Приложение № 1
к приказу Минэнерго России
от 06.11.2018 № 1015

Таблица № 1. Минимальный комплекс мероприятий для обеспечения безопасности среды функционирования СУМиД организационных требований к обеспечению информационной безопасности аппаратной инфраструктуры СУМиД

Идентификатор	Наименование цели	Описание
OE.SECURE	Контроль физического доступа	В местах размещения аппаратной инфраструктуры СУМиД должен быть обеспечен контроль физического доступа.
OE.I№STALL	Безопасная установка	Процесс установки, инсталляции и администрирования аппаратной инфраструктуры, программного обеспечения СУМиД должен соответствовать требованиям политики информационной безопасности, утвержденной собственником или иным законным владельцем объекта электроэнергетики. Контроль соответствия требований информационной безопасности осуществляется службой информационной безопасности объекта электроэнергетики.
OE.TRAI№	Повышение осведомленности	Администраторы СУМиД должны пройти обучение и получить сертификат об окончании обучения способам администрирования компонентов программного обеспечения. В составе программы обучения должны входить мероприятия по получению знаний и навыков реализации требований информационной безопасности, действующих в Российской Федерации.
OE.LIMEXT	Администратор безопасности	В рамках организационной структуры подразделения, эксплуатирующего программное обеспечение, должна быть предусмотрена роль администратора информационной безопасности. Роль администратора информационной безопасности должна быть регламентирована и утверждена службой информационной безопасности объекта. В качестве исполнителя роли администратора информационной безопасности может быть только сотрудник объекта в соответствии со штатным расписанием.

Таблица № 2. Описание целей информационной безопасности объекта электроэнергетики, организационных требований к обеспечению контроля информационной безопасности СУМиД

Идентификатор	Название	Описание
O.AUDITI№G	Аудит событий	Программное обеспечение должно обеспечивать: генерацию, запись и хранение событий информационной безопасности относящихся к функционированию встроенных средств защиты; защиту данных журналов (доступ к журналам разрешен пользователям, имеющим право допуска, правило получения, которого устанавливаются службой информационной безопасности объекта электроэнергетики). Хранимая в журналах информация, должна содержать: дату и время произошедшего события информационной безопасности, идентификационные данные пользователя, от имени которого совершалось действие или был запущен процесс, повлекший наступление события информационной безопасности; подробное описание предпринимаемых действий для последующего их анализа с целью выявления попыток несанкционированного доступа или несанкционированной модификации компонент программного обеспечения.
O.CRYPTO	Криптографическая защита	Программное обеспечение должно обеспечивать целостность и конфиденциальность информации. Целостность и конфиденциальность информации обеспечивается средствами криптографической защиты. Удаленное соединение должно обеспечиваться совместно со средствами криптографической защиты, в рамках открытых сессий обмена данными должны использоваться средства криптографической защиты. В случае с распределенной сетью хранения и получения данных должны использоваться средства криптографической защиты.
O.DACCESS	Дискретный доступ	Программное обеспечение должно осуществлять контроль доступа субъектов на основе идентификаторов объектов. Доступ к объектам пользователей должен осуществляться на основании правил доступа персонала к объектам, утвержденных службой безопасности объекта электроэнергетики.
O.№FLOW	Контроль сетевого взаимодействия	Программное обеспечение должно осуществлять контроль взаимодействия и передачи информации между сетевыми интерфейсами (в том числе виртуальными), между субъектами, между внутренними функциями на основании настраиваемой

		политики безопасности.
O.SUBJECT	Передача атрибутов безопасности	При взаимодействии пользователей программное обеспечение должно обеспечивать передачу атрибутов безопасности в соответствии с настраиваемой политикой безопасности.
O.I&A	Идентификация и аутентификация	Программное обеспечение должно обеспечивать идентификацию и аутентификацию пользователей для любых действий на основе сертификата открытого ключа подписи и связанного с ним закрытого ключа подписи, размещенного на отчуждаемом носителе. Доступ к объектам программного обеспечения должен предоставляться только авторизованным пользователям. Должна быть обеспечена строгая многофакторная аутентификация.
O.MA№AGE	Конфигурация безопасности	Программное обеспечение должно содержать необходимые механизмы для управления и настройки всех имеющихся функций безопасности. Доступ к этим механизмам должен быть обеспечен только авторизованным пользователям с выделенной ролью администратора информационной безопасности. Программное обеспечение должно иметь возможность указывать на ошибки персонала при конфигурации, а также должно запрещать возможность снижения уровня безопасности. Применяемые средства защиты информации должны соответствовать требованиям установленным пунктами 19 - 22 приказа ФСТЭК России от 21.12.2017 № 235 "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования".
O.TRUSTCHA№	Установление доверенных соединений	Программное обеспечение должно быть спроектировано и разработано таким образом, чтобы позволять установление доверенного соединения с информационными системами того же класса доверия, гарантируя при этом целостность, доступность и конфиденциальность передаваемых в рамках соединения данных, взаимную авторизацию и возможность обмена атрибутами безопасности.
O.AVAIL	Доступность	Функционирование программного обеспечения должно осуществляться на постоянной основе. В случае выходов из строя каналов связи функционирование программного обеспечение

		должно продолжаться. Должны быть предусмотрены механизмы обеспечения продолжения функционирования при переполнении баз данных. Должен осуществляться контроль целостности компонентов в процессе их загрузки. Должно быть исключено неконтролируемое, несанкционированное вмешательство в процессы перезагрузки или восстановления после сбоев компонентов программного обеспечения. В процессе функционирования программного обеспечения должны быть предусмотрены на периодической основе проверки на наличие уязвимостей компонентов программного обеспечения. Должны быть предусмотрены возможности восстановления данных и/или параметров конфигураций компонентов программного обеспечения из резервных копий в случае их компрометации или уничтожения. Должны быть предусмотрены возможности создания резервных копий в случае внесения изменений в конфигурации, с заданной периодичностью или комбинации этих вариантов.

Приложение № 2
к приказу Минэнерго России
от 06.11.2018 № 1015

Таблица № 1. Перечень базовых атак, необходимых при анализе уязвимостей системы удаленного мониторинга и диагностики энергетического оборудования

№ ПП	Объект атаки	Тип атаки	Результат атаки
1	атаки вследствие использования стека протокола IPSec	атаки типа: "человек в середине", "отказ в обслуживании"	возможность: получения прав администратора, нарушение конфиденциальности, целостности, доступности защищаемой информации.
2	атаки вследствие использования стека протоколов TCP	атаки типа "отказ в обслуживании, "инъекция данных"	возможность сканирования портов.
3	атаки вследствие использования стека	атаки типа "отказ в обслуживании", атаки через	-

	протоколов OPC	неизвестные или неклассифицированные векторы	
4	атаки вследствие использования стека протоколов FTP	атаки: направленные на получение злоумышленниками прав администратора, связанные с выполнением произвольного кода, типа "отказ в обслуживании"	возможность получения прав администратора.
5	атаки вследствие использования серверами системы удаленного мониторинга и диагностики программного обеспечения MS Windows	атаки, связанные с: выполнением злоумышленникам произвольного кода, повышением злоумышленниками своих привилегий, возможностью обхода процедуры аутентификации, позволяющие нарушителю получить доступ к защищаемой информации, обойти механизмы доверенной загрузки, типа "отказ в обслуживании"	-

Таблица № 2. Перечень базовых уязвимостей системы удаленного мониторинга и диагностики энергетического оборудования, необходимых для проведения анализа

№ п\п	Уязвимость
1.	Среда и инфраструктура:
1.1.	отсутствие физической защиты зданий, дверей и окон
1.2.	неправильное или халатное использование физических средств управления доступом в зданиях, помещениях и энергоустановками
1.3.	нестабильная работа электросети собственных нужд
1.4.	отсутствие системы обеспечения аварийного электропитания оборудования
1.5.	отсутствие средств пожарной сигнализации
1.6.	отсутствие средств пожаротушения
1.7.	размещение в зонах возможного затопления компонентов систем или энергоустановок
2.	Линии связи и сетевые подключения
2.1.	незащищенные линии связи
2.2.	неудовлетворительная стыковка кабелей, спайка оптоволоконных линий

