**ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)**

107016, Москва, ул. Неглинная, д. 12, к. В
www.cbr.ru
тел.: (499) 300-30-00, 8 (800) 300-30-00

От 26.12.2025 № ИН-017-56/118

Операторам по переводу денежных средств

Некредитным финансовым организациям

Операторам услуг платежной инфраструктуры

Информационное письмо Банка России
о новой редакции методического документа

В рамках подкомитета № 1 «Безопасность финансовых (банковских) операций» Технического комитета по стандартизации № 122 «Стандарты финансовых операций»[1] одобрена новая редакция методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций» (далее – документ), размещенная на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» в подразделе «Стандарты Банка России» раздела «Информационная безопасность».

Документ обновлен, в том числе с учетом практики применения «ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования»[2].

[1] Организован в соответствии с приказом Росстандарта от 21.08.2017 № 1759 «Об организации деятельности технического комитета по стандартизации «Стандарты финансовых операций».

[2] Утвержден и введен в действие приказом Росстандарта от 24.10.2024 № 1504-ст.

В целях разработки и внедрения безопасных программных продуктов при сохранении гарантированного и достаточного уровня защищенности прикладного программного обеспечения автоматизированных систем и приложений, используемых при осуществлении финансовых (в том числе банковских) операций, Банк России рекомендует использовать актуализированный документ.

Настоящее Информационное письмо Банка России подлежит размещению на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Заместитель Председателя
Банка России Г.А. Зубарев

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

ПРОФИЛЬ ЗАЩИТЫ
прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций

2025

Содержание

Перечень сокращений

АСБиФО – автоматизированная система банковских и финансовых операций

АС – автоматизированная система

БС – банковская система

ЗБ – задание по безопасности

ЗИ – защита информации

ИБ – информационная безопасность

ИС – информационная система

ИТ – информационная технология

ИФБО – интерфейс функциональной возможности безопасности объекта оценки

НСД – несанкционированный доступ

ОО – объект оценки

ОС – операционная система

ОУД – оценочный уровень доверия

ПЗ – профиль защиты

ПФБ – политика функции безопасности

ПО – программное обеспечение

ППО – прикладное программное обеспечение

РБПО – разработка безопасного программного обеспечения

СЗИ – средство защиты информации

СВТ – средство вычислительной техники

СМИБ – система менеджмента информационной безопасности

СОИБ – система обеспечения информационной безопасности

СПО – системное программное обеспечение

ТДБ – требования доверия к безопасности объекта оценки

УК – управление конфигурацией

ФБО – функциональные возможности безопасности объекта оценки

ФТБ – функциональные требования безопасности к объекту оценки

1. Общие положения

Настоящий документ разработан Банком России и предназначен для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций (далее – разработчик), заявителей на осуществление сертификации продукции (далее – заявители), а также для органов по сертификации, испытательных лабораторий и организаций, самостоятельно проводящих оценку соответствия (далее – оценщик), выполняющих работы по сертификации прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей.

Профиль защиты учитывает:

- положения национальных стандартов Российской Федерации:
  - ГОСТ Р ИСО/МЭК 15408-1-2012 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»;
  - ГОСТ Р ИСО/МЭК 15408-2-2013 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности»;
  - ГОСТ Р ИСО/МЭК 15408-3-2013 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки

безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»;

- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»;
- ГОСТ Р 59792-2021 "Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем";
- ГОСТ Р 57628-2017 "Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности";
- ГОСТ Р ИСО/МЭК 18045-2013 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»;
- ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»;

- требования нормативных актов и рекомендаций Банка России:
  - Рекомендаций в области стандартизации Банка России РС БР ИББС-2.6-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем»;
  - Положения Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»;
  - Положения Банка России от 30.01.2025 № 851-П «Об установлении обязательных для кредитных организаций требований к

обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»;

- Положения Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»;
- Положения Банка России от 25.07.2022 г. № 802-П "О требованиях к защите информации в платежной системе Банка России";
- Положения Банка России от 17.10.2022 г. № 808-П "О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона "О кредитных историях", при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства";
- Положения Банка России от 07.12.2023 г. №833-П “О требованиях к обеспечению защиты информации для участников платформы цифрового рубля”;
- иных нормативных актов Банка России, устанавливающих требования к обеспечению защиты информации для кредитных организаций и некредитных финансовых организаций.

2. Введение профиля защиты

Данный раздел содержит информацию общего характера. Подраздел «Справка профиля защиты» содержит идентификационные сведения о ПЗ, которые включают обозначение и описательную информацию, необходимую для идентификации ПЗ и ОО, к которому он относится. Подраздел «Аннотация объекта оценки» содержит краткое описание использования ОО и его основные характеристики безопасности.

2.1. Справка профиля защиты

Наименование ПЗ:	Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций.
Тип ПО:	Прикладное программное обеспечение автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций.
Версия ПЗ:	Версия 4.0.
Обозначение ПЗ:	ИТ. ПО АС ФО.ПЗ.
Идентификация ОО:	Прикладное программное обеспечение автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций.

Уровень доверия:	Оценочный уровень доверия 4 (ОУД4), *усиленный компонентами* *ADV_IMP.2 «Полное отображение представления реализации ФБО»,* *ALC_FLR.2 «Процедуры сообщений о недостатках»,* *AVA_VAN.5 «Усиленный методический анализ»,* *ACO_DEV.1 «Функциональное описание»,* *ACO_REL.1 «Базовая информация о зависимостях»,* *ACO_VUL.2 «Анализ уязвимостей композиции»,* *расширенный компонентами* *ADV_IMP_EXT.3 «Реализация ОО»,* *ADV_TDS_EXT.3 «Разработка, уточнение и анализ архитектуры программного обеспечения ОО»,* *AGD_OPE_EXT.1 «Правила кодирования»,* *ALC_DEL_EXT.1 «Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок»,* *ALC_DVS_EXT.1 «Моделирование угроз и разработка описания поверхности атаки»,* *ALC_DVS_EXT.2 «Обеспечение безопасности сборочной среды программного обеспечения»,* *ALC_DVS_EXT.3 «Управление доступом и контроль целостности кода при разработке программного обеспечения»,* *ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения»,* *ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки»,* *ALC_TAT_EXT.1 «Статический анализ исходного кода»,* *ALC_TAT_EXT.2 «Динамический анализ кода программы»,* *ATE_IND.EXT.1 «Нефункциональное тестирование»,*

	AVA_VAN_EXT.1 «Реагирование на информацию об уязвимостях», *AVA_CCA_EXT.1 «Анализ скрытых каналов»,* *AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность»*.
Идентификация:	Нормативные акты Банка России, устанавливающие требования к обеспечению защиты информации для кредитных организаций и некредитных финансовых организаций, требования к которым указаны в настоящем разделе.
Ключевые слова:	Программное обеспечение, автоматизированные системы и приложения кредитных организаций и некредитных финансовых организаций, ОУД4.

