оценка соответствия алгоритмического описания функциональному.

Эксперт ДОЛЖЕН:

1 Используя ТНПА, программную документацию и исходные тексты программ, определить список вспомогательных алгоритмов.

2 Для функционально заданных алгоритмов оценить их соответствие функциональному описанию.

3 Оценить корректность программной реализации вспомогательных алгоритмов.

А-9 (реализация криптографических алгоритмов и протоколов). Эксперт проводит оценку корректности реализации криптографических алгоритмов и протоколов. Эксперт учитывает результаты выполнения предыдущих шагов и проверяет, что реализация функционально соответствует ТНПА на целевой алгоритм или протокол.

Эксперт ДОЛЖЕН проверить, что:

1 Не допускается сужение пространства ключей.

2 Корректно обрабатываются граничные ситуации (например, хэширование пустого сообщения).

3 Корректно обрабатываются исключительные ситуации протоколов (например, нужный пакет не получен, сертификат не действителен).

А-10 (использование ключей). Эксперт проверяет, что личные и секретные ключи используются только для выполнения криптографических преобразований и уничтожаются сразу после использования.

Эксперт ДОЛЖЕН проверить, что уничтожаются все копии ключей в локальных или глобальных переменных.

Для проверки корректности уничтожения ключей эксперт МОЖЕТ воспользоваться результатами проверки ЗО.12.

Приложение Б
Тестирование реализаций криптографических алгоритмов и протоколов

Список тестов. При тестировании реализаций криптографических алгоритмов и протоколов МОГУТ использоваться следующие тесты:

- точечный,
- случайного блуждания,
- прямого и обратного преобразований,
- длин,
- разбиений,
- тождеств.

Точечный тест является обязательным. Если целевой алгоритм поддерживает тест прямого и обратного преобразований, то данный тест также является обязательным.

Эталонная реализация. В тесте случайного блуждания и тесте длин используется эталонная реализация.

Эталонная реализация ДОЛЖНА удовлетворять, по крайней мере, одному из следующих условий:

1 Проведен анализ исходных текстов программ эталонной реализации. К анализу привлекались, по меньшей мере, два независимых эксперта. Использовалась методика анализа исходных текстов, определенная в Приложении А.

2 Проведено тестирование эталонной реализации. Использовались две другие независимые реализации, считавшиеся (в момент тестирования) эталонными. Использовался план тестирования, определенный в данном приложении.

Точечный тест. Испытуемая реализация выполняет преобразование фиксированного блока данных на фиксированном ключе. Результат преобразования сравнивается с эталонным. Эталонным считается результат, который получен с помощью эталонной реализации и зафиксирован в ТНПА или в согласованной Органом по сертификации методике испытаний.

Тест случайного блуждания. Испытуемая и эталонная реализации одновременно выполняют преобразования одинаковых случайных данных на одинаковых случайных ключах. Результаты преобразований сравниваются. Должно быть проведено не менее 8192 случайных экспериментов.

Тест прямого и обратного преобразований. Испытуемая реализация выполняет прямое (например, зашифрование) преобразование случайных данных на случайных ключах. Затем выполняется обратное (например, расшифрование) преобразование. Полученный результат сравнивается с исходными данными. Должно быть проведено не менее 8192 случайных экспериментов.

Для алгоритмов ЭЦП тест состоит сначала в выработке подписи, а затем в проверке того, что подпись верна.

Тест длин. Испытуемая и эталонная реализация одновременно выполняют преобразование случайных блоков данных различных длин на случайных ключах. Результаты преобразований сравниваются. Должно быть проведено не менее 8192 случайных экспериментов.

Тест разбиений. Случайный блок данных разбивается на два последовательных фрагмента различными способами. Выполняется преобразование блока на случайных ключах и проверяется, что результат преобразования не зависит от способа разбиения на фрагменты. Должно быть проведено не менее 8192 случайных экспериментов.

Тест тождеств. Проверяется, что для испытуемой реализации выполняются известные тождества, связывающие входные данные, выходные данные и ключи.

Примечание — Тождества известны для следующих криптографических алгоритмов:

– алгоритм шифрования блока данных ГОСТ 28147-89 (свойство дополнения, тождество для слабых ключей);

– алгоритм шифрования блока данных DES (свойство дополнения, тождество для слабых ключей);

– алгоритм шифрования блока данных TripleDES (свойство дополнения, тождество для слабых ключей, редукция к DES).

Приложение В
Анализ исходных текстов программ

При анализе исходных текстов программных реализаций эксперт ДОЛЖЕН проверить, что в программах СКЗИ соблюдаются следующие условия:

1 Переменные инициализируются перед использованием.

2 Не нарушаются границы массивов.

3 Переменные вещественного типа (с плавающей точкой) не используются в операциях сравнения.

4 Динамическая память освобождается.

5 Фрагменты памяти (переменные) с критическими данными очищаются перед завершением работы с ними.

6 Оптимизатор не отключает бесполезную (на его взгляд) очистку.

7 Все разобранные варианты условных переходов возможны.

8 Все адреса безусловных переходов доступны.

9 Каждый цикл завершается за конечное число шагов.

10 Нет недостижимых участков кода.

11 Цепочки последовательных действий (например, открытие файла, чтение из файла, закрытие файла) корректны.

12 При вызове функции соблюдается ее интерфейс.

13 Соблюдаются предусловия функций.

14 Возвращаемые функциями значения не игнорируются и корректно интерпретируются.

15 Исключительные ситуации обрабатываются.

16 Учитываются все возможные типы исключительных ситуаций.

17 Пространство ключей не сужается.

18 Используются средства синхронизации (для многозадачных программ).

19 Обрабатываются граничные ситуации криптографических алгоритмов (например, хэширование пустого сообщения).

20 Обрабатываются исключительные ситуации криптографических протоколов (например, обрыв связи).