Утвержден ФСТЭК России
14 июня 2012 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ ТИПА «Б» ШЕСТОГО КЛАССА ЗАЩИТЫ

ИТ.САВЗ.Б6.ПЗ

Содержание

Перечень сокращений

АРМ – автоматизированное рабочее место
БД ПКВ – база данных признаков вредоносных компьютерных программ (вирусов)
ЗБ – задание по безопасности
ИС – информационная система
ИТ – информационная технология
КВ – вредоносные компьютерные программы (вирусы)
ОДФ – область действия функции безопасности
ОО – объект оценки
ОУД – оценочный уровень доверия
ПБО – политика безопасности объекта оценки
ПЗ – профиль защиты
ПО – программное обеспечение
САВЗ – средство антивирусной защиты
УК – управление конфигурацией
ФБО – функции безопасности объекта оценки
ФТБ – функциональные требования безопасности

1. Общие положения

Настоящий методический документ ФСТЭК России разработан и утвержден в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и предназначен для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств защиты информации (далее – разработчики), заявителей на осуществление сертификации продукции (далее – заявители), а также испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств защиты информации на соответствие обязательным требованиям по безопасности информации (далее – оценщики) при проведении ими работ по сертификации средств антивирусной защиты (САВЗ) на соответствие Требованиям к средствам антивирусной защиты, утвержденным приказом ФСТЭК России от 20 марта 2012 г. № 28.

Настоящий методический документ ФСТЭК России детализирует и определяет взаимосвязи требований к функциям безопасности САВЗ, установленным Требованиями к средствам антивирусной защиты, утвержденными приказом ФСТЭК России от 20 марта 2012 г. № 28.

Профиль защиты разработан в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

1.1. Введение профиля защиты

Данный раздел содержит информацию общего характера. Подраздел «Идентификация профиля защиты» предоставляет маркировку и описательную информацию, которые необходимы, чтобы контролировать и идентифицировать профиль защиты (ПЗ) и объект оценки (ОО), к которому он относится. Подраздел «Аннотация профиля защиты» содержит общую характеристику ПЗ, позволяющую определить применимость ОО, к которому относится настоящий ПЗ, в конкретной ситуации. В подразделе «Соглашения» дается описание операций конкретизации компонентов требований безопасности САВЗ. В подразделе «Термины и определения» представлены определения основных терминов, специфичных для данного ПЗ. В подразделе «Организация профиля защиты» дается пояснение организации документа.

1.2. Идентификация профиля защиты

Название ПЗ:	Профиль защиты средств антивирусной защиты типа «Б» шестого класса защиты.
Тип САВЗ:	САВЗ типа «Б».
Класс защиты САВЗ:	Шестой.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИТ.САВЗ.Б6.ПЗ.

Идентификация ОО:	САВЗ типа «Б» шестого класса защиты.
Уровень доверия:	Оценочный уровень доверия 1 (ОУД1), усиленный компонентом AVA_SOF.1 «Оценка стойкости функции безопасности ОО» и расширенный компонентами ALC_UPV_EXT.1 «Процедуры обновления БД ПКВ» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность САВЗ».
Идентификация:	Требования к средствам антивирусной защиты, утвержденные приказом ФСТЭК России от 20 марта 2012 г. № 28. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
Ключевые слова:	Средство антивирусной защиты, ОУД1.

1.3. Аннотация профиля защиты

Настоящий ПЗ определяет требования безопасности для САВЗ типа «Б» шестого класса защиты (объекта оценки), предназначенных для применения на серверах информационных систем.

Основными угрозами, для противостояния которым используются САВЗ типа «Б», являются угрозы, связанные с внедрением в информационные системы из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования) и(или) съемных машинных носителей информации, вредоносных компьютерных программ (вирусов) (КВ).

В САВЗ должны быть реализованы следующие функции безопасности:

разграничение доступа к управлению САВЗ;

управление работой САВЗ;

управление параметрами САВЗ;

управление установкой обновлений (актуализации) базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ) САВЗ;

аудит безопасности САВЗ;

выполнение проверок объектов воздействия;

обработка объектов воздействия;

сигнализация САВЗ.

В среде, в которой САВЗ функционирует, должны быть реализованы следующие функции безопасности среды:

обеспечение доверенной связи (маршрута) между САВЗ и пользователями;

обеспечение доверенного канала получения обновлений САВЗ;

обеспечение условий безопасного функционирования;

управление атрибутами безопасности.

Функции безопасности САВЗ должны обладать составом функциональных возможностей, обеспечивающих реализацию этих функций.

В ПЗ изложены следующие виды требований безопасности, предъявляемые к САВЗ:

функциональные требования безопасности;

требования доверия к безопасности.

Функциональные требования безопасности САВЗ, изложенные в ПЗ, включают:

требования к режимам и методам выполнения проверок в целях обнаружения КВ;

требования к функциональным возможностям по обновлению базы данных признаков вредоносных компьютерных программ (вирусов) (БД ПКВ);

требования по управлению режимами выполнения функций безопасности САВЗ (работой САВЗ);

требования по управлению данными функций безопасности (данными САВЗ);

требования по управлению ролями субъектов;

требования к аудиту функционирования САВЗ.

Функциональные требования безопасности для САВЗ выражены на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408-2, при этом часть требований сформулированы в явном виде в стиле компонентов из ГОСТ Р ИСО/МЭК 15408-2.

Состав функциональных требований безопасности (ФТБ), включенных в настоящий ПЗ, обеспечивает следующие функциональные возможности САВЗ:

выполнение проверки с целью обнаружения зараженных КВ объектов;

выполнение проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных;

выполнение проверки с целью обнаружения зараженных КВ объектов по команде; в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; путем запуска с необходимыми параметрами функционирования своего кода внешней программой;

выполнение проверки с целью обнаружения зараженных КВ объектов сигнатурными методами;

удаление (если удаление технически возможно) кода КВ из зараженных объектов;

возможность получения и установки обновлений БД ПКВ без применения средств автоматизации;

генерация записи аудита для событий, подвергаемых аудиту;

чтение информации из записей аудита;

возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;

возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;

поддержка определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами серверов.

Требования доверия к безопасности САВЗ охватывают следующие основные вопросы:

управление конфигурацией;
поставка и эксплуатация;
разработка;
руководства;
поддержка жизненного цикла;
тестирование;
оценка уязвимостей;
обновление САВЗ.

Требования доверия к безопасности САВЗ сформированы на основе компонентов требований из ГОСТ Р ИСО/МЭК 15408–3. При этом часть требований сформулированы в явном виде в стиле компонентов из ГОСТ Р ИСО/МЭК 15408–3.