2.2. Термины и определения

В настоящем документе и при задании требований безопасности ОО используются следующие определения:

Администратор ППО	Субъект доступа из состава эксплуатационного персонала, уполномоченный выполнять некоторые действия по администрированию ППО (имеющий административные полномочия) в соответствии с установленной ролью и требуемыми привилегиями в прикладном программном обеспечении финансовой организации и обеспечивающих компонентах АС на выполнение этих действий.
Администратор безопасности	Субъект доступа, ответственный за защиту АС от несанкционированного доступа к информации, на которого возложены обязанности по мониторингу ИБ и контролю защитных мер, аудиту прав и контролю действий пользователей и эксплуатационного персонала.
Безопасный жизненный цикл разработки ПО (DevSecOps)	Термином DevSecOps обозначается цикл разработки программного обеспечения с непрерывной поставкой, в котором особое внимание уделяется вопросам обеспечения информационной безопасности.
Доверенный продукт ИТ	Продукт ИТ, отличный от ОО, для которого имеются свои функциональные требования, организационно скоординированные с ОО, и который, как предполагается, реализует свои функциональные требования корректно.
Задание по безопасности (ЗБ)	Зависимое от реализации изложение потребностей в безопасности для ППО и приложений финансовых организаций.

Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями действующего законодательства Российской Федерации или требованиями, устанавливаемыми собственником информации. При этом несанкционированное раскрытие, модификация или сокрытие такой информации может повлечь убытки собственника информации.
Команда безопасной разработки ПО (команда DevSecOps)	Команда людей, участвующих в реализации безопасного жизненного цикла ОО. Включает участников с необходимыми компетенциями, в том числе в области безопасности прикладного программного обеспечения и принципов безопасной разработки.
Композиционный анализ программного обеспечения (КАПО)	Вид работ, основанный на анализе сторонних компонентов ПО, определении особенностей их использования, наличии уязвимостей и/или иных недостатков компонентов, на основании фактов публикаций результатов тестирования этих компонентов.
Краткая спецификация ОО (КСО)	Описание в ЗБ того, как ОО удовлетворяет ФТБ.
Обеспечивающие компоненты АС	Компоненты обеспечивающей среды функционирования ППО АС и приложений финансовых организаций, а также всего аппаратного, программного и программно-аппаратного обеспечения, в том числе системное программное обеспечение, средства вычислительной техники, средства защиты информации.
Объект доступа	В настоящем документе под объектом доступа понимается ресурс доступа – объект, представляющий собой

	совокупность информации ППО АС и приложений финансовых организаций.
Объект оценки (ОО)	ППО АС и приложений финансовых организаций, предназначенных для осуществления финансовых операций, и поддерживающая его документация, выступающие продуктом для оценки. Совокупность программного, программно-аппаратного и/или аппаратного обеспечения, возможно, сопровождаемая руководствами.
Поверхность атаки	Совокупность ресурсов АС, которые напрямую или косвенно подвержены потенциальному риску атаки.
Пользователь ППО	Субъект доступа, в том числе клиент финансовой организации, осуществляющий доступ к объекту доступа с целью использования финансовых услуг, предоставляемых информационной инфраструктурой финансовой организации. Пользователь ППО не имеет административных полномочий.
Пользователь	Субъект доступа, которому в соответствии с ФТБ разрешено выполнять некоторые действия (операции) по администрированию ППО или обработке информации в ППО.
Права логического доступа	Набор действий, разрешенных для выполнения субъектом доступа над объектом (ресурсом) доступа с использованием соответствующей учетной записи.
Профиль защиты (ПЗ)	Независимое от реализации изложение потребностей в безопасности для ППО и приложений финансовых организаций.
Разработчик	Организация, выполняющая и ответственная за разработку ОО.

Роль	Заранее определенная совокупность функций и задач субъекта доступа, для выполнения которых необходим определенный набор прав логического доступа.
Субъект доступа	Работник финансовой организации или иное лицо, осуществляющее физический и (или) логический доступ, или программный сервис, осуществляющий логический доступ.
Требования доверия к безопасности (ТДБ)	Требования к обеспечению безопасности ОО: требования, обеспечивающие уверенность в том, что ППО АС и приложений финансовых организаций соответствует функциональным требованиям безопасности.
Финансовая организация	Кредитная организация и некредитная финансовая организация.
Функция обеспечения ИБ	Реализованная функциональная возможность одного или нескольких компонентов ППО АС и приложений финансовых организаций, связанная с обеспечением ИБ.
Функциональное требование безопасности (ФТБ)	Требование к осуществлению безопасности ОО: требования к функциям обеспечения информационной безопасности ППО АС и приложений финансовых организаций.
Функциональные возможности безопасности ОО (ФБО)	Совокупность функциональных возможностей всего аппаратного, программного и программно-аппаратного обеспечения ОО, которые необходимо использовать для корректной реализации ФТБ.
Эксплуатационный персонал	Субъект доступа, в том числе представитель подрядной организации,

	который решает задачи обеспечения эксплуатации и (или) администрирования объекта доступа, для которого необходимо осуществление логического доступа, включая задачи, связанные с эксплуатацией и администрированием технических мер защиты информации.

2.3. Аннотация объекта оценки

2.3.1. Использование и основные функциональные возможности безопасности ОО

Настоящий ПЗ определяет требования безопасности к ОО. На ОО обрабатывается защищаемая информация на участках, используемых для передачи и приема первичных документов (содержащихся в электронных сообщениях) к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»).

ОО представляет собой прикладное программное обеспечение, предоставляемое поставщиком или разработчиком, которое используется для предоставления клиентам финансовых организаций сервисов и доступа клиентам к услугам дистанционного обслуживания.

ОО размещается на технологических участках передачи и приема первичных документов (содержащихся в электронных сообщениях) к исполнению финансовой организацией с использованием сети «Интернет».

При этом ОО:

- устанавливается в изолированном сегменте сети, сопряженном с сетью «Интернет», на инфраструктуре финансовой организации, входит в состав автоматизированной системы финансовой организации и взаимодействует с обеспечивающими компонентами автоматизированных систем (фронт-офисное СПО);

- устанавливается на отдельном устройстве или компоненте инфраструктуры клиента финансовой организации, сопряженном с сетью «Интернет», в качестве прикладного программного обеспечения – приложения (клиентское ППО).