2.3.	отсутствие идентификации и/или аутентификации отправителя и получателя в прикладном программном обеспечении
2.4.	подмена данных
3.	Отказ в обслуживании
3.1.	несанкционированный доступ к каналам связи
3.2.	перехват информации
3.3.	получение несанкционированного доступа к учетной информации (учетные данные пользователей, конфигурационные файлы и прочее)
3.4.	получение несанкционированного доступа
3.5.	коммутируемые линии связи и/или использование сотовых сетей передачи информации
3.6.	незащищенные потоки конфиденциальной информации
3.7.	незащищенные подключения к сетям общего пользования
4.	Сетевое оборудование
4.1.	отсутствие достаточной гибкости маршрутизации для безопасного управления сетью
4.2.	ошибки конфигурации сетевых устройств
4.3.	отсутствие обновлений и патчей на сетевом оборудовании
4.4.	неправильная сетевая топология (например, использование "плоских" локальных сетей)
4.5.	использование паролей с малым набором символов, "паролей по умолчанию" или ненадежных механизмов аутентификации на сетевом оборудовании
4.6.	отказ системы вследствие отказа одного из элементов телекоммуникационного оборудования или агрегирующего контроллера (возможна, например, угроза сбоев в функционировании услуг связи)
5.	Аппаратное обеспечение
5.1.	отсутствие схем периодической замены оборудования системы удаленного мониторинга и диагностики
5.2.	подверженность колебаниям напряжения оборудования системы удаленного мониторинга и диагностики
5.3.	подверженность температурным колебаниям оборудования системы удаленного мониторинга и диагностики
5.4.	подверженность воздействию влаги, пыли, загрязнения оборудования системы удаленного мониторинга и диагностики
5.5.	чувствительность к воздействию электромагнитного излучения оборудования системы удаленного мониторинга и диагностики

5.6.	недостаточное обслуживание/неправильная инсталляция запоминающих сред (в том числе систем хранения данных) системы удаленного мониторинга и диагностики
5.7.	отсутствие контроля за эффективным изменением конфигурации оборудования или телекоммуникационного оборудования сетей связи в системе удаленного мониторинга и диагностики
6.	Программное обеспечение
6.1.	отсутствие полного описания технических требований к разработке программного (программно-аппаратного) обеспечения, применяемого в системе удаленного мониторинга и диагностики
6.2.	отсутствие тестирования или упрощенное тестирование программного обеспечения (возможна угроза использования программного обеспечения несанкционированными пользователями)
6.3.	сложный пользовательский интерфейс компонентов мониторинга и управления энергосетью (возможна, например, угроза ошибки операторов)
6.4.	отсутствие механизмов идентификации и аутентификации, например аутентификации пользователей
6.5.	отсутствие аудиторской проверки установленного программного обеспечения
6.6.	ошибки конфигурации программного обеспечения
6.7.	неустановленные патчи и обновления программного обеспечения (в том числе системного программного обеспечения)
6.8.	отсутствие системы управление паролями учетных записей операторов, управление паролями оборудования, в т.ч. программируемых контроллеров (легко определяемые пароли, хранение в незашифрованном виде, недостаточно частая замена паролей)
6.9.	неправильное присвоение прав доступа (возможна угроза использования программного обеспечения несанкционированным способом)
6.10.	неконтролируемая загрузка, установка и использование программного обеспечения (возможна угроза столкновения с вредоносным программным обеспечением)
6.11.	отсутствие регистрации окончания сеанса при выходе с рабочей станции (возможна, например, угроза использования программного обеспечения несанкционированными пользователями)
6.12.	отсутствие эффективного контроля внесения изменений (возможна угроза программных сбоев)
6.13.	отсутствие документации (возможна угроза ошибки операторов)
6.14.	отсутствие резервных копий информации, обрабатываемой в системе
6.15.	списание или повторное использование запоминающих сред без надлежащего стирания записей
6.16.	наличие недекларированных возможностей (программных и аппаратных

	закладок) в оборудовании иностранных производителей.
7.	Документация
7. 1.	хранение в незащищенных местах (возможна, например, угроза хищения)
7.2.	недостаточная внимательность при уничтожении (возможна, например, угроза хищения)
7.3.	бесконтрольное копирование (возможна угроза хищения)
8.	Персонал
8.1.	отсутствие квалифицированного персонала (возможна, например, угроза халатного отношения работников к своим обязанностям)
8.2.	отсутствие надзора за работой лиц, приглашенных со стороны, или за работой обслуживающего персонала (возможна, например, угроза хищения)
8.3.	недостаточная подготовка персонала по вопросам обеспечения безопасности (возможна, например, угроза ошибки операторов)
8.4.	отсутствие необходимых знаний по вопросам безопасности (возможна, например, угроза ошибок пользователей)
8.5.	неправильное использование программно-аппаратного обеспечения (возможна, например, угроза ошибки операторов)
8.6.	отсутствие механизмов отслеживания и мониторинга (возможна, например, угроза использования программного обеспечения несанкционированным способом)
8.7.	отсутствие политики допустимого использования телекоммуникационных систем для обмена сообщениями (возможна, например, угроза использования сетевых средств несанкционированным способом)
8.8.	несоответствующие процедуры набора кадров (возможна, например, угроза намеренного повреждения или недостаточной квалификации дежурного и оперативного персонала)

Приложение № 3
к приказу Минэнерго России
от 06.11.2018 № 1015

Таблица № 1. Описание угроз информационной безопасности для определения возможных деструктивных действий для каждой из угроз информационной безопасности

Код	Угроза информационной безопасности	Деструктивное действие (Д.№.)										
		1	2	3	4	5	6	7	8	9	10	11
УФД1	Физическое проникновение на		+								+	+

	территорию без возможности проникновения в помещения с техническими средствами обработки, носителями информации, энергоустановок.											
УФД2	Хищение носителя информации, средств обработки информации (процессора, микросхемы, контроллеров, серверов и т.п.), средств коммуникации (маршрутизатора, коммутатора, сетевой карты, модема и т.п.), средств ввода вывода информации (клавиатура и т.п.).	+	+	+	+			+				+
УФД3	Уничтожение носителя информации, средств обработки информации (процессора, микросхемы, контроллеров, серверов и т.п.), средств коммуникации (маршрутизатора, коммутатора, сетевой карты, модема и т.п.), средств ввода вывода информации (клавиатура и т.п.).		+									+
УФД4	Потеря носителя информации.	+	+		+							+
УФД5	Чтение информации с устройств отображения.						+					
УФД6	Повреждение оборудования и/или линий связи.				+						+	+
УФД7	Навязывание ложной информации на уровне конечного оборудования или линий связи (при обмене данными между датчиками и контроллерами, между контроллерами и автоматизированной системы управления).			+	+							+
УФД8	Съем информации с конечного оборудования или линий связи (датчиков, контроллеров).	+				+						
УФД9	Захват объекта защиты, установление над объектом защиты контроля силой или угрозой применения силы, или путем любой другой формы запугивания.								+			+

УФД10	Разрушение объекта защиты или нанесение объекту защиты, здоровью персонала и другим лицам повреждений путем взрыва (обстрела).								+		+	+
УФД11	Размещение и (или) совершение действий в целях размещения каким бы то ни было способом на объекте защиты взрывных устройств (взрывчатых веществ).								+		+	+
УФД12	Загрязнение объекта защиты опасными веществами, угрожающих жизни и здоровью персонала и других лиц.								+	+		
УНДА1	Подбор пароля BIOS или системного программного обеспечения контроллера путем перебора вручную на основе предварительно собранных данных о пользователе.	+		+								
УНДА2	Обход заданного пароля BIOS или системного программного обеспечения контроллера (воздействие на аппаратное обеспечение).	+		+								
УНДА3	Загрузка альтернативной операционной системы с нештатного носителя.	+		+	+							
УНДБ1	Подбор пароля доступа (администратора) в операционную систему компьютера или к системному программному обеспечению контроллера с использованием заданных по умолчанию значений ("заводских" паролей).	+		+	+							
УНДБ 1.2	Подбор пароля доступа (администратора) в операционную систему компьютера или к системному программному обеспечению контроллера посредством перебора различных вариантов.	+		+								
УНДВ	Подбор пароля доступа (администратора) в операционную систему компьютера посредством	+		+								+