Требования доверия к безопасности САВЗ образуют оценочный уровень доверия 1 (ОУД1), усиленный компонентом AVA_SOF.1 «Оценка стойкости функции безопасности ОО» и расширенный компонентами ALC_UPV_EXT.1 «Процедуры обновления БД ПКВ» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность САВЗ».

В целях обеспечения условий для безопасного функционирования САВЗ в настоящем ПЗ также определены цели и требования для среды функционирования САВЗ.

1.4. Соглашения

ГОСТ Р ИСО/МЭК 15408 допускает выполнение определенных операций над требованиями безопасности. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор» и «назначение».

Операция **«уточнение»** используется для добавления к требованию некоторых подробностей (деталей) и, таким образом, ограничивает диапазон возможностей его удовлетворения. Результат операции **«уточнение»** в настоящем ПЗ обозначается **полужирным текстом.**

Операция **«выбор»** используется для выбора одного или нескольких элементов из перечня в формулировке требования. Результат операции **«выбор»** в настоящем ПЗ обозначается *подчеркнутым курсивным текстом*.

Операция **«назначение»** используется для присвоения конкретного значения ранее неконкретизированному параметру. Операция **«назначение»** обозначается заключением значения параметра в квадратные скобки, [назначаемое значение].

В настоящем ПЗ используются компоненты требований безопасности, включающие частично выполненные операции **«назначение»** и предполагающие завершение операций в задании по безопасности (ЗБ) В данных компонентах незавершенная часть операции **«назначение»** обозначается как [назначение: *область предполагаемых значений*].

В настоящем ПЗ используются компоненты требований безопасности, включающие незавершенные операции **«назначение»,** в которых область предполагаемых значений уточнена по отношению к исходному компоненту из ГОСТ Р ИСО/МЭК 15408. В данных компонентах операции **«назначение»** с уточненной областью предполагаемых значений обозначаются как [назначение: ***уточненная область предполагаемых значений***].

В настоящий ПЗ включен ряд требований безопасности, сформулированных в явном виде. Краткая форма имен компонентов требований, сформулированных в явном виде, содержит текст (EXT).

Настоящий профиль защиты содержит ряд незавершенных операций над компонентами функциональных требований безопасности. Эти операции должны быть завершены в задании по безопасности на конкретную реализацию САВЗ.

1.5. Термины и определения

В настоящем ПЗ применяются следующие термины с соответствующими определениями.

Администратор безопасности – уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию ОО.

Антивирусная защита – защита информации и компонентов информационной системы (ИС) от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

База данных признаков вредоносных компьютерных программ (вирусов) – составная часть САВЗ, содержащая информацию о вредоносных компьютерных программах (вирусах) (сигнатуры), используемая САВЗ для обнаружения вредоносных компьютерных программ (вирусов) и их обработки.

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки (сертификации) конкретного ОО.

Объект оценки – подлежащее сертификации (оценке) САВЗ с руководствами по эксплуатации.

Политика безопасности ОО – совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых ОО.

Профиль защиты – совокупность требований безопасности для САВЗ типа «Б» второго класса защиты.

Сигнатура – характерные признаки компьютерной вредоносной программы (вируса), используемые для ее обнаружения.

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или

нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

Угроза безопасности информации – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.

Функции безопасности ОО – совокупность всех функций безопасности ОО, направленных на осуществление политики безопасности объекта оценки (ПБО).

1.6. Организация профиля защиты

Раздел 1 «Введение профиля защиты» содержит информацию управления документооборотом и описательную информацию, необходимые для идентификации ПЗ и ОО, к которому он относится.

Раздел 2 «Описание объекта оценки» содержит описание функциональных возможностей ОО, среды функционирования ОО и границ ОО, служащее цели лучшего понимания требований безопасности и дающее представление о типе продукта.

Раздел 3 «Среда безопасности объекта оценки» содержит описание аспектов среды безопасности ОО. В данном разделе определяется совокупность угроз, имеющих отношение к безопасному функционированию ОО, политика безопасности организации, которой должен следовать ОО, и предположения (обязательные условия) безопасного использования ОО.

В разделе 4 «Цели безопасности» определена совокупность целей безопасности для ОО и среды функционирования ОО.

В разделе 5 «Требования безопасности» на основе ГОСТ Р ИСО/МЭК 15408–2 и ГОСТ Р ИСО/МЭК 15408–3 определены, соответственно, функциональные требования безопасности информационных технологий (ИТ) и требования доверия к безопасности ОО.

В Разделе 6 «Обоснование» демонстрируется, что ПЗ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что ОО учитывает идентифицированные аспекты среды безопасности ОО.

2. Описание объекта оценки

2.1. Тип изделия информационных технологий

Объектом оценки в настоящем ПЗ является САВЗ типа «Б».

Объект оценки представляет собой программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации, предназначенное для применения на серверах информационных систем.

2.2. Основные функциональные возможности объекта оценки

В данном подразделе представлено краткое описание функциональных возможностей ОО.

Средства антивирусной защиты, соответствующие настоящему ПЗ, должны обеспечивать:

возможность выполнения проверок с целью обнаружения зараженных КВ объектов;

возможность выполнения проверок с целью обнаружения зараженных КВ объектов в режиме реального времени в файлах, полученных по каналам передачи данных;

возможность выполнения проверок с целью обнаружения зараженных КВ объектов по команде; в режиме динамического обнаружения в процессе выполнения операций доступа к объектам; путем запуска с необходимыми параметрами функционирования своего кода внешней программой;

возможность выполнения проверок с целью обнаружения зараженных КВ объектов сигнатурными методами;

возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов;

возможность получения и установки обновлений БД ПКВ без применения средств автоматизации;

возможность генерирования записей аудита для событий, подвергаемых аудиту;

возможность чтения информации из записей аудита;

возможность уполномоченным пользователям (ролям) управлять режимом выполнения функций безопасности САВЗ;

возможность уполномоченным пользователям (ролям) управлять параметрами настройки функций безопасности САВЗ;

поддержку определенных ролей для САВЗ и их ассоциации с конкретными администраторами безопасности и администраторами серверов.

Средства антивирусной защиты типа «Б» устанавливаются на серверы информационной системы, функционирующей на базе вычислительной сети.

Типовая схема применения в ИС САВЗ типа «Б» представлена на рисунке 2.1.