Функциональные требования безопасности (ФТБ), включенные в настоящий ПЗ, обеспечивают исключение возникновения типовых

недостатков при реализации требований к ППО АС и приложений финансовых организаций, создающих условия для возникновения недопустимых рисков при эксплуатации автоматизированных систем финансовой организации.

Состав ФТБ, включенных в настоящий ПЗ, обеспечивает следующие функциональные возможности ОО:

- защиту пользовательских данных (ограничение доступа к аппаратным ресурсам платформы, хранилищам защищаемой информации, сетевым коммуникациям);
- управление безопасностью (использование механизмов конфигурации, определение параметров конфигурации по умолчанию, назначение функций управления);
- защиту персональной идентификационной информации;
- защиту функций безопасности ОО (ограничение использования поддерживаемых сервисов, противодействие использованию уязвимостей безопасности, обеспечение целостности при установке и обновлении, ограничение использования сторонних библиотек);
- использование доверенного пути/канала передачи данных.

Функциональные требования безопасности для ОО выражены на основе компонентов требований из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» и специальных (расширенных) компонентов.

Требования доверия к безопасности ОО включают оценочный уровень доверия 4 (ОУД4) согласно ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3.

Компоненты доверия к безопасности», усиленный дополнительными компонентами из ГОСТ Р ИСО/МЭК 15408-3-2013, а также расширенный компонентами, определенными в явном виде. Компоненты требований доверия учитывают положения Рекомендаций в области стандартизации Банка России РС БР ИББС-2.6-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем».

2.3.2. Тип объекта оценки

Прикладное программное обеспечение автоматизированных систем и приложений финансовых организаций (ППО АС ПФО).

Совместимым ОО для настоящего ПЗ является ППО АС ПФО, предназначенное для функционирования на средствах вычислительной техники общего назначения (автоматизированные рабочие места, серверы), а также на мобильных устройствах (ноутбуки, смартфоны, планшеты, телефоны и иные).

2.3.3. Доступные аппаратные средства, программное обеспечение, программно-аппаратные средства, не входящие в ОО

При разработке заданий по безопасности ОО на основе настоящего ПЗ, аппаратные средства, программное обеспечение, программно-аппаратные средства, не входящие в ОО, не рассматриваются.

2.4. Соглашения

Комплекс национальных стандартов Российской Федерации ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» допускает выполнение определенных операций над компонентами требований безопасности. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор», «назначение» и «итерация».

Для удобства восприятия операции «уточнение», «выбор», «назначение» и «итерация» в тексте настоящего ПЗ выделены полужирным шрифтом.

Операция **«уточнение»** используется для добавления в компонент требований некоторых подробностей (деталей) и таким образом ограничивает диапазон возможностей по удовлетворению требований. Результат операции **«уточнение»** в настоящем ПЗ обозначается **полужирным текстом**.

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

Операция **«назначение»** используется для присвоения конкретного значения ранее не конкретизированному параметру в компоненте требований. Операция **«назначение»** обозначается заключением присвоенного значения параметра в квадратные скобки, [назначаемое (присвоенное) значение параметра].

Операция **«итерация»** используется для выражения двух или более требований безопасности на основе одного компонента требований безопасности; при этом осуществляются различные варианты выполнения других операций («уточнение», «выбор» и (или) «назначение») над этим компонентом.

В ПЗ используются компоненты требований безопасности, включающие

частично выполненные операции **«назначение», «выбор»** и предполагающие завершение операций в ЗБ. В данных компонентах незавершенная часть операции **«назначение»** обозначается как [**назначение**: *область предполагаемых значений*], часть операции **«выбор»** обозначается как [**выбор**: *область предполагаемых значений выбора*].

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

ПЗ содержит ряд компонентов функциональных требований безопасности с незавершенными операциями. Эти операции должны быть завершены в задании по безопасности для конкретной реализации ОО.

3. Утверждение о соответствии

3.1. Утверждение о соответствии ГОСТ Р ИСО/МЭК 15408

Настоящий ПЗ разработан с учетом положений национальных стандартов Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» и ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

ПЗ содержит расширенные требования безопасности, разработанные в соответствии с правилами, установленными комплексом национальных стандартов Российской Федерации ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

3.2. Утверждение о соответствии ГОСТ Р 56939-2024

Настоящий ПЗ (раздел 7.4) разработан с учетом положений национального стандарта Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» и является его расширением.

3.3. Утверждение о соответствии профилям защиты

Соответствие другим профилям защиты не требуется.

3.4. Утверждение о соответствии пакетам

Настоящий ПЗ соответствует пакету требований доверия: оценочный уровень доверия 4 (ОУД4), усиленный компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ALC_FLR.2 «Процедуры сообщений о недостатках», AVA_VAN.5 «Усиленный методический анализ»,

ACO_DEV.1 «Функциональное описание», ACO_REL.1 «Базовая информация о зависимостях», ACO_VUL.2 «Анализ уязвимостей композиции», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ADV_TDS_EXT.3 «Разработка, уточнение и анализ архитектуры программного обеспечения ОО», AGD_OPE_EXT.1 «Правила кодирования», ALC_DEL_EXT.1 «Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок», ALC_DVS_EXT.1 «Моделирование угроз и разработка описания поверхности атаки», ALC_DVS_EXT.2 «Обеспечение безопасности сборочной среды программного обеспечения», ALC_DVS_EXT.3 «Управление доступом и контроль целостности кода при разработке программного обеспечения», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», ALC_TAT_EXT.1 «Статический анализ исходного кода», ALC_TAT_EXT.2 «Динамический анализ кода программы», ATE_IND.EXT.1 «Нефункциональное тестирование», AVA_VAN_EXT.1 «Реагирование на информацию об уязвимостях», AVA_CCA_EXT.1 «Анализ скрытых каналов», и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность».

3.5. Обоснование соответствия

Функциональные требования и требования доверия к программному обеспечению автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций включены в настоящий ПЗ с учетом Рекомендаций в области стандартизации Банка России РС БР ИББС-2.6-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем» с учетом положений ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий, а также нормативных и

методических документов ФСТЭК России, определяющих требования к средствам защиты информации.

Требования к безопасной разработке автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций также включены в раздел 7.4 настоящего ПЗ с учетом положений национального стандарта Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

3.6. Изложение соответствия

При разработке ЗБ и (или) других ПЗ на основе настоящего ПЗ устанавливаются следующие типы соответствия: **«строгое соответствие»** – все требования настоящего ПЗ должны быть полностью удовлетворены в ЗБ, хотя при этом ЗБ может быть более широким, чем ПЗ.