	специализированного программного обеспечения.											
УНДГ1	Выявление пароля BIOS при загруженной операционной системы, посредством использования программ выявления пароля.	+		+								
УНДГ2	Выявление пароля доступа других пользователей при загруженной операционной системы (декодирование, из оперативной памяти, копирование хранилищ).	+		+								
УНДГ3	Создание новой учетной записи с расширенными привилегиями.	+		+								+
УНДГ4	Уничтожение системного реестра, обнуление памяти контроллера.				+							+
УНДГ5	Редактирование системного реестра с целью нарушения работоспособности операционной системы и/или прикладного программного обеспечения.	+		+	+							+
УНДГ6	Использование стороннего программного обеспечения с целью несанкционированного воздействия на объект защиты.	+		+	+							+
УНДГ6.4	Заражение вредоносным программным обеспечением автоматизированных рабочих мест, серверов, контроллеров.	+	+	+	+							+
УНДГ7	Перезагрузка операционной системы с целью загрузки альтернативной операционной системы с нештатного носителя для расширения привилегий.	+		+	+							+
УНДГ8	Копирование информации на нештатные носители информации.	+										
УНДГ9	Модификация информации.			+								
УНДГ10	Уничтожение (стирание) информации		+		+							+
УНДГ11	Уничтожение информации путем форматирования		+									+

	носителей информации.											
УУДА1	Сканирование сегмента сети с целью сбора информации.	+										
УУДБ1	Удаленный подбор пароля (администратора) посредством ввода имени и пароля, заданных по умолчанию для используемой операционной системы.	+		+								
УУДБ1.2	Удаленный подбор имени и пароля (администратора) посредством перебора.	+		+	+							+
УУДБ2	Удаленный подбор пароля (пользователя).	+										
УУДБ3	Получение доступа к программам удаленного администрирования.	+		+	+							+
УУДБ4	Внедрение ложного доверенного объекта.	+		+	+							+
УУДБ5	Угрозы удаленного перехвата внешнесегментного сетевого трафика.	+				+						
УУДБ5.3	Удаленный перехват аутентификационной информации, передаваемой в открытом виде.	+										
УУДВ2	Переполнение буфера с запуском исполняемого кода.	+		+	+							
УУДВ10	Перенаправление сетевого трафика.	+		+		+						
УУДГ	Атаки на узлы, подключенные к сети Интернет.	+	+	+	+							+
УУДД	Угрозы отказа в обслуживании (DoS).				+							+
УУДЕ1	Обход межсетевого экрана посредством инкапсуляции данных в заголовки пакетов протокола обмена сообщениями.	+		+	+							+
УМУ1	Хищение мобильного устройства.	+										
УМУ2	Потеря мобильного устройства.	+										
УМУ3	Несанкционированное считывание информации с	+										

	дисплея мобильного устройства.											
УМУ4	Внедрение вредоносного программного обеспечения на мобильное устройство.	+		+								
УМУ5	Перехват паролей/хэшей паролей при доступе с мобильного устройства через незащищенные сети, а также использование мобильного устройства в незащищенных сетях.	+			+							
УМУ6	Выявление хранящихся на мобильном устройстве паролей/хэшей паролей.	+			+							
УО 1	Ошибки при проектировании программных средств.	+	+	+	+							+
УО 2	Ошибки при проектировании технических средств.	+	+	+	+							+
УО 3	Ошибки при изготовлении программных средств.	+	+	+	+							
УО 4	Ошибки при изготовлении технических средств.	+	+	+	+							
УО 5	Ошибки при эксплуатации технических средств.	+	+	+	+							+
УО 6	Ошибки при эксплуатации программных средств.	+	+	+	+							+
УТХ 1	Сбои, отказы технических средств.				+							+
УТХ 2	Сбои, отказы программных средств.				+							+
УБИЛ 80	Отказа подсистемы обеспечения температурного режима.		+								+	+
УБИЛ 82	Физическое устаревание аппаратных компонентов.											+

Приложение № 4
к приказу Минэнерго России
от 06.11.2018 № 1015

Таблица № 1. Классификация нарушителей по направлениям для установления

модели нарушителя информационной безопасности СУМиД

№ ПП	Основные направления для установления модели нарушителя информационной безопасности СУМиД	Виды нарушителей	Описание нарушителей
1	По отношению к СУМиД	внутренние нарушители	с разрешенным доступом к компонентам системы СУМиД и разрешенным доступом на территорию объекта электроэнергетики (эксплуатация, постановка, сопровождение, обслуживание и ремонт аппаратного обеспечения)
		внешние нарушители	посторонние лица, лица, разрабатывающие/распространяющие вирусы и другие программы, предназначенные для осуществления несанкционированного доступа и (или) воздействия на ресурсы и информацию, хранимую на ресурсах, с целью несанкционированного использования или причинения вреда (нанесения ущерба) владельцу информации, ресурса, путем копирования, искажения, удаления или подмены информации) программы, лица, организующие атаки на отказ в обслуживании
		иные нарушители	лица, осуществляющие попытки несанкционированного доступа к СУМиД
2	По правам доступа к компонентам СУМиД	авторизованные (зарегистрированные) пользователи	лица, имеющие разрешенный доступ к компонентам СУМиД.
		системные администраторы, администраторы безопасности компонент СУМиД	
		иные нарушители	лица, не имеющие прав доступа к компонентам СУМиД.
3	По мотивации нарушения	с немотивированными	действие или бездействие пользователей без злого умысла, связанное со случайным нарушением свойств информационной

		действиями	безопасности информационных активов.
		действия в целях самоутверждения	действия пользователей, приводящие к нарушению свойств безопасности СУМиД, в целях самоутверждения.
		корыстный интерес и терроризм	действия пользователей, приводящие к нарушению свойств безопасности информационных активов, направленные на получение выгоды.
4	По возможностям физического доступа	без доступа в контролируемую зону	-
		с доступом в контролируемую зону	без доступа в помещения, в которых расположены компоненты СУМиД; с доступом к техническим средствам СУМиД (в том числе за пределами контролируемой зоны); с доступом к рабочему месту администратора СУМиД.
5	По квалификации	с отсутствием знаний	об устройстве и особенностях функционирования СУМиД
		со знанием	функциональных особенностей СУМиД, протоколов передачи информации, основных закономерностей формирования в ней массивов данных и потоков запросов к ним, с умением пользоваться штатными средствами операционных систем, систем управления базами данных и прикладным программным обеспечением
		с высоким уровнем знаний	в области программирования и уязвимостей применяемых технологий обеспечения функционирования СУМиД
		с обладанием возможностями активного воздействия СУМиД	разработчики, профильные эксперты и другие лица
6	По направлению реализации угроз информационной безопасности	реализация угроз направлена на физический вектор	-
		реализация угроз направлена на СУМиД из сети	-

		Интернет, корпоративной информационной вычислительной системы	
		реализация угроз осуществляется с использованием вредоносного программного обеспечения и сетевых атак внутри СУМиД	-

Приложение № 5
к приказу Минэнерго России
от 06.11.2018 № 1015

Таблица № 1. Взаимосвязь функциональных требований информационной безопасности и целей информационной безопасности представлена

Функциональные требования безопасности	Цели безопасности
FAU_ARP.1	O.AUDITI№G
FAU_GE№.1	O.AUDITI№G
FAU_GE№.2	O.AUDITI№G
FAU_SAA.1	O.AUDITI№G
FAU_SAR.1	O.AUDITI№G
FAU_SAR.2	O.AUDITI№G
FAU_SEL.1	O.AUDITI№G
FAU_STG.1	O.AUDITI№G
FAU_STG.3	O.AUDITI№G
FAU_STG.4	O.AUDITI№G
FAU_COP.1	O.CRYPTO O.I&A
FDP_ACC.1	O.DACCESS

FDP_ACF.1	O.DACCESS
FDP_IFC.2	O.№FLOW
FDP_IFF.1	O.№FLOW
FDP_ITC.2	O.DACCESS O.SUBJECT O.№FLOW
FDP_ITT.1	O.№FLOW
FDP_RIP.2	O.AUDITI№G O.CRYPTO O.DACCESS O.SUBJECT O.№FLOW O.I&A
FDP_ROL.2	O.AVAIL
FDP_SDI.1	O.AVAIL
FIA_AFL.1	O.I&A
FIA_ATD.1	O.I&A O.№FLOW
FIA_SOS.1	O.I&A
FIA_UAU.2	O.I&A
FIA_UID.2	O.I&A O.№FLOW
FIA_USB.2	O.I&A
FMT_MSA.1	O.MA№AGE
FMT_MSA.3	O.MA№AGE
FMT_MTD.1	O.MA№AGE
FMT_REV.1	O.MA№AGE
FMT_SMF.1	O.MA№AGE
FMT_SMR.1	O.MA№AGE
FPT_STM.1	O.AUDITI№G
FPT_TDC.1	O.DACCESS
FPT_ITC.1	O.TRUSTCHA№
FTA_SSL.1	O.I&A
FTA_SSL.2	O.I&A

Таблица № 2. Перечень функциональных компонент для установления функциональных требований к информационной безопасности СУМиД представлен в приложении № 4 к настоящим требованиям.