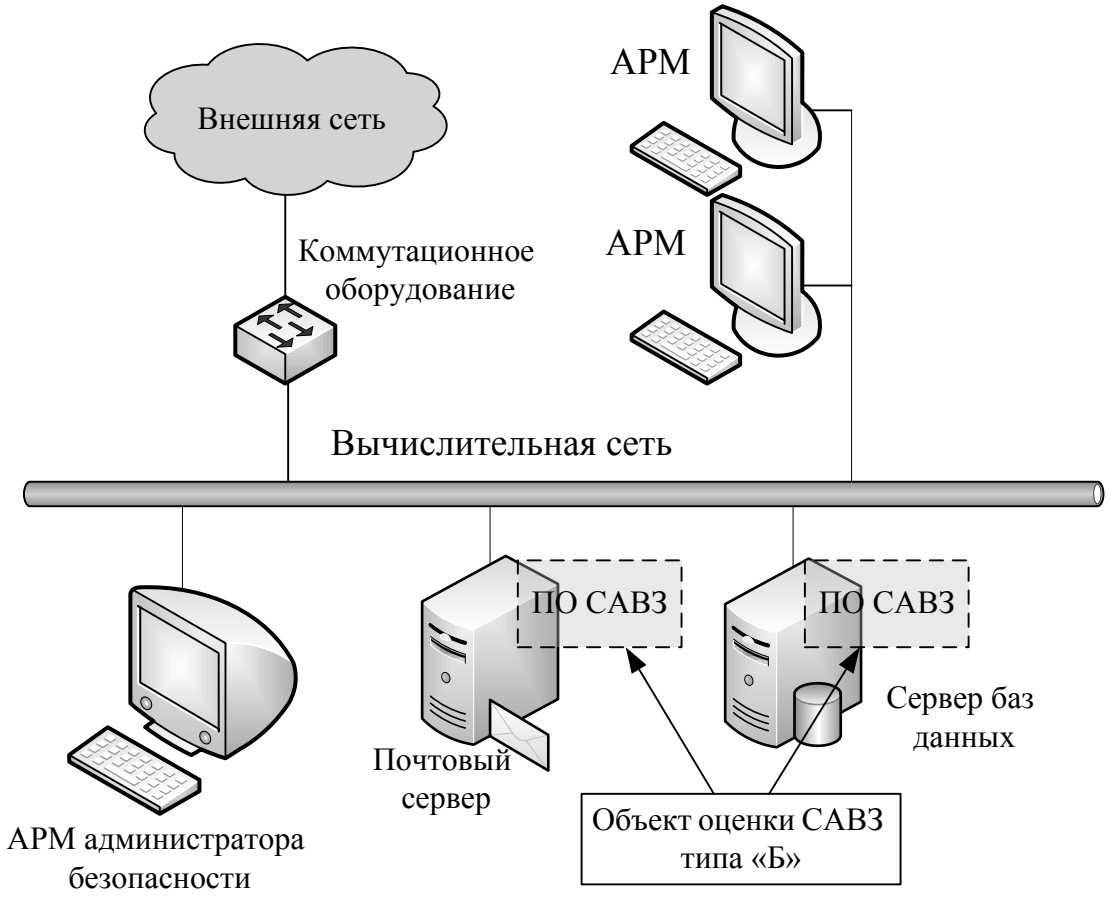

Рисунок 2.1 – Типовая схема ИС, в которой применяется САВЗ типа «Б»

3. Среда безопасности объекта оценки

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

предположений относительно предопределенного использования ОО и среды функционирования ОО;

угроз безопасности, которым необходимо противостоять средствами ОО;

политики безопасности организации, которой должен следовать ОО.

3.1. Предположения безопасности

Предположения относительно предопределенного использования ОО

Предположение-1

Должен быть обеспечен доступ ОО ко всем объектам ИС, которые необходимы ОО для реализации своих функциональных возможностей (к контролируемым объектам ИС).

Предположение-2

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с эксплуатационной документацией.

Предположение-3

Должна быть обеспечена совместимость ОО с контролируемыми ресурсами ИС.

Предположение-4

Должна быть обеспечена возможность корректной совместной работы САВЗ с САВЗ других производителей в случае их совместного использования в информационной системе.

Предположения, связанные с защитой ОО

Предположение-5

Должна быть обеспечена физическая защита элементов ИС, на которых установлен ОО.

Предположение-6

Должна быть обеспечена синхронизация по времени между компонентами ОО, а также между ОО и средой его функционирования.

Предположение, имеющее отношение к персоналу

Предположение-7

Персонал, ответственный за функционирование ОО, должен обеспечивать надлежащее функционирование ОО, руководствуясь эксплуатационной документацией.

3.2. Угрозы безопасности информации

3.2.1. Угрозы, которым должен противостоять объект оценки

В настоящем ПЗ определены следующие угрозы, которым необходимо противостоять средствами ОО.

Угроза-1

1. Аннотация угрозы – внедрение КВ в серверы ИС при осуществлении информационного взаимодействия с внешними информационно-телекоммуникационными сетями, в том числе сетями международного информационного обмена (сетями связи общего пользования).

2. Источник угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы - внедрение КВ в ИС при осуществлении информационного обмена.

4. Используемые уязвимости – неполнота комплекса средств защиты информации, применяемых в ИС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информационные ресурсы ИС, в которой установлен ОО.

6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность, целостность, доступность.

7. Возможные последствия реализации угрозы – заражение компьютерными вирусами программно-технических средств вычислительной сети ИС, утечка конфиденциальной информации, нарушение режимов функционирования ИС.

Угроза-2

1. Аннотация угрозы – внедрение КВ в серверы ИС со съемных машинных носителей информации.

2. Источник угрозы – внутренний нарушитель.

3. Способ реализации угрозы – внедрение КВ в объекты ИС пользователями со съемных машинных носителей информации.

4. Используемые уязвимости – неполнота комплекса средств защиты информации, применяемых в ИС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информационные ресурсы ИС, в которой установлен ОО.

6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность, целостность, доступность.

7. Возможные последствия реализации угрозы – заражение компьютерными вирусами программно-технических средств вычислительной сети ИС, утечка конфиденциальной информации, нарушение режимов функционирования ИС.

3.2.2. Угрозы, которым должна противостоять среда

В настоящем ПЗ определены следующие угрозы, которым должна противостоять среда функционирования ОО.

Угроза среды-1

1. Аннотация угрозы – отключение или блокирование САВЗ нарушителями.

2. Источники угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированный доступ к САВЗ с использованием штатных и нештатных средств.

4. Используемые уязвимости – недостатки процедур разграничения полномочий в ИС, уязвимости технических, программных и программно-технических средств ИС, которые взаимодействуют с САВЗ и могут влиять на функционирование САВЗ, недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования в ИС.

5. Вид информационных ресурсов, потенциально подверженных угрозе – данные функций безопасности объекта оценки (ФБО).

6. Нарушаемые свойства безопасности информационных ресурсов – целостность, доступность.

7. Возможные последствия реализации угрозы – неэффективность работы САВЗ.

Угроза среды-2

1. Аннотация угрозы – несанкционированное изменение конфигурации САВЗ.

2. Источник угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – несанкционированный доступ к конфигурационной информации (настройкам) САВЗ.