Допустимой является реализация отдельных предположений, ФТБ, не влияющих на конечный уровень доверия, компенсационными и/или организационно-технологическими мерами при обязательном наличии достаточного обоснования, учитывающего технические ограничения и особенности компонент инфраструктуры и применяемых информационных технологий, а также риск-ориентированный подход организации при проведении оценки рисков нарушения информационной безопасности и особенности моделирования угроз и нарушителей.

4. Определение проблемы безопасности

Данный раздел содержит описание следующих аспектов решаемой с использованием ОО проблемы безопасности:

- угроз безопасности, которым должны противостоять ОО и среда функционирования ОО;
- политик безопасности, которые должен выполнять ОО;
- предположений безопасности (обязательных условий безопасного использования ОО).

4.1. Угрозы

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

Угроза-1

1. Аннотация угрозы – несанкционированный доступ к защищаемой информации ОО при наличии недостатков и уязвимостей информационной инфраструктуры на стороне финансовых организаций.

2. Источники угрозы – внешний или внутренний нарушитель.

3. Способ реализации угрозы – нарушитель получает доступ к программному обеспечению ОО. Осуществление компьютерной атаки, связанной с использованием вредоносного программного обеспечения, применительно к объектам информационной инфраструктуры участников информационного обмена. Нарушитель может участвовать в информационном обмене с программным обеспечением или изменять связи между программным обеспечением и другими конечными точками с целью несанкционированного доступа к информации, обрабатываемой ОО.

4. Используемые уязвимости – недостатки реализации механизмов защиты, недостатки механизмов разграничения доступа к ОО по каналам связи, наличие уязвимостей в ОО, использование устаревшего ПО,

использование ненадежных механизмов аутентификации и авторизации, нарушение логики работы ОО.

5. Вид информационных ресурсов, потенциально подверженных угрозе – электронные сообщения, криптографические ключи и информация, обрабатываемая и передаваемая между финансовыми организациями и клиентом.

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

7. Возможные последствия реализации угрозы – модификация ОО, вследствие повышения привилегий процессов, команд, пользователей, используемых в ОО, выполнение произвольного кода на удаленной системе, внедрение несанкционированных данных в систему, выполнение несанкционированных действий от имени законного пользователя, внедрение вредоносного ПО в скомпрометированную систему, нарушение целостности и конфиденциальности электронных сообщений.

Угроза-2

1. Аннотация угрозы – возможность перехвата информации, передаваемой между ОО и другими конечными точками.

2. Источники угрозы – внешний нарушитель.

3. Способ реализации угрозы – нарушитель имеет доступ к каналу связи или к узлу сетевой инфраструктуры. Нарушитель может перехватывать и получать доступ к данным, передаваемым между ОО и другими конечными точками, с последующей модификацией передаваемых данных или без таковой.

4. Используемые уязвимости – недостатки и уязвимости в платформе и механизмах обеспечения конфиденциальности и целостности информации, передаваемой между ОО и другими конечными точками.

5. Вид информационных ресурсов, потенциально подверженных угрозе – электронные сообщения, криптографические ключи и иная информация, обрабатываемые и передаваемые между финансовой организацией и клиентом.

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

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, передаваемой в сообщениях прикладного программного обеспечения, выполнение несанкционированных действий от имени законного пользователя, влекущих за собой незаконные финансовые операции.

Угроза-3

1. Аннотация угрозы – воздействие на ПО на стороне клиента.

2. Источники угрозы – внутренний и внешний нарушитель.

3. Способ реализации угрозы – нарушитель может действовать с использованием разрешенного ПО (в том числе сторонние компоненты, которые разработчик включил в код), функционирующего на той же вычислительной платформе, что и ОО. Осуществление компьютерной атаки, связанной с использованием вредоносного ПО, применительно к объектам информационной инфраструктуры участников информационного обмена.

4. Используемые уязвимости – недостатки в проектировании и в реализации ОО, заражение программного кода, в том числе сторонних компонент, недостатки в программном коде, связанные с ненадлежащим контролем вводимых данных, несовместимость ОО с другим ПО, несовместимость ОО с компонентами среды исполнения, небезопасное хранение данных, наследование уязвимостей и недекларированных возможностей при использовании сторонних компонент.

5. Вид информационных ресурсов, потенциально подверженных угрозе – электронные сообщения, криптографические ключи и информация, обрабатываемые ПО.

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

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, обрабатываемой в ПО, повышение привилегий скомпрометированного ОО, выполнение произвольного кода в локальной системе, внедрение несанкционированных данных в систему, выполнение несанкционированных действий от имени законного пользователя, внедрение вредоносного ПО в скомпрометированную систему, нарушение конфиденциальности и целостности электронных сообщений и информации, обрабатываемых ПО.

4.2. Политика безопасности

Политика безопасности-1

ОО должен осуществлять запись в журнал установленных событий безопасности и предоставлять возможность их просмотра уполномоченным пользователям. ОО должен исключать от записи в журнал защищаемую информацию, если иное не предусмотрено целями функционирования и техническими особенностями, а также ограничениями реализации АСБиФО.

Политика безопасности-2

ОО должен осуществлять:

- проверку корректности входных данных на соответствие синтактической и семантической норме при импорте данных пользователя из-за пределов ОО;

- проверку корректности на соответствие синтактической и семантической норме выходных данных при экспорте данных пользователя из ОО;
- контроль отсутствия защищаемой информации в сообщениях от ППО.

Политика безопасности-3

ОО должен, при наличии технической возможности и необходимости, предоставлять для уполномоченных субъектов доступа возможность возвратной операции, отмены последней операции или ряда операций, ограниченных некоторым пределом (например, периодом времени), и возврата к предшествующему известному состоянию, чтобы сохранить целостность данных пользователя.

Политика безопасности-4

ОО должен предоставить уполномоченным пользователям возможность верифицировать целостность данных ФБО путем самотестирования ФБО в части некоторых операций с известным результатом.

Политика безопасности-5

При наличии технической возможности и отсутствии технологических ограничений в ОО должны использоваться механизмы защиты, предоставляемые архитектурой процессора, ОС и средствами компиляции кода. При реализации ФБО должны использоваться только поддерживаемые поставщиком платформы сервисы и API.

Политика безопасности-6

В ОО должны использоваться только разрешенные сторонние библиотеки и сторонние компоненты, прошедшие проверку и анализ разработчиком ОО, включая композиционный анализ и проверку на отсутствие вредоносного ПО.