Идентификатор	Название компоненты
Класс FAU: Аудит информационной безопасности	
FAU_ARP.1	Сигналы нарушения безопасности
FAU_GE№.1	Генерация данных аудита
FAU_GE№.2	Ассоциация идентификатора пользователя
FAU_SAA.1	Анализ потенциального нарушения
FAU_SAR.1	Просмотр журналов аудита
FAU_SAR.2	Ограниченный просмотр журналов аудита
FAU_SEL.1	Избирательный аудит
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.4	Предотвращение потери данных аудита
Класс FCS: Криптографическая защита	
FCS_COP.1	Криптографические операции
Класс FDP: Защита данных пользователя	
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_IFC.2	Полное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FDP_ITC.2	Импорт данных пользователя с атрибутами безопасности
FDP_ITT.1	Базовая защита внутренней передачи
FDP_ROL.2	Расширенный откат к исходному состоянию
FDP_SDI.2	Мониторинг целостности хранимых данных и предпринимаемые действия
Класс FIA: Идентификация и аутентификация	
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов

FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UID.2	Идентификация до любых действий пользователя
FIA_USB.1	Связывание "пользователь-субъект"
Класс FMT: Управление безопасностью	
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными функций безопасности объекта энергетики
FMT_REV.1	Отмена атрибутов безопасности
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности
Класс FPT: Защита функций безопасности объекта энергетики	
FPT_STM.1	Надежные метки времени
FPT_TDC.1	Базовая согласованность данных функций безопасности объекта энергетики между функциями безопасности
Класс FTA: Доступ к программному обеспечению	
FTA_SSL.1	Блокирование сеанса, инициированное функциями безопасности
FTA_SSL.2	Блокирование, инициированное пользователем
FTP_ITC.1	Конфиденциальность экспортируемых данных при передаче

Таблица № 3. Класс FAU: Аудит безопасности

Идентификатор семейства класса FAU	Описание	Применение	Зависимости
FAU_ARP.1	Сигналы нарушения безопасности		
FAU_ARP.1.1	Функции безопасности программного обеспечения должны информировать администратора при обнаружении возможного нарушения безопасности.	Разработчик задания по безопасности для реализации программного обеспечения СУМиД или оборудования, входящего в ее состав, помимо непосредственно информирования администратора может перечислить и другие действия при обнаружении возможного нарушения	FAU_SAA.1 Анализ потенциального нарушения

		безопасности.	
FAU_GE№.1	Генерация данных аудита		
FAU_GE№.1.1	Функции безопасности программного обеспечения должны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту: a) запуск и завершение выполнения функций аудита; b) все события, потенциально подвергаемые аудиту, на базовом уровне аудита; c) другие специально определенные события, подвергаемые аудиту.		
FAU_GE№.1.2	Функции безопасности программного обеспечения должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию: a) дата и время события, тип события, идентификатор субъекта, результат события (успешный или неуспешный); b) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных	В пункте b) FAU_GE№.1.1 выбран уровень аудита базовый, с учетом этого разработчик задания по безопасности в рамках сертификации должен следовать инструкциям ГОСТ Р ИСО/МЭК 15408-2 по включению в FAU_GE№.1 событий согласно выбранному уровню аудита, используя пункты в рубрике "Аудит" для каждого функционального компонента из ГОСТ Р ИСО/МЭК 15408-2, включенного в задание по безопасности и каждого компонента функциональных требований безопасности, определенных настоящими требованиями. Разработчик задания по безопасности может	FPT_STM.1 Надежные метки времени.

	компонентах, которые включены в задание по безопасности на конкретное программное обеспечение.	дополнительно указать в пункте c) FAU_GE№.1.1 другие события, которые программное обеспечение способно подвергать аудиту.	
FAU_GE№.2	Ассоциация идентификатора пользователя		
FAU_GE№.2.1	Функции безопасности программного обеспечения должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.		FAU_GE№.1 Генерация данных аудита; FIA_UID.1 Выбор момента идентификации.
FAU_SAA.1	Анализ потенциального нарушения		
FAU_SAA.1.1	Функции безопасности программного обеспечения должны быть способны применить набор правил мониторинга событий, подвергающихся аудиту и указать на возможное нарушение реализации функциональных требований безопасности, основываясь на этих правилах.		FAU_GE№.1 Генерация данных аудита; FIA_UID.1 Выбор момента идентификации.
FAU_SAA.1.2	Функции безопасности программного обеспечения должны осуществлять следующие правила при мониторинге событий, подвергающихся		

	аудиту: c) накопление или объединение известных подмножество определенных событий, подвергаемых аудиту, указывающих на возможное нарушение безопасности; d) другие правила.		
FAU_SAR.1	Просмотр журналов аудита		
FAU_SAR.1.1	Функции безопасности программного обеспечения должны предоставлять уполномоченные идентифицированные роли из состава ролей безопасности возможность читать список информации аудита из записей аудита.		
FAU_SAR.1.2	Функции безопасности программного обеспечения должны предоставлять записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.		FAU_GE№.1 Генерация данных аудита.
FAU_SAR.2	Ограниченный просмотр журналов аудита		
FAU_SAR.2.1	Функции безопасности программного обеспечения должны предотвращать доступ к чтению записей аудита всем пользователям, за исключением тех, кому явно предоставлен доступ		FAU_SAR.1 Просмотр журналов аудита.

	на чтение.		
FAU_SEL.1	Избирательный аудит		
FAU_SEL.1.1	Функции безопасности программного обеспечения должны обеспечить выбор совокупности событий подвергающихся аудиту из совокупности событий потенциально подверженных аудиту базируясь на следующих атрибутах: e) тип события; f) идентификатор субъекта или пользователя; g) результат (успех или отказ) операции, подверженной аудиту; h) список дополнительных атрибутов, определяемых в задании по безопасности на конкретное программное обеспечение.		FAU_GE№.1 Генерация данных аудита; FMT_MTD.1 Управление данными функций безопасности.
FAU_STG.1	Защищенное хранение журнала аудита		
FAU_STG.1.1	Функции безопасности программного обеспечения должны защищать хранимые в журнале аудита записи от несанкционированного удаления.	Программное обеспечение может обеспечивать хранение журналов аудита как локально, так и обеспечивать передачу журналов на удаленные серверы централизованной системы журналирования для дальнейшей обработки. В последнем случае в системе реализуется локальный стек для записей аудита, перед их отправкой на удаленные сервера, при этом к локальному стеку	

		предъявляются все описанные выше требования.	
FAU_STG.1.2	Функции безопасности программного обеспечения должны обнаруживать и предотвращать несанкционированную модификацию хранимых записей в журналах аудита.		
FAU_STG.3	Действия в случае возможной потери данных аудита		
FAU_STG.3.1	Функции безопасности программного обеспечения должны обеспечить резервное копирование на внешние ресурсы журналов аудита, в случае если журналы аудита превышают допустимое ограничение.		FAU_STG.1 Защищенное хранение журналов аудита.
FAU_STG.4	Предотвращение потери данных аудита		
FAU_STG.4.1	Функции безопасности программного обеспечения должны обеспечить удаление самой старой (по временному параметру) записи аудита и записи поверх нее новой при переполнении журнала аудита.		FAU_STG.1 Защищенное хранение журналов аудита.

Таблица № 4. Класс FCS: Криптографическая защита

Идентификатор	Описание	Замечания по применению	Зависимости
FCS_COP.1	Криптографические операции		
FCS_COP.1.1	Функции безопасности программного обеспечения должны поддерживать	Криптографические механизмы защиты реализуются в случае предоставления доступа к программному обеспечению	

	шифрование, расшифрование, контроль целостности и аутентификацию сторон в соответствии с одним из перечисленных криптографических алгоритмов: i) SSH с применением ГОСТ 28147 с 256-битным ключом и ГОСТ 34.10 (а также другими действующими на момент применения Требований принятых в качестве государственных стандартов Российской Федерации), в качестве цифровой подписи; j) TLS с применением ГОСТ 28147 с 256-битным ключом и ГОСТ 34.10 (а также другими действующими на момент применения требований принятых в качестве государственных стандартов Российской Федерации), в качестве цифровой подписи; k) IPSEC с IKE позволяющем применять ГОСТ 28147 с 256-битным ключом и ГОСТ 34.10 (а также другими действующими на момент применения Требований принятых в качестве государственных стандартов	или при обмене информацией по открытым каналам связи (каналам операторов связи сети связи общего пользования), а также в целях взаимной аутентификации с иными информационными системами с отличным от текущей уровнем доверия.	