4. Используемая уязвимость – недостатки процедур разграничения полномочий в ИС, уязвимости технических, программных и программно-технических средств ИС, которые взаимодействуют с САВЗ и могут влиять на функционирование САВЗ, недостатки механизмов управления доступом, защиты сеансов, физической защиты оборудования в ИС.

5. Вид информационных ресурсов, потенциально подверженные угрозе – настройки программного обеспечения САВЗ.

6. Нарушаемые характеристики безопасности информационных ресурсов – целостность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования САВЗ, необнаружение внедрения в ИС КВ.

Угроза среды-3

1. Аннотация угрозы – несанкционированное внесения изменений в логику функционирования САВЗ через механизм обновления БД ПКВ.

2. Источник угрозы – внутренний нарушитель, внешний нарушитель.

3. Способ реализации угрозы – осуществление несанкционированных действий с использованием штатных средств, предоставляемых ИС, а также специализированных инструментальных средств.

4. Используемая уязвимость – недостатки механизмов обеспечения доверенного канала получения обновлений БД ПКВ.

5. Вид информационных ресурсов, потенциально подверженных угрозе – программное обеспечение и БД ПКВ САВЗ.

6. Нарушаемые свойства безопасности информационных ресурсов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования САВЗ, необнаружение внедрения в ИС КВ.

3.3. Политика безопасности организации

Объект оценки должен следовать приведенным ниже правилам политики безопасности организации.

Политика безопасности-1

Должны быть обеспечены надлежащие механизмы регистрации и предупреждения о любых событиях, относящихся к возможным нарушениям безопасности. Механизмы регистрации должны предоставлять уполномоченным на это субъектам ИС возможность выборочного ознакомления с информацией о произошедших событиях.

Политика безопасности-2

Управление параметрами САВЗ, которые влияют на выполнение функций безопасности САВЗ, должно осуществляться только уполномоченными субъектами ИС.

Политика безопасности-3

Должно осуществляться управление со стороны уполномоченных субъектов ИС режимами выполнения функций безопасности САВЗ.

Политика безопасности-4

Объект оценки должен быть защищен от несанкционированного доступа и нарушений в отношении функций и данных ОО.

Политика безопасности-5

Объект оценки должен обеспечивать выполнение проверок с целью обнаружения зараженных КВ объектов в заданных областях памяти и файлах.

Политика безопасности-6

Объект оценки должен обеспечивать возможность установки режимов выполнения проверок с целью обнаружения зараженных КВ объектов.

Политика безопасности-7

Объект оценки должен обеспечивать возможность установки режимов выполнения обновлений БД ПКВ САВЗ.

Политика безопасности-8

Объект оценки должен обеспечивать возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов.

4. Цели безопасности

4.1. Цели безопасности для объекта оценки

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Аудит безопасности САВЗ

Объект оценки должен располагать механизмами регистрации и предупреждения о любых событиях, относящихся к возможным нарушениям безопасности. Механизмы регистрации должны предоставлять уполномоченным субъектам ИС возможность выборочного ознакомления с информацией о произошедших событиях.

Цель безопасности-2

Управление параметрами САВЗ

Объект оценки должен обеспечить возможность управления параметрами САВЗ, которые влияют на выполнение функций безопасности САВЗ, со стороны уполномоченных субъектов ИС.

Цель безопасности-3

Управление работой САВЗ

Объект оценки должен обеспечивать управление со стороны уполномоченных субъектов ИС режимами выполнения функций безопасности САВЗ.

Цель безопасности-4

Разграничение доступа к управлению САВЗ

Объект оценки должен обеспечивать разграничение доступа к управлению САВЗ на основе ролей субъектов ИС.

Цель безопасности-5

Выполнение проверок объектов

Объект оценки должен обеспечивать выполнение проверок с целью обнаружения зараженных КВ объектов.

Цель безопасности-6

Режимы выполнения проверок

Объект оценки должен обеспечивать возможность установки режимов выполнения проверок с целью обнаружения зараженных КВ объектов.

Цель безопасности-7

Обновление базы данных

Объект оценки должен обеспечивать возможность установки режимов выполнения обновлений БД ПКВ САВЗ.

Цель безопасности-8

Обработка зараженных объектов

Объект оценки должен обеспечивать возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов.

4.2. Цели безопасности для среды

В данном разделе дается описание целей безопасности для среды функционирования ОО.

Цель для среды функционирования ОО-1

Доступ к данным ИС

Должен быть обеспечен доступ объекта оценки к данным ИС, которые необходимы объекту оценки для реализации своих функциональных возможностей.

Цель для среды функционирования ОО-2

Эксплуатация ОО

Должны быть обеспечены установка, конфигурирование и управление объектом оценки в соответствии с эксплуатационной документацией.

Цель для среды функционирования ОО-3

Совместимость

Должна быть обеспечена совместимость объекта оценки с контролируемыми ресурсами ИС.

Цель для среды функционирования ОО-4

Совместная работа

Должна быть обеспечена возможность корректной совместной работы САВЗ с САВЗ других производителей в случае их совместного использования в информационной системе.

Цель для среды функционирования ОО-5

Физическая защита частей ОО

Должна быть обеспечена физическая защита программно-технических средств, на которых установлен ОО.

Цель для среды функционирования ОО-6

Синхронизация по времени

Должна быть обеспечены быть обеспечены надлежащий источник меток времени и синхронизация по времени между компонентами ОО, а также между ОО и средой его функционирования.

Цель для среды функционирования ОО-7

Требования к персоналу

Персонал, ответственный за функционирование объекта оценки, должен обеспечивать надлежащее функционирование объекта оценки, руководствуясь эксплуатационной документацией.

Цель для среды функционирования ОО-8

Доверенная связь

Должна быть обеспечена доверенная связь между ОО и уполномоченными субъектами ИС (администраторами безопасности).

Цель для среды функционирования ОО-9

Механизмы аутентификации и идентификации

Функционирование ОО должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности САВЗ.

Цель для среды функционирования ОО-10

Доверенный канал

Должен быть обеспечен доверенный канал получения обновлений БД ПКВ САВЗ.

Цель для среды функционирования ОО-11

Защита данных ФБО

Должна быть обеспечена защищенная область для выполнения функций безопасности САВЗ.

Цель для среды функционирования ОО-12

Управление атрибутами безопасности

Управление атрибутами безопасности, связанными с доступом к функциям и данным ОО, должно предоставляться только уполномоченным ролям (администраторам САВЗ и ИС).