Политика безопасности-7

ОО должен реализовывать или использовать механизмы платформы для проверки целостности ОО при установке и обновлении, реализации соответствующих протоколов и форматов распространения обновлений, осуществления процедур деинсталляции ОО, проверки версии ОО.

Политика безопасности-8

ОО должен, при необходимости, осуществлять идентификацию, аутентификацию и авторизацию субъектов доступа.

4.3. Предположения безопасности

Предположение-1

ОО для своего выполнения полагается на доверенную вычислительную платформу или другие доверенные вычислительные мощности с возможностью распределенной обработки данных в режиме реального времени. Она включает базовую или облачную платформу и некоторую среду ее выполнения, предоставляемые ОО. Для осуществления ИБ применяются технологические меры защиты информации.

Предположение-2

Пользователь АСБиФО может быть преднамеренно небрежным или враждебным и может использовать ПО не в соответствии с применимыми правилами политики безопасности организации.

Предположение-3

Администратор АСБиФО не является невнимательным, преднамеренно небрежным или враждебным и управляет ОО в соответствии с применимыми правилами политики безопасности организации.

Предположение-4

Обеспечивается контроль установки и, при наличии технической возможности, контроль запуска компонентов программного обеспечения автоматизированных банковских систем (автоматизированных систем) финансовых организаций.

Предположение-5

В АСБиФО осуществляется защита от выполнения произвольного машинного кода.

Предположение-6

Осуществляется управление физическим доступом к элементам инфраструктуры АСБиФО.

Предположение-7

В документации должен быть отражен запрет на использование предсказуемых идентификаторов (например, производных от имени и фамилии пользователя, совпадающих с идентификаторами в адресах электронной почты, порядковых номеров, формирование идентификаторов по единому алгоритму) или отражен механизм защиты от перебора идентификаторов (например, временные задержки или captcha после определенного количества неуспешных попыток ввода), за исключением случаев, в которых подобные идентификаторы используются в качестве аналога собственноручной подписи.

Пароли пользователей хранятся с использованием необратимых преобразований. Запрещено использовать предсказуемые алгоритмы формирования однократных паролей. Должна осуществляться проверка соответствия однократного пароля и операции.

Предположение-8

Права на восстановление или смену необратимо утраченных аутентификационных данных предоставлены:

- администраторам безопасности АСБиФО;
- администраторам АСБиФО с обязательным контролем со стороны администратора безопасности АСБиФО;
- иным ответственным ролям эксплуатационного персонала по согласованию с администратором безопасности АСБиФО.

Предположение-9

В АСБиФО присутствуют и используются средства синхронизации времени.

Предположение-10

В АСБиФО имеются средства регистрации событий и просмотра журналов регистрации событий безопасности. При этом, при наличии такой возможности и целесообразности, обеспечивается:

- регистрация отдельных типов событий, существенных для расследования инцидентов, в том числе:
  - создание новых учетных записей и изменение прав доступа учетных записей,
  - неуспешные операции (например, ошибки аутентификации, недостаточные права доступа при выполнении операций, недоступность интерфейсов составных частей АСБиФО),

  - срабатывание функций безопасности, направленных на противодействие компьютерным атакам (например, автоматическое блокирование учетных записей, автоматическое завершение сессий, поступление некорректных исходных данных на внешние интерфейсы АСБиФО),
  - выполнение операций, предусмотренных моделью угроз в качестве составной части реализации угрозы;
- регистрация информации о проблемах и инцидентах ИБ, возникших при использовании клиентом компонентов АСБиФО и приложений;
- наличие в данных журналов регистрации событий существенных сведений о регистрируемых событиях, позволяющих установить обстоятельства наступления события;
- обеспечение конфиденциальности данных в журналах при регистрации в них событий с использованием защищаемой информации (пароли пользователей, данные платежных карт и т.п.);
- регистрация событий безопасности недоступными нарушителю составными частями АСБиФО и приложений;
- хранимые журналы регистрации событий защищены от НСД;
- невозможность изменения пользователями параметров регистрации событий;
- наличие встроенных или специализированных средств анализа журналов регистрации событий, в том числе поиска событий по заданным критериям (по имени и идентификатору пользователя, дате, времени или, в случае необходимости, другим специально определенным критериям);
- наличие механизмов оперативного уведомления администраторов ИБ АСБиФО о событиях, имеющих признаки инцидента безопасности. В

финансовой организации определены признаки инцидентов безопасности, способы уведомления о них администраторов ИБ АСБиФО и порядок реагирования на них.

Предположение-11

В АСБиФО и приложениях имеется возможность защиты от несанкционированного доступа к разделяемым ресурсам ОС (например, к разделяемой памяти, именованным каналам, отображаемым в памяти файлам). Обеспечивается корректное использование средств синхронизации доступа к разделяемым ресурсам ОС (например, критических секций, семафоров).

Предположение-12

При использовании в составе АСБиФО СУБД обеспечивается:

- недоступность протоколов взаимодействия с СУБД, использование которых не предусмотрено проектной документацией;
- невозможность доступа составных частей АСБиФО и приложений к функциям СУБД без аутентификации;
- отсутствие у администраторов СУБД учетных записей ОС с правами, не являющимися безусловно необходимыми для обслуживания СУБД;
- отсутствие у технологических учетных записей, используемых составными частями АСБиФО и приложений для доступа к СУБД, прав, не являющихся безусловно необходимыми для выполнения предусмотренных документацией операций;
- обособление СУБД от других составных частей АСБиФО и приложений;
- при наличии такой возможности, использование ограничения доступа к СУБД, в том числе на сетевом уровне;

- невозможность доступа пользователей, не являющихся администраторами, к таблицам и конфигурационным настройкам, не предусмотренным предоставленными полномочиями;
- отсутствие размещения данных нескольких приложений в одном разделе СУБД в случае, когда такое размещение не предусмотрено явно проектной документацией.