	Российской Федерации), в качестве цифровой подписи.		
FCS_COP.1.2	Функции безопасности программного обеспечения должны поддерживать технологическую подпись данных и защиту целостности данных с применением криптографических алгоритмов: ГОСТ 34.10, в качестве цифровой подписи и ГОСТ 34.11 в качестве выработки хеш-функции (а также другими действующими на момент применения Требований, принятых в качестве государственных стандартов Российской Федерации).		

Таблица № 5. Класс FDP: Защита данных пользователя

Идентификатор семейства класса FDP	Описание	Замечания по применению	Зависимости
FDP_ACC.1	Ограниченное управление доступом		
FDP_ACC.1.1	Функции безопасности программного обеспечения должны осуществлять ролевой контроль доступа для субъектов: пользователи системы, процессы; объектов: данные обрабатываемые программным обеспечением;		

	операций: все реализованные программным обеспечением операции.		
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности		
FDP_ACF.1.1	Функции безопасности программного обеспечения должны осуществлять ролевой контроль доступа к объектам основываясь на атрибутах безопасности субъекта: идентификатор пользователя/процесса, роль пользователя/процесса, атрибутах безопасности объекта: идентификатор объекта, разрешения для объекта.		
FDP_ACF.1.2	Функции безопасности программного обеспечения должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: субъект должен быть связан с правами доступа к объекту в соответствии с назначенной ролью.		
FDP_ACF.1.3	Функции безопасности программного обеспечения должны явно разрешать доступ субъектов к		

	объектам, основываясь на следующих дополнительных правилах, дополнительные правила		
FDP_ACF.1.4	Функции безопасности программного обеспечения должны отказывать в доступе субъектов к объектам, если доступ не разрешен.		FDP_ACC.1 Ограниченное управление доступом. FMT_MSA.3 Инициализация статических атрибутов.
FDP_IFC.2	Полное управление информационными потоками		
FDP_IFC.2.1	Функции безопасности программного обеспечения должны осуществлять контроль информационных потоков для: l) Субъектов: Неавторизованные внешние по отношению к программному обеспечению сущности (иные информационные системы), которые получают или передают информацию для обработки рассматриваемым программным обеспечением. m) Информации: перечень обрабатываемой программным обеспечением информации. и всеми операциями перемещения управляемой информации к управляемым		

	субъектам, обрабатываемым программным обеспечением, и от них.		
FDP_IFF.1	Простые атрибуты безопасности		
FDP_IFF.1.1	Функции безопасности программного обеспечения должны осуществлять контроль информационных потоков, основанный на следующих атрибутах безопасности субъектов и информации: n) идентификатор пользователя или процесса; o) логический или физический сетевой интерфейс, по которому данные загружаются в систему; p) атрибуты безопасности стека протоколов TCP/IP: IP адрес источника и назначения порт UDP источника и назначения флаги в заголовках протокола TCP q) атрибуты безопасности протокола IEEE 802.1Q VLA№: теги VLA№		
FDP_IFF.1.2	Функции безопасности программного обеспечения должны разрешать информационный поток для управляемого субъекта и управляемой		FDP_IFC.1 Ограниченное управление информационными потоками FDP_MSA.3 Инициализация статических атрибутов

	информации посредством управляемой операции, если заданы правила обмена в следующем формате: перечень операций - список поддерживаемых отношений, основанный на атрибутах безопасности		
FDP_ITC.2	Импорт данных пользователя с атрибутами безопасности		
FDP_ITC.2.1	Функции безопасности программного обеспечения должны осуществлять контроль информационных потоков и управление доступом при импорте данных пользователя из иного программного обеспечения.		
FDP_ITC.2.2	Функции безопасности программного обеспечения должны использовать атрибуты безопасности, ассоциированные с импортируемыми данными пользователя.		
FDP_ITC.2.3	Функции безопасности программного обеспечения должны обеспечить такой протокол интеграции, который предусматривает однозначную ассоциацию между атрибутами безопасности и полученными		

	данными пользователя.		
FDP_ITC.2.4	Функции безопасности программного обеспечения должны обеспечить интерпретацию атрибутов безопасности пользователя такой как предусмотрено источником данных пользователя.		
FDP_ITT.1	Базовая защита внутренней передачи		
FDP_ITT.1.1	Функции безопасности программного обеспечения должны осуществлять контроль информационных потоков и управление доступом, чтобы предотвратить модификацию и недоступность данных при их передаче между физически разделенными компонентами аппаратной платформы, на которой функционирует программное обеспечение.		
FDP_ROL.2	Расширенный откат к исходному состоянию		
FDP_ROL.2.1	Функции безопасности программного обеспечения должны осуществлять управление доступом для разрешения возврата (отката) всех операций к определенному начальному		

	состоянию.		
FDP_SDI.2	Мониторинг целостности хранимых данных и предпринимаемые действия		
FDP_SDI.2.1	Функции безопасности программного обеспечения должны контролировать данные, хранимые в местах хранения, контролируемых программным обеспечением, на наличие ошибок контрольных сумм для всех объектов.		
FDP_SDI.2.2	При обнаружении ошибки целостности данных функции безопасности программного обеспечения должны обеспечить загрузку данных по умолчанию (эталонных).		

Таблица № 6. Класс FIA: Идентификация и аутентификация

Идентификатор семейства класса FIA	Описание	Замечания по применению	Зависимости
FIA_AFL.1	Обработка отказов аутентификации		
FIA_AFL.1.1	Функции безопасности программного обеспечения должны обнаруживать, когда произойдет три неуспешных попыток аутентификации, относящихся к вводу пароля пользователя.		
FIA_AFL.1.2	При достижении определенного числа неуспешных попыток аутентификации функции безопасности		FIA_UAU.1 Выбор момента аутентификации

	программного обеспечения должны выполнить блокировку доступа пользователям на 30 минут.		
FIA_ATD.1	Определение атрибутов пользователя		
FIA_ATD.1.1	Функции безопасности программного обеспечения должны поддерживать для каждого пользователя следующий список атрибутов безопасности: роль пользователя; сертификат пользователя выданный доверенной стороной; иные атрибуты определенные в рамках Задания по безопасности на программное обеспечение.		
FIA_SOS.1	Верификация секретов		
FIA_SOS.1.1	Функции безопасности должны предоставить механизм для верификации. Механизм верификации должен соответствовать следующей метрике: вероятность того, что секретная информация может быть обнаружена нарушителем в течение существования секрета должна быть меньше чем 20 процентов		
FIA_UAU.2	Аутентификация до любых действий пользователя		

FIA_UAU.2.1	Функции безопасности должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве функций безопасности от имени этого пользователя.		FIA_UID.1 Выбор момента идентификации.
FIA_UID.2	Идентификация до любых действий пользователя		
FIA_UID.2.1	Функции безопасности программного обеспечения должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве функций безопасности от имени этого пользователя.		
FIA_USB.1	Связывание "пользователь-субъект"		
FIA_USB.1.1	Функции безопасности программного обеспечения должны ассоциировать соответствующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя.		

Таблица № 7. Класс FMT: Управление безопасностью

Идентификатор семейства	Описание	Замечания по применению	Зависимости

класса FMT			
FMT_MSA.1	Управление атрибутами безопасности		
FMT_MSA.1.1	Функции безопасности программного обеспечения должны осуществлять управление доступом, основанное на ролях, чтобы ограничить возможность модификации, изменения значений по умолчанию атрибутов безопасности объектов программного обеспечения, только владельцам объектов.		FDP_ACC.1 Ограниченное управление доступом или FDP_IFC.1 Ограниченное управление информационными потоками. FMT_SMR.1 Роли безопасности.
FMT_MSA.3	Инициализация статических атрибутов		
FMT_MSA.3.1	Функции безопасности должны осуществлять управление доступом, основанное на ролях, чтобы обеспечить ограничительные значения по умолчанию для атрибутов безопасности, которые используются для реализации требований безопасности.		
FMT_MSA.3.2	Функции безопасности должны предоставлять возможность уполномоченному пользователю в соответствии с его ролью определять альтернативные начальные значения для отмены значений		FMT_MSA.1 Управление атрибутами безопасности. FMT_SMR.1 Роли безопасности.