5. Требования безопасности

В данном разделе ПЗ представлены функциональные требования и требования доверия, которым должен удовлетворять ОО. Функциональные требования, представленные в настоящем ПЗ, основаны на функциональных компонентах из ГОСТ Р ИСО/МЭК 15408–2. Кроме того, в настоящий ПЗ включен ряд требований безопасности, сформулированных в явном виде (расширение ГОСТ Р ИСО/МЭК 15408–2). Требования доверия основаны на компонентах требований доверия из ГОСТ Р ИСО/МЭК 15408–3 и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД1, усиленного компонентом AVA_SOF.1 «Оценка стойкости функции безопасности ОО» и расширенного компонентами ALC_UPV_EXT.1 «Процедуры обновления БД ПКВ» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность САВЗ». Требования безопасности ALC_UPV_EXT.1 «Процедуры обновления БД ПКВ» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность САВЗ» сформулированы в явном виде (расширение ГОСТ Р ИСО/МЭК 15408–3).

5.1. Требования безопасности для объекта оценки

5.1.1. Функциональные требования безопасности ОО

Функциональные компоненты из ГОСТ Р ИСО/МЭК 15408–2, на которых основаны функциональные требования безопасности ОО, приведены в таблице 5.1.

Таблица 5.1

Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_SAR.1	Просмотр аудита
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MTD.1	Управление данными ФБО
FMT_SMR.1	Роли безопасности
FAV_DET_EXT.1	Базовое обнаружение КВ
FAV_DET_EXT.3	Проверка файлов, полученных по каналам передачи данных
FAV_MTH_EXT.1	Методы анализа
FAV_MTH_EXT.2	Выполнение проверок
FAV_MTH_EXT.3	Запуск выполнения проверок внешней программой
FAV_ACT_EXT.1	Удаление КВ
FAV_UPD_EXT.1	Обновление БД ПКВ

5.1.1.1. Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на [выбор (выбрать одно из): *минимальный, базовый, детализированный, неопределенный*] уровне аудита;

в) [события, приведенные во втором столбце таблицы 5.2].

Таблица 5.2

События, подлежащие аудиту

Компонент	Событие	Детализация
FAV_MTH_EXT.2	Выполнение проверок	Режим запуска проверок, параметры функционирования ОО при выполнении проверок, результат проверок
FAV_UPD_EXT.1	Обновление базы данных КВ	Идентификаторы обновлений

FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:

а) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);

б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ, [информацию, определенную в третьем столбце таблицы 5.2].

Зависимости: FPT_STM.1 «Надежные метки времени».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [назначение: *уполномоченные пользователи*] возможность читать [назначение: *список информации аудита*] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

Зависимости: FAU_GEN.1 «Генерация данных аудита».

5.1.1.2. Управление безопасностью (FMT)

FMT_MTD.1 Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность [задания], **а также** [выбор: *изменение значений по умолчанию, модификация, [*назначение: *другие операции]*] [параметров поиска КВ] и следующих данных [назначение: *список других данных ФБО*] только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность ***управления*** *режимами выполнения* ***функций безопасности, указанных в***

первом столбце таблицы 5.3, а также *[назначение: другие режимы]* определенных функций, [указанных во втором столбце таблицы 5.1, **а также** [назначение: *список функций*]] только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.3

Режимы выполнения функций безопасности

Режим выполнения функций безопасности	ФБО
Определение режима выполнения, модификация режима выполнения	Обработка зараженных объектов
Определение режима выполнения, модификация режима выполнения	Выполнение файловых операций (создание, удаление, модификация), проводимых при проверке САВЗ заархивированных объектов

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

[а) администратор безопасности;

б) администратор сервера;

в) [назначение: *другие роли*]].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать пользователей с ролями.

Зависимости: FIA_UID.1 «Выбор момента идентификации».

5.1.1.3. Проверки объектов заражения (FAV_DET_EXT)

FAV_DET_EXT.1 Базовое обнаружение вредоносных компьютерных программ (вирусов)

FAV_DET_EXT.1.1 ФБО должны выполнять проверки с целью обнаружения вредоносных компьютерных программ (вирусов) [выбор: *в файловых областях носителей информации, в исполняемых файлах, в заархивированных файлах, [назначение: другие объекты]*].

Зависимости отсутствуют.

FAV_DET_EXT.3 Проверка файлов, полученных по каналам передачи данных

FAV_DET_EXT.3.1 ФБО должны выполнять проверки с целью обнаружения вредоносных компьютерных программ (вирусов) в файлах, полученных по каналам передачи данных [выбор: *в режиме реального времени, [назначение: другие режимы]*].

Зависимости отсутствуют.

5.1.1.4. Методы проверок объектов заражения (FAV_MTH_EXT)

FAV_MTH_EXT.1 Методы анализа

FAV_MTH_EXT.1.1 ФБО должны выполнять проверки с целью обнаружения КВ в объектах с использованием *сигнатурных методов,* [назначение: *другие методы*].

Зависимости отсутствуют.

FAV_MTH_EXT.2 Выполнение проверок

FAV_MTH_EXT.2.1 ФБО должны выполнять проверки с целью обнаружения зараженных КВ объектов *по команде [назначение: уполномоченные роли]; в режиме динамического обнаружения в процессе выполнения операций доступа к объектам* [назначение: *другие режимы выполнения проверок*].

Зависимости отсутствуют.

FAV_MTH_EXT.3 Запуск выполнения проверок внешней программой

FAV_MTH_EXT.3.1 ФБО должны выполнять проверки с целью обнаружения зараженных КВ объектов путем запуска своего кода средой функционирования.

FAV_MTH_EXT.3.2 ФБО должны поддерживать параметры запуска [назначение: *параметры запуска*], установленные [назначение: *уполномоченные роли*].

Зависимости отсутствуют.

5.1.1.5. Обработка объектов, подвергшихся воздействию (FAV_ACT_EXT)

FAV_ACT_EXT.1 Удаление КВ

FAV_ACT_EXT.1.1 При обнаружении КВ функции безопасности средства антивирусной защиты должны выполнять удаление КВ [выбор: *из файлов, системных областей носителей информации, сообщений электронной почты, [назначение: другие объекты]*].

Зависимости отсутствуют.

5.1.1.6. Обновление базы данных ПКВ (FAV_UPD_EXT)

FAV_UPD_EXT.1 Обновление базы данных ПКВ

FAV_UPD_EXT.1.1 ФБО должны обеспечивать получение и установку обновлений БД ПКВ *локально без применения средств автоматизации* [назначение: *другие режимы выполнения обновлений*].

Зависимости отсутствуют.

5.1.2. Требования доверия к безопасности объекта оценки

Требования доверия к безопасности ОО взяты из ГОСТ Р ИСО/МЭК 15408–3 и образуют ОУД1, усиленный компонентом AVA_SOF.1 «Оценка

стойкости функции безопасности ОО» и расширенный компонентами ALC_UPV_EXT.1 «Процедуры обновления БД ПКВ» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность САВЗ» (см. таблицу 5.4).