Предположение-13

В операционной системе АСБиФО обеспечивается:

- запрет использования незащищенных и слабозащищенных протоколов удаленного доступа к ОС (например, TELNET, PPTP) или с применением дополнительных мер защиты;
- невозможность доступа к настройке параметров ОС, заданий, журналу событий, системным файлам у пользователей, не являющихся администраторами ОС;
- отсутствие индивидуальных прав доступа к объектам ОС у отдельных пользователей (права пользователей задаются только в составе соответствующих групп) либо проведение процедур регулярного контроля прав пользователей в ОС, где группы пользователей не предусмотрены;
- невозможность интерактивного входа в систему для системных учетных записей, использующихся приложениями и сервисами, если подобное не предусмотрено техническими особенностями и характеристиками;
- отсутствие у пользователей, не являющихся администраторами ОС, прав на чтение и (или) модификацию файлов в домашних каталогах других пользователей;

- наличие минимально необходимого количества свободного места на дисках АСБиФО контролируется с использованием автоматизированных средств постоянно либо вручную администраторами АСБиФО с заданной периодичностью;
- соответствие настроек ОС рекомендациям разработчика по ее безопасной настройке;
- отсутствие в ОС серверных компонентов АСБиФО программного обеспечения, не предусмотренного эксплуатационной документацией, или наличие утвержденного разрешенного списка компонентов;
- отсутствие возможности доступа к ОС без аутентификации через вспомогательные и (или) редко используемые интерфейсы;
- аутентификация пользователя при доступе к параметрам BIOS, параметрам загрузчика ядра ОС, входе в режим восстановления системы;
- активация в настройках ядра ОС механизмов настройки ядра, предотвращающих выполнение кода в области данных и стека;
- активация в настройках ядра ОС функции очистки файла/раздела подкачки виртуальной памяти;
- осуществление контроля и обеспечение конфиденциальности хранения защищаемой информации в оперативной памяти;
- отключение в настройках ОС возможности выгрузки образов областей памяти (дампов) на диск пользователями вручную либо автоматически при возникновении ошибок;
- отключение в настройках ОС возможности гибернации (перехода в ждущий режим);
- отсутствие возможности отключения используемых средств защиты сторонних производителей;

- задействование программного или программно-аппаратного средства контроля и фильтрации сетевого трафика в ОС, наличие в настройках правил фильтрации, блокирующих взаимодействие, не предусмотренное эксплуатационной документацией АСБиФО, либо использование межсетевого экранирования на уровне сегмента.

Предположение-14

При использовании в АСБиФО технологий виртуализации обеспечивается:

- отсутствие доступа к данным виртуальных машин (например, настройкам виртуального аппаратного обеспечения, образам дисков) пользователей, не являющихся администраторами сервера виртуализации;
- запрет доступа виртуальным машинам к разделяемым ресурсам ОС сервера виртуализации в случаях, когда такой доступ не предусмотрен явно эксплуатационной документацией АСБиФО;
- наличие средств мониторинга объема свободных ресурсов сервера виртуализации;
- ограничение удаленного доступа администраторов сервера виртуализации путем ограничения IP-адресов, с которых разрешен доступ, и сетевого интерфейса для доступа администраторов;
- отсутствие использования для удаленного администрирования сервера виртуализации сетевых интерфейсов, используемых виртуальными машинами;
- отсутствие хранения журналов регистрации событий средств виртуализации в каталогах, доступных на чтение и (или) запись виртуальным машинам;

- непосредственный доступ к виртуальным машинам, к физическим дискам и логическим томам памяти сервера виртуализации должен контролироваться СЗИ;
- отсутствие использования в графическом интерфейсе сервера виртуализации расширенных механизмов обмена данными между виртуальными машинами и сервером виртуализации;
- отсутствие использования расширенных механизмов обмена данными между виртуальными машинами, если иное не предусмотрено эксплуатационной документацией;
- невозможность изменения пользователем режима загрузки виртуальной машины.

Предположение-15

На этапе снятия с эксплуатации осуществляется контроль соблюдения правил и процедур обеспечения информационной безопасности. В случае необходимости дальнейшего использования ОО осуществляется архивирование информации, содержащейся в ОО.

Предположение-16

В АСБиФО присутствуют и используются:

- механизмы защиты от несанкционированного доступа к настройкам приложения;
- средства контроля целостности программного кода и корректности настроек составных частей АСБиФО;
- механизмы, блокирующие отключение отдельных функций безопасности при переводе АСБиФО в аварийный режим функционирования, при наличии такого специального режима в АСБиФО;

- механизмы генерации диагностической информации при переводе АСБиФО в аварийный режим функционирования, при наличии такого специального режима в АСБиФО;
- механизмы установления защищенного соединения и/или взаимной аутентификации серверной и клиентской стороны.

Предположение-17

Предполагается, что на этапах приемки и ввода в действие в части обеспечения ИБ ставятся задачи:

- контроля развертывания компонентов АСБиФО в информационной инфраструктуре организации БС;
- проведения опытной эксплуатации;
- устранения недостатков в реализации требований частного технического задания на подсистему ИБ АСБиФО;
- проведения приемочных испытаний.

Предполагается, что для контроля развертывания компонентов АСБиФО в промышленной среде:

- обеспечивается контроль корректности версий и целостности компонентов АСБиФО при передаче из среды разработки и тестирования в промышленную среду;
- обеспечивается контроль выполнения требований проектной и эксплуатационной документации в части размещения и установления параметров настройки технических защитных мер, реализации организационных защитных мер, определения и назначения ролей.

Предполагается, что опытная (опытно-промышленная) эксплуатация АСБиФО предусматривает проверку функциональных и эксплуатационных характеристик, обучение пользователей и эксплуатационного персонала с учетом задач, сценариев и порядка проведения, определенного в документе, содержащем программу проведения опытной эксплуатации.

Предполагается, что в рамках проведения опытной эксплуатации в части обеспечения ИБ проводится проверка корректности функционирования подсистемы ИБ АСБиФО в промышленной либо приближенной к промышленной среде, а также проверка возможности реализации на этапе эксплуатации положений проектной и эксплуатационной документации в части контроля эксплуатации технических защитных мер, включая правила их обновления, управления и контроля параметров их настройки.

Предположение-18

Шифрование применяется с использованием стойких криптографических алгоритмов. Все учетные данные для проверки подлинности хранятся и передаются только в защищенном виде с использованием стойких криптографических алгоритмов или по зашифрованному каналу передачи данных.

Предположение – 19

Используемые сторонние компоненты разрабатываются с учётом признанных стандартов безопасного кодирования и поставляются в формате, достаточном для приёмочного контроля со стороны разработчика ОО.

Предположение – 20

Инфраструктура среды разработки коммерчески распространяемого программного обеспечения сторонних поставщиков ПО размещена на территории РФ.

Предположение – 21

ПО поставляется пользователям вместе с эксплуатационной документацией, содержащей описание и характеристики ПО, в том числе с точки зрения информационной безопасности.