	по умолчанию при создании объекта или информации.		
FMT_MTD.1	Управление данными функций безопасности		
FMT_MTD.1.1	Функции безопасности программного обеспечения должны ограничивать возможность модификации следующих данных: текущее значение времени, показания счетчиков команд, записи журнала аудита информационной безопасности только администраторам информационной безопасности.		FMT_SMR.1 Роли безопасности.
FMT_REV.1	Отмена атрибутов безопасности		
FMT_REV.1.1	Функции безопасности программного обеспечения должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с пользователями, субъектами и объектами программного обеспечения для администратора информационной безопасности.		
FMT_SMF.1	Спецификация функций управления		
FMT_SMF.1.1	Функции безопасности программного обеспечения должны быть способны к выполнению следующих функций управления:		

	резервное копирование конфигурации, загрузка резервной копии конфигурации.		
FMT_SMR.1	Роли безопасности		
FMT_SMR.1.1	Функции безопасности программного обеспечения должны поддерживать следующие роли по умолчанию: администратор; администратор ИБ; оператор.		FIA_UID.1 Выбор момента идентификации.

Таблица № 8. Класс FPT: Защита функций безопасности объекта энергетики

Идентификатор семейства класса FPT	Описание	Замечания по применению	Зависимости
FPT_STM.1	Надежные метки времени		
FPT_STM.1.1	Функции безопасности программного обеспечения должны быть способны предоставлять надежные метки времени для собственного использования.		
FPT_ITC.1	Конфиденциальность экспортируемых данных при передаче		
FPT_ITC.1.1	Функции безопасности программного обеспечения должны обеспечить конфиденциальность всех данных передаваемых от функций безопасности программного обеспечения другому доверенному программному продукту.		

FPT_TDC.1	Базовая согласованность данных функций безопасности объекта между функциями безопасности		
FPT_TDC.1.1	Функции безопасности программного обеспечения должны обеспечить способность согласованно интерпретировать типы данных функций безопасности, совместно используемые с другим доверенным программным продуктом.		

Таблица № 9. Класс FTA: Доступ к программному обеспечению

Идентификатор семейства класса FTA	Описание	Замечания по применению	Зависимости
FTA_SSL.1	Блокирование сеанса, инициированное функциями безопасности		
FTA_SSL.1.1	Функции безопасности программного обеспечения должны блокировать интерактивный сеанс после 30 минут бездействия пользователя, для чего предпринимаются следующие действия: r) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида; s) блокирование любых действий по доступу к данным пользователей/устройствам отображения, кроме необходимых для разблокировки		

	сеанса.		
FTA_SSL.2	Блокирование сеанса, инициированное пользователем		
FTA_SSL.2.1	Функции безопасности программного обеспечения должны допускать инициированное пользователем блокирование своего интерактивного сеанса, для чего предпринимаются следующие действия: t) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида; u) блокирование любых действий по доступу к данным пользователей/устройствам отображения, кроме необходимых для разблокировки сеанса.		

Приложение № 6
к приказу Минэнерго России
от 06.11.2018 № 1015

Таблица № 1. Описание взаимосвязи классов доверия и компонентов доверия для достижения целей информационной безопасности

Классы доверия	Идентификаторы семейства классов доверия	Названия компонентов доверия
Класс ACM Управление конфигурацией (УК)	ACM_AUT.1	Частичная автоматизация УК
	ACM_CAP.4	Поддержка генерации, процедуры приемки
	ACM_SCP.2	Охват УК отслеживания проблем
Класс ADO	ADO_DEL.2	Обнаружение модификации

Поставка и эксплуатация	ADO_IGS.1	Процедуры установки, генерации и запуска
Класс ADV Разработка	ADV_FSP.2	Полностью определенные внешние интерфейсы
	ADV_HLD.2	Детализация вопросов безопасности в проекте верхнего уровня
	ADV_IMP.1	Подмножество реализации ФБО
	ADV_LLD.1	Описательный проект нижнего уровня
	ADV_RCR.1	Неформальная демонстрация соответствия
	ADV_SPM.1	Неформальная модель политики безопасности программного обеспечения
Класс AGD Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Класс ALC Поддержка жизненного цикла	ALC_DVS.1	Идентификация мер безопасности
	ALC_LCD.1	Определение модели жизненного цикла разработчиком
	ALC_TAT.1	Полностью определенные инструментальные средства разработки
Класс ALC Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.1	Тестирование: проект верхнего уровня
	ATE_FU№.1	Функциональное тестирование
	ATE_I№D.2	Выборочное независимое тестирование
Класс AVA Оценка уязвимостей	AVA_MSU.2	Подтверждение правильности анализа
	AVA_SOF.1	Оценка стойкости функции безопасности программного обеспечения
	AVA_VLA.2	Независимый анализ уязвимостей

Таблица № 2. Класс ACM: Управление конфигурацией

Идентификатор		Зависимости		Элементы действий разработчика		Элементы содержания и представления свидетельств		Элементы действий оценщика	
ACM_AUT.1	Частичная автоматизация УК	ACM_CAP.3	Средства контроля авторизации.	ACM_AUT.1.1D	Разработчик должен использовать систему УК.	ACM_AUT.1.1C	Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации программного обеспечения производятся только санкционированные изменения.	ACM_AUT.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
				ACM_AUT.1.2D	Разработчик должен представить план УК.	ACM_AUT.1.2C	Система УК должна предоставить автоматизированные средства для поддержки генерации программного обеспечения.		
						ACM_AUT.1.3C	План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.		
						ACM_AUT.1.4C	План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.		
ACM_CAP.4	Поддержка генерации, процедуры приемки	ACM_SCP.1 ALC_DVS.1	Охват УК объекта оценки, Идентификация мер безопасности.	ACM_CAP.4.1D	Разработчик должен предоставить маркировку для программного обеспечения	ACM_CAP.4.1C	Маркировка программного обеспечения должна быть уникальна для каждой версии программного обеспечения.	ACM_CAP.4.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
				ACM_CAP.4.2D	Разработчик должен использовать систему УК.	ACM_CAP.4.2C	Программное обеспечение должно быть помечено маркировкой.		
				ACM_CAP.4.3D	Разработчик должен представить документацию УК.	ACM_CAP.4.3C	Документация УК должна включать в себя список конфигурации, план УК и план приемки.		
						ACM_CAP.	Список конфигурации должен		

						4.4C	содержать описание элементов конфигурации, входящих в программное обеспечение.		
						ACM_CAP.4.5C	Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.		
						ACM_CAP.4.6C	Система УК должна уникально идентифицировать все элементы конфигурации.		
						ACM_CAP.4.7C	План УК должен содержать описание, как используется система УК.		
						ACM_CAP.4.8C	Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.		
						ACM_CAP.4.9C	Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.		
						ACM_CAP.4.10C	Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.		
						ACM_CAP.4.11C	Система УК должна поддерживать генерацию программного обеспечения.		
						ACM_CAP.4.12C	План приемки должен содержать описание процедур, используемых для приемки модифицированного или вновь созданного элемента конфигурации как части программного обеспечения.		
ACM_SCP.2	Охват УК отслеживания проблем	ACM_CAP.3	Средства контроля авторизации.	ACM_SCP.3.1D	Разработчик должен представить документацию УК.	ACM_SCP.2.1C	Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации программного обеспечения,	ACM_SCP.2.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет

							проектную документацию, тестовую документацию, документацию пользователя, документацию администратора, документацию УК и недостатки безопасности.		всем требованиям к содержанию и представлению свидетельств.