Таблица 5.4

Требования доверия к безопасности ОО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Управление конфигурацией	ACM_CAP.1	Номера версий
Поставка и эксплуатация	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1	Неформальная функциональная спецификация
	ADV_RCR.1	Неформальная демонстрация соответствия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Тестирование	ATE_IND.1	Независимое тестирование на соответствие
Оценка уязвимостей	AVA_SOF.1	Оценка стойкости функции безопасности ОО
Обновление базы решающих правил	ALC_UPV_EXT.1	Процедуры обновления БД ПКВ
	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность САВЗ

5.1.2.1. Управление конфигурацией (ACM)

ACM_CAP.1 Номера версий

Зависимости отсутствуют.

Элементы действий разработчика

ACM_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

ACM_CAP.1.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

ACM_CAP.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.2. Поставка и эксплуатация (ADO)

ADO_IGS.1 Процедуры установки, генерации и запуска

Зависимости

AGD_ADM.1 Руководство администратора.

Элементы действий разработчика

ADO_IGS.1.1D Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

Элементы содержания и представления свидетельств

ADO_IGS.1.1C Документация должна содержать описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.

Элементы действий оценщика

ADO_IGS.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.1.2E Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

5.1.2.3. Разработка (ADV)

ADV_FSP.1 Неформальная функциональная спецификация

Зависимости

ADV_RCR.1 Неформальная демонстрация соответствия.

Элементы действий разработчика

ADV_FSP.1.1D Разработчик (заявитель) должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.1.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.1.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

ADV_FSP.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.1.2E Оценщик должен сделать независимое заключение, что функциональная спецификация – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 Неформальная демонстрация соответствия

Зависимости отсутствуют.

Элементы действий разработчика

ADV_RCR.1.1D Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные

возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

ADV_RCR.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.4. Руководства (AGD)

AGD_ADM.1 Руководство администратора

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация.

Элементы действий разработчика

AGD_ADM.1.1D Разработчик должен представить руководство администратора, предназначенное для персонала системного администрирования.

Элементы содержания и представления свидетельств

AGD_ADM.1.1C Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.

AGD_ADM.1.2C Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.

AGD_ADM.1.3C Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_ADM.1.4C Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.

AGD_ADM.1.5C Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.

AGD_ADM.1.6C Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.

AGD_ADM.1.7C Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_ADM.1.8C Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.

Элементы действий оценщика

AGD_ADM.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AGD_USR.1 Руководство пользователя

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация.

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

AGD_USR.1.1C Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.

AGD_USR.1.2C Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.

AGD_USR.1.3C Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_USR.1.4C Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.

AGD_USR.1.5C Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_USR.1.6C Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.

Элементы действий оценщика

AGD_USR.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.5. Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ATE_FUN.1 Функциональное тестирование.

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ATE_IND.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.1.2E Оценщик должен протестировать необходимое подмножество ФБО, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

5.1.2.6. Оценка уязвимостей (AVA)

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация,

ADV_HLD.1 Описательный проект верхнего уровня.

Элементы действий разработчика

AVA_SOF.1.1D Разработчик должен выполнить анализ стойкости функции безопасности ОО для каждого механизма, идентифицированного в ПЗ как имеющего утверждение относительно стойкости функции безопасности ОО.

Элементы содержания и представления свидетельств

AVA_SOF.1.1C Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ.

AVA_SOF.1.2C Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в ПЗ.

Элементы действий оценщика

AVA_SOF.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_SOF.1.2E Оценщик должен подтвердить, что утверждения относительно стойкости корректны.

5.1.2.7. Требования к ОО, сформулированные в явном виде

ALC_UPV_EXT.1 Процедуры обновления БД ПКВ

Зависимости отсутствуют.

Элементы действий разработчика

ALC_UPV_EXT.1.1D Разработчик должен разработать и реализовать процедуру фиксации момента получения новой КВ, основанную на [назначение: *способы фиксации*].

ALC_UPV_EXT.1.2D Разработчик должен разработать и реализовать технологию, обеспечивающую время выпуска обновлений БД ПКВ не более [назначение: *заданное значение времени*].

ALC_UPV_EXT.1.3D Разработчик должен разработать и реализовать процедуру уведомления об обновлении БД ПКВ, основанную на [назначение: *способы уведомления*].

ALC_UPV_EXT.1.4D Разработчик должен разработать и реализовать процедуру доставки обновлений БД ПКВ, основанную на [назначение: *способы доставки обновлений*].

ALC_UPV_EXT.1.5D Разработчик должен разработать процедуру контроля целостности обновлений БД ПКВ со стороны [назначение: *идентифицированные уполномоченные роли*], основанную на [назначение: *способы контроля целостности*].

ALC_UPV_EXT.1.6D Разработчик должен разработать и реализовать процедуру представления обновлений для проведения внешнего контроля, основанную на [назначение: *способы предоставления обновлений для контроля*].

Элементы содержания и представления свидетельств

ALC_UPV_EXT.1.1C Документация процедуры фиксации момента новой КВ должна содержать описание способов фиксации.

ALC_UPV_EXT.1.2C Документированные материалы должны содержать аргументацию, что время выпуска обновлений БД ПКВ не превышает заданного.

ALC_UPV_EXT.1.3C Документация процедуры уведомления об обновлении БД ПКВ должна содержать описание способов уведомления.

ALC_UPV_EXT.1.4C Документация процедуры доставки обновлений БД ПКВ должна содержать описание способов доставки обновлений.

ALC_UPV_EXT.1.5C Документация процедуры контроля целостности обновлений БД ПКВ должна содержать описание способов контроля целостности обновлений.

ALC_UPV_EXT.1.6C Документация процедуры представления обновлений для проведения внешнего контроля должна содержать описание способов предоставления разработчиком обновлений для контроля.

Элементы действий оценщика

ALC_UPV_EXT.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению документированных материалов.

ALC_UPV_EXT.1.2E Оценщик должен проверить, что способы предоставления обновлений для контроля позволяют организовать и проводить их внешний контроль.

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность САВЗ

Элементы действий разработчика

AMA_SIA_EXT.3.1D Разработчик должен представить материалы анализа влияния обновлений на безопасность САВЗ.

Элементы содержания и представления свидетельств

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность САВЗ должны содержать краткое описание влияния обновлений на задание по безопасности, функции безопасности САВЗ или содержать логическое обоснование отсутствия такого влияния.

AMA_SIA_EXT.3.2C Материалы анализа влияния обновлений на безопасность САВЗ должны для обновлений, влияющих на безопасность, идентифицировать функции безопасности, компоненты САВЗ, на которые влияет данное обновление.

Элементы действий оценщика

AMA_SIA_EXT.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению документированных материалов.

5.2. Требования безопасности для среды информационных технологий

Функциями безопасности, реализуемыми средой ИТ в интересах обеспечения безопасности ОО, являются функции «Идентификация и аутентификация» и «Защита ФБО».