5. Цели безопасности

5.1. Цели безопасности для объекта оценки

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности ОО-1

ОО должен обеспечивать контроль целостности своей установки и пакетов обновлений, а также эффективно использовать способы предотвращения нарушений целостности, предоставляемые средой выполнения, эффективно использовать документированные и поддерживаемые возможности, предоставляемые средой выполнения. Обеспечивать контроль доступа (ролевой, дискреционный, мандатный) к объектам, находящимся под контролем ПО.

Цель безопасности ОО-2

ОО должен предоставлять пользователям и платформе функционирования непротиворечивые интерфейсы для управления и конфигурирования, связанные с обеспечением безопасности и обслуживанием.

Цель безопасности ОО-3

ОО должен предоставлять пользователю возможность управлять уровнем раскрытия любой персональной идентификационной информации.

Цель безопасности ОО-4

ОО должен использовать доверенный канал для передачи защищаемой информации и обеспечивать защиту хранимой, обрабатываемой и передаваемой к компонентам ППО защищаемой информации.

Цель безопасности ОО-5

ОО должен обеспечить регистрацию и учет выполнения функций безопасности ОО и предотвращать использование аппаратных и программных ресурсов платформы, доступ к которым не предусмотрен для ОО.

Цель безопасности ОО-6

ОО должен при необходимости обеспечивать идентификацию, аутентификацию и авторизацию пользователей ППО.

5.2. Цели безопасности для среды функционирования

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

Цель безопасности среды-1

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-1**, так как обеспечивает применение ОО на доверенной совместимой вычислительной платформе, которая включает как основную ОС, так и любую другую отдельную среду выполнения, под управлением которой функционирует ОО.

Цель безопасности среды-2

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-4**, так как обеспечивает контроль установки и, при наличии технической возможности, контроль запуска компонентов программного обеспечения автоматизированных банковских систем (автоматизированных систем) финансовых организаций.

Цель безопасности среды-3

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-5**, так как обеспечивает защиту от выполнения произвольного машинного кода.

Цель безопасности среды-4

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-7**, так как обеспечивает наличие в документации запрета на использование предсказуемых идентификаторов или отражения механизма защиты от перебора идентификаторов, за исключением случаев использования идентификаторов в качестве аналога собственноручной подписи.

Цель безопасности среды-5

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-8**, так как обеспечивает предоставление прав на восстановление или смену необратимо утраченных аутентификационных данных только уполномоченным персоналом.

Цель безопасности среды-6

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-9**, так как обеспечивает надлежащий источник меток времени и синхронизацию по времени между компонентами ОО, а также между ОО и средой его функционирования.

Цель безопасности среды-7

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-10**, так как обеспечивает в ППО наличие средств регистрации событий и просмотра журналов регистрации событий безопасности, обеспечивающих надлежащий учет и представление событий безопасности и сопровождающей их информации.

Цель безопасности среды-8

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности

Предположение-11, так как обеспечивает в ППО защиту от несанкционированного доступа к разделяемым ресурсам операционной системы и корректное использование средств синхронизации доступа к разделяемым ресурсам операционной системы.

Цель безопасности среды-9

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-21**, так как обеспечивает в ППО надлежащее соблюдение условий безопасного использования сторонних программных продуктов.

Цель безопасности среды-10

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-13** так как обеспечивает настройку операционной системы, применяемой в ППО, в соответствии с политикой безопасности организации и требованиями к параметрам конфигурации механизмов безопасности, определённым в эксплуатационной документации.

Цель безопасности среды-11

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположений безопасности **Предположение-12**, **Предположение-14**, **Предположение-16** и **Предположение-17**, так как обеспечивает в ППО надлежащее соблюдение условий безопасного использования информационных технологий, включая СУБД и технологии виртуализации.

Цель безопасности среды-12

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-18**, так как обеспечивает хранение учетных данных для проверки подлинности только в защищенном виде, а также их передачу с

использованием стойких криптографических алгоритмов или по зашифрованному каналу передачи данных.

Цель безопасности среды-13

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположений безопасности **Предположение-19** и **Предположение-20**, так как обеспечивает безопасность заимствованного ПО сторонних поставщиков.

Цель безопасности среды-14

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-2**, так как обеспечивает безопасность в случае использования ОО не в соответствии с применимыми правилами политики безопасности организации.

Цель безопасности среды-15

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-3**, так как обеспечивает функциональное тестирование ОО.

Цель безопасности среды-16

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-6**, так как обеспечивает защиту от осуществления действий, направленных на нарушение физической целостности СВТ.

Цель безопасности среды-17

Достижение этой цели безопасности для среды функционирования необходимо в связи с реализацией предположения безопасности **Предположение-15**, так как обеспечивает безопасность среды на этапе снятия с эксплуатации ОО.

5.3. Обоснование целей безопасности

В таблице 5.3.1 приведено отображение целей безопасности для среды функционирования на предположения безопасности.

Таблица 5.3.1 - Отображение целей безопасности для среды функционирования на предположения безопасности

	Цель безопасности среды 1	**Цель безопасности среды 2**	**Цель безопасности среды 3**	**Цель безопасности среды 4**	**Цель безопасности среды 5**	**Цель безопасности среды 6**	**Цель безопасности среды 7**	**Цель безопасности среды 8**	**Цель безопасности среды 9**	**Цель безопасности среды 10**	**Цель безопасности среды 11**	**Цель безопасности среды 12**	**Цель безопасности среды 13**	**Цель безопасности среды 14**	**Цель безопасности среды 15**	**Цель безопасности среды 16**	**Цель безопасности среды 17**
Предположение 1	+																
Предположение 2														+			
Предположение 3															+		
Предположение 4		+															
Предположение 5			+														
Предположение 6																+	
Предположение 7				+													
Предположение 8					+												
Предположение 9						+											
Предположение 10							+										
Предположение 11								+									
Предположение 12											+						
Предположение 13										+							
Предположение 14											+						
Предположение 15																	+
Предположение 16											+						
Предположение 17											+						
Предположение 18												+					
Предположение 19													+				
Предположение 20													+				
Предположение 21									+								

Цель безопасности-1

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-3** и реализации политик безопасности **Политика безопасности-3, Политика безопасности-5, Политика безопасности-6,**

Политика безопасности-7, так как обеспечивает использование разрешенных механизмов безопасности среды функционирования.

Цель безопасности-2

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1, Угроза-3** и реализации политики безопасности **Политика безопасности-4,** так как обеспечивает использование корректных интерфейсов управления и конфигурирования ОО.

Цель безопасности-3

Достижение этой цели безопасности необходимо для противостояния угрозе **Угроза-1** и реализации политики безопасности **Политика безопасности-2,** так как обеспечивает защиту персональной идентификационной информации.