Таблица № 3. Класс ADO: Поставка и эксплуатация

Идентификатор		Зависимости		Элементы действий разработчика		Элементы содержания и представления свидетельств		Элементы действий оценщика	
ADO_DEL.2	Обнаружение модификации	ACM_CAP.3	Средства контроля авторизации.	ADO_DEL.2.1D	Разработчик должен документировать процедуры поставки программного обеспечения или его частей пользователю.	ADO_DEL.2.1C	Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий к местам использования.	ADO_DEL.2.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
				ADO_DEL.2.2	Разработчик должен использовать процедуры поставки.	ADO_DEL.2.2C	Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.		
						ADO_DEL.2.3C	Документация поставки должна содержать описание, как различные процедуры позволяют обнаружить попытку подмены от имени разработчика, даже в тех случаях, когда разработчик ничего не отсылал к месту использования.		
ADO_IGS.1	Процедуры установки, генерации и запуска	AGD_ADM.1	Руководство администратора.	ADO_IGS.1.1D	Разработчик должен задокументировать процедуры, необходимы	ADO_IGS.1.1C	Документация должна содержать описание последовательности действий, необходимых для безопасной установки, генерации и запуска программного	ADO_IGS.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям

					е для безопасной установки, генерации и запуска программного обеспечения.		обеспечения.		к содержанию и представлению свидетельств.
								ADO_IGS.1.2E	Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

Таблица № 4. Класс ADV: Разработка

Идентификатор		Зависимости		Элементы действий разработчика		Элементы содержания и представления свидетельств		Элементы действий оценщика	
ADV_FSP.2	Полностью определенные внешние интерфейсы	ADV_RCR.1	Неформальная демонстрация соответствия.	ADV_FSP.2.1D	Разработчик должен представить функциональную спецификацию.	ADV_FSP.2.1C	Функциональная спецификация должна содержать неформальное описание функций безопасности программного обеспечения (ФБО) и их внешних интерфейсов.	ADV_FSP.2.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
						ADV_FSP.2.2C	Функциональная спецификация должна быть внутренне непротиворечивой.	ADV_FSP.2.2E	Оценщик должен сделать независимое заключение, что функциональная спецификация - точное и полное отображение функциональных требований безопасности программного обеспечения.
						ADV_FSP.2.3C	Функциональная спецификация должна содержать описание назначения и методов		

							использования всех внешних интерфейсов ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.		
						ADV_FSP.2.4C	Функциональная спецификация должна полностью представить ФБО.		
						ADV_FSP.2.5C	Функциональная спецификация должна включать в себя логическое обоснование, что ФБО полностью представлены.		
ADV_HLD.2	Детализация вопросов безопасности в проекте верхнего уровня	ADV_FSP.1	Неформальная функциональная спецификация	ADV_HLD.3.1D	Разработчик должен представить проект верхнего уровня функций безопасности программного обеспечения.	ADV_HLD.2.1C	Представление проекта верхнего уровня должно быть неформальным.	ADV_HLD.2.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
		ADV_RCR.1	Неформальная демонстрация соответствия.			ADV_HLD.2.2C	Проект верхнего уровня должен быть внутренне непротиворечивым.	ADV_HLD.2.2E	Оценщик должен сделать независимое заключение, что проект верхнего уровня - точное и полное отображение функциональных требований безопасности программного обеспечение.
						ADV_HLD.2.3C	Проект верхнего уровня должен содержать описание структуры Функций безопасности в терминах подсистем безопасности.		
						ADV_HLD.2.4C	Проект верхнего уровня должен содержать описание функциональных		

							возможностей безопасности, предоставленных каждой подсистемой программного обеспечения.		
						ADV_HLD.2.5C	Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации функций безопасности.		
						ADV_HLD.2.6C	Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем безопасности.		
						ADV_HLD.2.7C	Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем безопасности являются видимыми извне программного обеспечения.		
						ADV_HLD.2.8C	Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем безопасности, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.		
						ADV_HLD.2.9C	Проект верхнего уровня должен содержать описание разделения программного обеспечения на подсистемы, осуществляющие политику безопасности, и прочие.		
ADV_IMP.1	Подмножество реализации ФБО	ADV_LLD.1	Описательный проект нижнего уровня,	ADV_IMP.1.1D	Разработчик должен обеспечить представление реализации для выбранного подмножества функций безопасности.	ADV_IMP.1.1C	Представление реализации должно однозначно определить функции безопасности программного обеспечения на таком уровне детализации, что они могут быть созданы без дальнейших проектных решений.	ADV_IMP.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

		ADV_RCR.1	Неформальная демонстрация соответствия,			ADV_IMP.1.2C	Представление реализации должно быть внутренне непротиворечивым.	ADV_IMP.1.2E	Оценщик должен сделать независимое заключение, что наименее абстрактное представление функций безопасности - точное и полное отображение функциональных требований безопасности к программному обеспечению.
		ALC_TAT.1	Полностью определенные инструментальные средства разработки.						
ADV_LLD.1	Описательный проект нижнего уровня	ADV_HLD.2	Детализация вопросов безопасности в проекте верхнего уровня.	ADV_LLD.1.1D	Разработчик должен представить проект нижнего уровня функций безопасности.	ADV_LLD.1.1C	Представление проекта нижнего уровня должно быть неформальным.	ADV_LLD.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
		ADV_RCR.1	Неформальная демонстрация соответствия.			ADV_LLD.1.2C	Проект нижнего уровня должен быть внутренне непротиворечивым.	ADV_LLD.1.2E	Оценщик должен сделать независимое заключение, что проект нижнего уровня - точное и полное отображение функциональных требований безопасности к программному обеспечению.
						ADV_LLD.1.3C	Проект нижнего уровня должен содержать описание функций безопасности в терминах модулей.		
						ADV_LLD.1	Проект нижнего уровня		

						.4C	должен содержать описание назначения каждого модуля.		
						ADV_LLD.1.5C	Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.		
						ADV_LLD.1.6C	Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих политики безопасности.		
						ADV_LLD.1.7C	Проект нижнего уровня должен идентифицировать все интерфейсы модулей безопасности.		
						ADV_LLD.1.8C	Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей безопасности являются видимыми извне.		
						ADV_LLD.1.9C	Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей безопасности, предоставляя, при необходимости, детализацию результатов, нештатных ситуаций и сообщений об ошибках.		
						ADV_LLD.1.10C	Проект нижнего уровня должен содержать описание разделения программного обеспечения на модули, осуществляющие политики безопасности, и прочие.		
ADV_RCR.1 (1)	Неформальная демонстрация соответствия			ADV_RCR.1.1D	Разработчик должен представить анализ соответствия между всеми смежными	ADV_RCR.1.1C	Для каждой смежной пары, имеющихся представлений безопасности, анализ должен демонстрировать, что все функциональные возможности более абстрактного представления функций безопасности	ADV_RCR.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению

					парами имеющихся представлений функций безопасности.		правильно и полностью уточнены в менее абстрактном представлении функций безопасности.		свидетельств.
ADV_RCR.1 (2)	Неформальная демонстрация соответствия			ADV_RCR.1.1D	Разработчик должен представить анализ соответствия между исходными текстами программного обеспечения и его объектным (загрузочным) кодом.	ADV_RCR.1.1C	Для смежной пары представлений функций безопасности, указанных в ADV_RCR.1.1D, анализ должен демонстрировать, что все функциональные возможности более абстрактного представления функций безопасности, правильно и полностью уточнены в менее абстрактном представлении функций безопасности	ADV_SPM.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
								ADV_RCR.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
ADV_SPM.1	Неформальная модель политики безопасности ОО	ADV_FSP.1	Неформальная функциональная спецификация.	ADV_SPM.1.1D	Разработчик должен представить модель политики безопасности.	ADV_SPM.1.1C	Модель политики безопасности должна быть неформальной.		
				ADV_SPM.1.2D	Разработчик должен продемонстрировать или доказать, где это требуется, соответствие между функциональной спецификацией и моделью политики безопасности.	ADV_SPM.1.2C	Модель политики безопасности должна содержать описание правил и характеристик всех политик, которые могут быть смоделированы.		
				ADV_SPM.1.3C			Модель политики		

							безопасности должна включать в себя логическое обоснование, которое демонстрирует, что она согласована и полна относительно всех политик безопасности, которые могут быть смоделированы.		
				ADV_SPM.1.4C			Демонстрация соответствия между моделью политики безопасности и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели политики безопасности.		

Таблица № 5. Класс AGD: Руководства

Идентификатор		Зависимости		Элементы действий разработчика		Элементы содержания и представления свидетельств		Элементы действий оценщика	
AGD_ADM.1	Руководство администратора	ADV_FSP.1	Неформальная функциональная спецификация.	AGD_ADM.1.1D	Разработчик должен представить руководство администратора, предназначенное для персонала системного администрирования	AGD_ADM.1.1C	Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору программного обеспечения.	AGD_ADM.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
						AGD_ADM.1.2C	Руководство администратора должно содержать описание того, как управлять программным обеспечением 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 программного обеспечения.		
						AGD_ADM.1.5C	Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором информационной безопасности, 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 функциями безопасности программного обеспечения.		
						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.		
AGD_USR.1	Руководство пользователя	ADV_FSP.1	Неформальная функциональная спецификация.	AGD_USR.1.1D	Разработчик должен представить руководство пользователя.	AGD_USR.1.1C	Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям программного обеспечения, не связанным с администрированием.	AGD_USR.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
						AGD_USR.1.2C	Руководство пользователя должно содержать описание		

							применения доступных пользователям функций безопасности, предоставляемых программным обеспечением.		
						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 программного обеспечения, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности программного обеспечения.		
						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.		