Функциональные компоненты из ГОСТ Р ИСО/МЭК 15408–2, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.5.

Таблица 5.5

Функциональные компоненты, на которых основаны ФТБ среды ИТ

Идентификатор компонента требований	Название компонента требований
FIA_AFL.1	Обработка отказов аутентификации
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UID.2	Идентификация до любых действий пользователя
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО

5.2.1 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 **Функции безопасности среды ИТ** должны обнаруживать, когда произойдет [назначение: *число попыток*] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

FIA_AFL.1.2 При **достижении** определенного **в элементе FIA_AFL.1.1** числа неуспешных попыток аутентификации **функции безопасности среды ИТ** должны: [назначение: *список действий, **направленных на дальнейшее предотвращение попыток доступа со стороны субъекта, ограниченное временным интервалом***].

Зависимости: FIA_UAU.2 «Аутентификация до любых действий пользователя».

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 **Функции безопасности среды ИТ** должны предоставить механизм для верификации того, что **пароли на доступ к ОО** отвечают [назначение: *определенная метрика качества* ***паролей, включающая требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов***].

Зависимости отсутствуют.

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 **Функции безопасности среды ИТ** должны требовать, чтобы каждый **субъект доступа к ОО** был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа.**

Зависимости: FIA_UID.1 «Выбор момента идентификации».

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 **Функции безопасности среды ИТ** должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве среды ИТ от имени этого пользователя.

Зависимости отсутствуют.

5.2.2 Защита ФБО (FPT)

FPT_RVM.1 Невозможность обхода ПБО

FPT_RVM.1.1 **Функции безопасности среды ИТ** должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах области действия функции безопасности объекта оценки (ОДФ).

Зависимости отсутствуют.

FPT_SEP.1 Отделение домена ФБО

FPT_SEP.1.1 **Функции безопасности среды ИТ** должны поддерживать домен безопасности для выполнения **ФБО**, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 **Функции безопасности среды ИТ** должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости отсутствуют.

Замечания по применению: Представленные в данном подразделе требования могут быть реализованы средой ИТ, непосредственно ОО или совместно – средой ИТ и ОО.

6. Обоснование

В данном разделе дано обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ПЗ.

6.1. Обоснование целей безопасности

6.1.1. Обоснование целей безопасности для ОО

В таблице 6.1 приведено отображение целей безопасности для ОО на угрозы и политику безопасности организации.

Таблица 6.1

Отображение целей безопасности на угрозы и политику безопасности организации

	Цель безопасности-1	**Цель безопасности-2**	**Цель безопасности-3**	**Цель безопасности-4**	**Цель безопасности-5**	**Цель безопасности-6**	**Цель безопасности-7**	**Цель безопасности-8**
Угроза-1	**X**	**X**	**X**					
Угроза-2	**X**	**X**	**X**	**X**				
Политика безопасности-1	**X**							
Политика безопасности-2		**X**						
Политика безопасности-3			**X**					
Политика безопасности-4				**X**				
Политика безопасности-5					**X**			
Политика безопасности-6						**X**		
Политика безопасности-7							**X**	
Политика безопасности-8								**X**

Цель безопасности-1

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности организации **Политика безопасности-1**, так как обеспечивает надлежащую регистрацию и предупреждение о любых событиях, относящихся к возможным нарушениям безопасности, возможность выборочного ознакомления с информацией о произошедших событиях.

Цель безопасности-2

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности организации **Политика безопасности-2**, так как обеспечивает возможность управления параметрами САВЗ, которые влияют на выполнение функций безопасности САВЗ, со стороны уполномоченных субъектов ИС.

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1, Угроза-2** и реализацией политики безопасности организации **Политика безопасности-3**, так как обеспечивает управление со стороны уполномоченных субъектов ИС режимами выполнения функций безопасности САВЗ.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-2** и реализацией политики безопасности организации **Политика безопасности-4**, так как обеспечивает разграничение доступа к управлению САВЗ на основе ролей уполномоченных субъектов ИС.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-5**, так как обеспечивает выполнение проверок с целью обнаружения зараженных КВ объектов в заданных областях памяти и файлах.

Цель безопасности-6

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-6**, так как обеспечивает возможность установки режимов выполнения проверок с целью обнаружения зараженных КВ объектов.

Цель безопасности-7

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-7,** так как обеспечивает возможность установки режимов выполнения обновлений БД ПКВ САВЗ.

Цель безопасности-8

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-8,** так как обеспечивает возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов.

6.1.2. Обоснование целей безопасности для среды

В таблице 6.2 приведено отображение целей безопасности для среды на предположения безопасности, политику безопасности и угрозы.

Цель для среды функционирования ОО-1

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-1,** так как обеспечивается доступ ОО ко всем данным ИС, которые необходимы ОО для реализации своих функциональных возможностей.

Таблица 6.2

Отображение целей безопасности для среды на предположения безопасности, политики безопасности и угрозы

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-6	Цель для среды функционирования ОО-7	Цель для среды функционирования ОО-8	Цель для среды функционирования ОО-9	Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11	Цель для среды функционирования ОО-12
Предположение-1	X											
Предположение-2		X										
Предположение-3			X									
Предположение-4				X								
Предположение-5					X							
Предположение-6						X						X
Предположение-7							X					
Угроза среды-1					X				X		X	X
Угроза среды-2								X	X		X	X
Угроза среды-3										X		

Цель для среды функционирования ОО-2

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-2,** так как обеспечивается установка, конфигурирование и управление ОО в соответствии с эксплуатационной документацией.

Цель для среды функционирования ОО-3

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-3**, так как обеспечивает совместимость объекта оценки с контролируемыми информационными ресурсами ИС.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-4,** так как обеспечивается возможность корректной совместной работы средств антивирусной защиты со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-1** и

реализацией предположения безопасности **Предположение-5,** так как обеспечивается физическая защита элементов ИС, на которых установлен ОО.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Предположение-6,** так как обеспечивается синхронизация по времени между компонентами ОО, а также между ОО и средой его функционирования.

Цель для среды функционирования ОО-7

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-7,** так как персонал, ответственный за функционирование ОО, обеспечивает надлежащее функционирование ОО, руководствуясь эксплуатационной документацией.

Цель для среды функционирования ОО-8

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-2**, так как обеспечивает доверенную связь между ОО и уполномоченными субъектами ИС (администраторами безопасности).

Цель для среды функционирования ОО-9

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды **Угроза для среды-1** и **Угроза для среды-2**, так как обеспечивает функционирование ОО в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности САВЗ.

Цель для среды функционирования ОО-10

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе безопасности для среды **Угроза для среды-3,** так как обеспечивается доверенный канал получения обновлений БД ПКВ САВЗ.