Таблица № 6. Класс ALC: Поддержка жизненного цикла

Идентификатор		Зависимости		Элементы действий разработчика		Элементы содержания и представления свидетельств		Элементы действий оценщика	
ALC_DVS.1	Идентификация мер безопасности			ALC_DVS.1.1D	Разработчик должен иметь документацию по безопасности разработки.	ALC_DVS.1.1C	Документация по безопасности разработки должна содержать описание всех физических, процедурных, относящихся к персоналу и других мер безопасности, которые необходимы для защиты конфиденциальности и	ALC_DVS.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

							целостности проекта программного обеспечения и его реализации в среде разработки.		
						ALC_DVS.1.2C	Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения программного обеспечения.	ALC_DVS.1.2E	Оценщик должен подтвердить применение мер безопасности.
ALC_LCD.1	Определение модели жизненного цикла разработчиком			ALC_LCD.1.1D	Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении программного обеспечения.	ALC_LCD.1.1C	Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении программного обеспечения.	ALC_LCD.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
				ALC_LCD.1.2D	Разработчик должен представить документацию по определению жизненного цикла.	ALC_LCD.1.2C	Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением программного обеспечения.		
ALC_TAT.1	Полностью определенные инструментальные средства разработки	ADV_IMP.1	Подмножество реализации функций безопасности	ALC_TAT.1.1D	Разработчик должен идентифицировать инструментальные средства разработки программного обеспечения.	ALC_TAT.1.1C	Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.	ALC_TAT.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

				ALC_TAT.1.2D	Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.	ALC_TAT.1.2C	Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.		
						ALC_TAT.1.3C	Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.		

Таблица № 7. Класс ATE: Тестирование

Идентификатор		Зависимости		Элементы действий разработчика		Элементы содержания и представления свидетельств		Элементы действий оценщика	
ATE_COV.2	Анализ покрытия	ADV_FSP.1	Неформальная функциональная спецификация	ATE_COV.2.1D	Разработчик должен представить анализ покрытия тестами.	ATE_COV.2.1C	Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и описанием функций безопасности в функциональной спецификации.	ATE_COV.2.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
		ATE_FU№.1	Функциональное тестирование			ATE_COV.2.2C	Анализ покрытия тестами должен демонстрировать полное соответствие между описанием функций безопасности в функциональной спецификации и тестами, идентифицированными в тестовой документации.		
ATE_DPT.1	Тестирование: проект верхнего уровня	ADV_HLD.1	Описательный проект верхнего уровня	ATE_DPT.1.1D	Разработчик должен представить анализ глубины тестирования.	ATE_DPT.1.1C	Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что функции безопасности выполняются в соответствии с проектом верхнего уровня.	ATE_DPT.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению

									свидетельств.
		ATE_FU№.1	Функциональное тестирование						
ATE_FU№.1	Функциональное тестирование			ATE_FU№.1.1D	Разработчик должен протестировать функции безопасности и задокументировать результаты.	ATE_FU№.1.1C	Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.	ATE_FU№.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
				ATE_FU№.1.2D	Разработчик должен представить тестовую документацию.	ATE_FU№.1.2C	Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей тестирования.		
						ATE_FU№.1.3C	Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.		
						ATE_FU№.1.4C	Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.		
						ATE_FU№.1.5C	Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.		
ATE_I№D.2	Выборочное независимое тестирование	ADV_FSP.1	Неформальная функциональная спецификаци	ATE_I№D.2.1D	Разработчик должен представить программное	ATE_I№D.2.1C	Программное обеспечение должно быть пригодно для тестирования.	ATE_I№D.2.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет

			я		обеспечение для тестирования.				всем требованиям к содержанию и представлению свидетельств.
		AGD_ ADM.1	Руководство администратора			ATE_I№D.2 .2C	Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании функций безопасности.	ATE_I№D.2 .2E	Оценщик должен протестировать подмножество функций безопасности, чтобы подтвердить, что программное обеспечение функционирует в соответствии со спецификациями.
		AGD_ USR.1	Руководство пользователя					ATE_I№D.2 .3E	Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.
		ATE_F U№.1	Функциональное тестирование						

Таблица № 8. Класс AVA: Оценка уязвимостей

Идентификатор		Зависимости		Элементы действий разработчика		Элементы содержания и представления свидетельств		Элементы действий оценщика	
AVA_ MSU.2	Подтверждение правильности анализа	ADO_I GS.1	Процедуры установки, генерации и запуска	AVA_MSU. 2.1	Разработчик должен представить руководства по применению программного обеспечения.	AVA_MSU. 2.1C	Руководства должны идентифицировать все возможные режимы эксплуатации программного обеспечения (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.	AVA_MSU. 2.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
		ADV_F SP.1	Неформальная функциональ	AVA_MSU. 2.2D	Разработчик должен задокумент	AVA_MSU. 2.2C	Руководства должны быть полны, понятны, непротиворечивы и	AVA_MSU. 2.2E	Оценщик должен повторить все процедуры

			ная спецификация		ировать анализ полноты и непротиворечивости руководств.		обоснованы.		конфигурирования и установки и выборочно другие процедуры для подтверждения, что программное обеспечение можно безопасно конфигурировать и использовать, применяя только представленные руководства.
		AGD_ADM.1	Руководство администратора			AVA_MSU.2.3C	Руководства должны содержать список всех предположений относительно среды эксплуатации.	AVA_MSU.2.3E	Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.
		AGD_USR.1	Руководство пользователя			AVA_MSU.2.4C	Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).	AVA_MSU.2.4E	Оценщик должен подтвердить, что документация анализа показывает обеспечение руководствами безопасного функционирования во всех режимах эксплуатации программного обеспечения.
						AVA_MSU.2.5C	Документация анализа должна демонстрировать, что руководства полны.		
AVA_SOF.1	Оценка стойкости функции безопасности ОО	ADV_FSP.1	Неформальная функциональная спецификация	AVA_SOF.1.1D	Разработчик должен выполнить анализ стойкости функции безопасности программного обеспечения	AVA_SOF.1.1C	Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности программного обеспечения, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в настоящих требованиях.	AVA_SOF.1.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

					для каждого механизма, идентифицированного в задании по безопасности как имеющего утверждение относительно стойкости функции безопасности программного обеспечения.				
		ADV_HLD.1	Описательный проект верхнего уровня			AVA_SOF.1.2C	Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности программного обеспечения, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в настоящих требованиях.	AVA_SOF.1.2E	Оценщик должен подтвердить, что утверждения относительно стойкости корректны.
AVA_VLA.2	Независимый анализ уязвимостей	ADV_FSP.1	Неформальная функциональная спецификация	AVA_VLA.2.1D	Разработчик должен выполнить и задокументировать анализ поставляемых материалов программного обеспечения по поиску путей, которыми пользователь может нарушить политики безопасности.	AVA_VLA.2.1C	Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования программного обеспечения.	AVA_VLA.2.1E	Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

		ADV_HLD.2	Детализация вопросов безопасности в проекте верхнего уровня	AVA_VLA.2.2D	Разработчик должен задокументировать местоположение идентифицированных уязвимостей.	AVA_VLA.2.2C	Документация должна содержать строгое обоснование, что программное обеспечение с идентифицированными уязвимостями является стойким к явным нападениям проникновения.	AVA_VLA.2.2E	Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.
		ADV_IMP.1	Подмножество реализации функций безопасности					AVA_VLA.2.3E	Оценщик должен выполнить независимый анализ уязвимостей, основываясь, в том числе, на результатах: - контроля связей функциональных объектов (модулей, процедур, функций) по управлению и по информации; - контроля информационных объектов различных типов, - формирования перечня маршрутов выполнения функциональных объектов (процедур, функций);
		ADV_LLD.1	Описательный проект нижнего уровня						
		AGD_ADM.1	Руководство администратора						
		AGD_USR.1	Руководство пользователя.						
									- контроля выполнения функциональных объектов (процедур, функций); - сопоставления фактических маршрутов

									выполнения функциональных объектов (процедур, функций) и маршрутов, построенных при формировании перечня маршрутов выполнения функциональных объектов.
								AVA_VLA.2.4E	Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.
								AVA_VLA.2.5E	Оценщик должен сделать независимое заключение, что программное обеспечение является стойким к нападениям проникновения, выполняемым нарушителем, обладающим средним и высоким потенциалом нападения.