Цель для среды функционирования ОО-11

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды **Угроза для среды-1** и **Угроза для среды-2**, так как обеспечивается защищенная область для выполнения функций безопасности САВЗ.

Цель для среды функционирования ОО-12

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам безопасности для среды **Угроза для среды-1** и **Угроза для среды-2,** так как обеспечивается предоставления возможности управления атрибутами безопасности, связанными с доступом к функциям и данным ОО, только уполномоченным ролям (администраторам САВЗ и ИС).

6.2. Обоснование требований безопасности

6.2.1. Обоснование требований безопасности для ОО

6.2.1.1. Обоснование функциональных требований безопасности ОО

В таблице 6.3 представлено отображение функциональных требований безопасности ОО на цели безопасности для ОО.

Таблица 6.3

Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8
FAU_GEN.1	X							
FAU_SAR.1	X							
FMT_MOF.1		X	X					
FMT_MTD.1		X	X					
FMT_SMR.1				X				
FAV_DET_EXT.1					X			
FAV_DET_EXT.3					X			
FAV_MTH_EXT.1						X		
FAV_MTH_EXT.2						X		
FAV_MTH_EXT.3						X		
FAV_ACT_EXT.1								X
FAV_UPD_EXT.1							X	

FAU_GEN.1 Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО. Рассматриваемый компонент сопоставлен с **Целью безопасности-1** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления администратору безопасности всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с **Целью безопасности-1** и способствует ее достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента обеспечивает задание параметров функционирования САВЗ. Рассматриваемый компонент сопоставлен с целями **Целью безопасности-2, Целью безопасности-3** и способствует их достижению.

FMT_SMR.1 Роли безопасности

Выполнение требований данного компонента обеспечивает выполнение поддержки ролей безопасности и осуществления ассоциаций пользователей с ролями. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAV_DET_EXT.1 Базовое обнаружение КВ

Выполнение требований данного компонента обеспечивает выполнение проверок с целью обнаружения зараженных КВ объектов. Рассматриваемый компонент сопоставлен с **Целью безопасности-5** и способствует ее достижению.

FAV_DET_EXT.3 Проверка файлов, полученных по каналам передачи данных

Выполнение требований данного компонента обеспечивает выполнение проверок с целью обнаружения зараженных КВ объектов в файлах, полученных по каналам передачи данных. Рассматриваемый компонент сопоставлен с **Целью безопасности-5** и способствует ее достижению.

FAV_MTH_EXT.1 Методы анализа

Выполнение требований данного компонента обеспечивает выполнение анализа с целью обнаружения зараженных КВ объектов различными методами. Рассматриваемый компонент сопоставлен с **Целью безопасности-6** и способствует ее достижению.

FAV_MTH_EXT.2 Выполнение проверок

Выполнение требований данного компонента обеспечивает выполнение проверок с целью обнаружения зараженных КВ объектов различными методами. Рассматриваемый компонент сопоставлен с **Целью безопасности-6** и способствует ее достижению.

FAV_MTH_EXT.3 Запуск выполнения проверок внешней программой

Выполнение требований данного компонента обеспечивает запуск выполнения проверок на предмет наличия зараженных КВ объектов внешней программой. Рассматриваемый компонент сопоставлен с **Целью безопасности-6** и способствует ее достижению.

FAV_ACT_EXT.1 Удаление КВ

Выполнение требований данного компонента обеспечивает возможность удаления (если удаление технически возможно) кода КВ из зараженных объектов. Рассматриваемый компонент сопоставлен с **Целью безопасности-8** и способствует ее достижению.

FAV_UPD_EXT.1 Обновление базы данных ПКВ

Выполнение требований данного компонента обеспечивает получение и установку обновлений БД ПКВ САВЗ. Рассматриваемый компонент сопоставлен с **Целью безопасности-7** и способствует ее достижению.

6.2.1.2. Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ПЗ соответствуют ОУД1, усиленному компонентом AVA_SOF.1 «Оценка стойкости функции безопасности ОО» и расширенному компонентами ALC_UPV_EXT.1 «Процедуры обновления БД ПКВ» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность САВЗ».

Включение указанных требований доверия к безопасности ОО в ПЗ определяется нормативным правовым актом ФСТЭК России «Требования в области технического регулирования продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам антивирусной защиты)».

6.2.2. Обоснование требований безопасности для среды информационных технологий

В таблице 6.4 представлено отображение функциональных требований безопасности среды ИТ на цели безопасности для среды.

Таблица 6.4

Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	Цель для среды функционирования ОО-9	Цель для среды функционирования ОО-11
FIA_AFL.1	**X**	
FIA_SOS.1	**X**	
FIA_UAU.2	**X**	
FIA_UID.2	**X**	
FPT_RVM.1		**X**
FPT_SEP.1		**X**

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает выполнение определенных действий, направленных на дальнейшее предотвращение попыток доступа со стороны субъекта, ограниченное временным интервалом, при достижении определенного числа неуспешных попыток аутентификации при доступе к ОО. Рассматриваемый компонент сопоставлен с целью

безопасности для среды **Цель для среды функционирования ОО-9** и способствует ее достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает верификацию качества паролей на доступ к ОО. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-9** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа к ОО до того, как функции безопасности среды ИТ разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-9** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение идентификации уполномоченного пользователя до того, как ФБО разрешат выполнять любые другие действия при посредничестве ФБО от имени этого пользователя. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-9** и способствует ее достижению.

FPT_RVM.1 Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-11** и способствует ее достижению.

FPT_SEP.1 Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью безопасности для среды **Цель для среды функционирования ОО-11** и способствует ее достижению.

6.2.3. Обоснование удовлетворения зависимостей требований

В таблице 6.5 представлены результаты удовлетворения зависимостей функциональных требований. Все зависимости компонентов требований удовлетворены в настоящем ПЗ либо включением компонентов, определенных в ГОСТ Р ИСО/МЭК 15408–2 под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в ГОСТ Р ИСО/МЭК 15408–2 под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 6.5 является справочным и содержит компоненты, определенные в ГОСТ Р ИСО/МЭК 15408–2 в описании компонентов требований, приведенных в столбце 1 таблицы 6.5, под рубрикой «Зависимости».

Столбец 3 таблицы 6.5 показывает, какие компоненты требований были реально включены в настоящий ПЗ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 6.5. Компоненты требований в столбце 3 таблицы 6.5 либо совпадают с компонентами в столбце 2 таблицы 6.5, либо иерархичны по отношению к ним.

Таблица 6.5

Зависимости функциональных требований

Функциональные компоненты	**Зависимости по ГОСТ Р ИСО/МЭК 15408**	**Удовлетворение зависимостей**
FAU_GEN.1	FPT_STM.1	Цель для среды функционирования-6
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1

Все зависимости включенных в ПЗ компонентов ФТБ удовлетворены.