Цель безопасности-4

Достижение этой цели безопасности необходимо для противостояния угрозам **Угроза-1**, **Угроза-2** и реализации политики безопасности **Политика безопасности-2,** так как обеспечивает использование надежных каналов передачи данных.

Цель безопасности-5

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-1,** так как обеспечивает регистрацию событий безопасности.

Цель безопасности-6

Достижение этой цели безопасности необходимо для реализации политики безопасности **Политика безопасности-8,** так как обеспечивает управление учетными записями пользователя.

В таблице 5.3.2 приведено отображение целей безопасности для ОО на угрозы и политику безопасности.

Таблица 5.3.2 – Отображение целей безопасности для ОО на угрозы и политику безопасности

	Цель безопасности ОО-1	Цель безопасности ОО-2	Цель безопасности ОО-3	Цель безопасности ОО-4	Цель безопасности ОО-5	Цель безопасности ОО-6
Угроза - 1		+	+	+		
Угроза - 2				+		
Угроза - 3	+	+				
Политика безопасности-1					+	
Политика безопасности-2			+	+		
Политика безопасности-3	+					
Политика безопасности-4		+				
Политика безопасности-5	+					
Политика безопасности-6	+					
Политика безопасности-7	+					
Политика безопасности-8						+

6. Определение расширенных компонентов

В данном разделе представлены расширенные компоненты ПЗ.

6.1. Определение расширенных компонентов функциональных требований безопасности ОО

Для ОО определены следующие компоненты функциональных требований безопасности, сформулированные в явном виде:

FAU_GEN_EXT.1 «Ассоциация защищаемой информации»

FDP_DAR_EXT.1 «Шифрование защищаемой информации приложения»,

FIA_IWS_EXT.1 «Идентификация сессий веб-приложений»,

FMT_CFG_EXT.1 «Конфигурация безопасности по умолчанию»,

FMT_MEC_EXT.1 «Поддерживаемый механизм конфигурации»,

FPR_ANO_EXT.1 «Согласие пользователей на обработку персональных данных (идентификационной информации)»,

FPT_AEX_EXT.1 «Противодействие использованию уязвимостей безопасности»,

FPT_API_EXT.1 «Использование поддерживаемых сервисов и прикладных программных интерфейсов»,

FPT_LIB_EXT.1 «Использование сторонних библиотек»,

FPT_TUD_EXT.1 «Целостность при установке и обновлении»,

FTP_DIT_EXT.1 «Защита данных при передаче»,

- в стиле компонентов из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» (расширенные (специальные) компоненты).

Компоненты функциональных требований безопасности, сформулированные в явном виде, представлены в приложении А к настоящему ПЗ.

6.2. Определение расширенных компонентов требований доверия к безопасности ОО

Для ОО определены следующие расширенные (специальные) компоненты требований доверия к безопасности:

ADV_IMP_EXT.3 «Реализация ОО»,

ADV_TDS_EXT.3 «Разработка, уточнение и анализ архитектуры программного обеспечения ОО»,

AGD_OPE_EXT.1 «Правила кодирования»,

ALC_DEL_EXT.1 «Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок»,

ALC_DVS_EXT.1 «Моделирование угроз и разработка описания поверхности атаки»,

ALC_DVS_EXT.2 «Обеспечение безопасности сборочной среды программного обеспечения»,

ALC_DVS_EXT.3 «Управление доступом и контроль целостности кода при разработке программного обеспечения»,

ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения ОО»,

ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки»,

ALC_TAT_EXT.1 «Статический анализ исходного кода»,

ALC_TAT_EXT.2 «Динамический анализ кода программы»,

ATE_IND_EXT.1 «Нефункциональное тестирование»,

AVA_VAN_EXT.1 «Реагирование на информацию об уязвимостях»,

AVA_CCA_EXT.1 «Анализ скрытых каналов»,

AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность»,

сформулированные в явном виде в стиле компонентов из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» с учетом положений ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Компоненты требований доверия к безопасности, сформулированные в явном виде, представлены в приложении Б к настоящему ПЗ.

7. 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 с учетом положений ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». 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 ОУД4, усиленного компонентами ADV_IMP.2 «Полное отображение представления реализации ФБО», ALC_FLR.2 «Процедуры сообщений о недостатках», AVA_VAN.5 «Усиленный методический анализ», ACO_DEV.1 «Функциональное описание», ACO_REL.1 «Базовая информация о зависимостях», ACO_VUL.2 «Анализ уязвимостей композиции», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность» и AVA_CCA_EXT.1 «Анализ скрытых каналов», AGD_OPE_EXT.1 «Правила кодирования», ALC_DEL_EXT.1 «Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок», ALC_DVS_EXT.1 «Моделирование угроз и разработка описания поверхности атаки», ALC_DVS_EXT.2 «Обеспечение безопасности сборочной среды программного обеспечения», ALC_DVS_EXT.3 «Управление доступом и контроль целостности кода при разработке программного обеспечения», ALC_TAT_EXT.1 «Статический анализ исходного кода», ALC_TAT_EXT.2 «Динамический анализ кода программы», ATE_IND.EXT.1 «Нефункциональное тестирование», ADV_TDS_EXT.3 «Разработка, уточнение и анализ архитектуры

программного обеспечения ОО», AVA_VAN_EXT.1 «Реагирование на информацию об уязвимостях».

7.1. Функциональные требования безопасности

Функциональные компоненты из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности», на которых основаны ФТБ ОО приведены в таблице 7.1, а компоненты сформулированные в явном виде расширенных (специальных) требований приведены в таблице 7.2.

Таблица 7.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	**Название компонента требований**
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.4	Предотвращение потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_ETC.1	Экспорт данных пользователя без атрибутов безопасности
FDP_IFC.1	Ограниченное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FDP_ITC.2	Импорт данных пользователя с атрибутами безопасности

Идентификатор компонента требований	Название компонента требований
FDP_RIP.2	Полная защита остаточной информации
FDP_ROL.1	Базовый откат
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов
FIA_SOS.2	Генерация секретов ФБО
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.4	Механизмы одноразовой аутентификации
FIA_UAU.5	Сочетание механизмов аутентификации
FIA_UAU.6	Повторная аутентификация
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.1	Выбор момента идентификации
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности
FPT_STM.1	Надежные метки времени
FPT_TDC.1	Базовая согласованность данных ФБО между ФБО
FPT_TST.1	Тестирование функциональных возможностей безопасности
FTA_MCS.1	Базовое ограничение на параллельные сеансы
FTP_ITC.1	Доверенный канал передачи между ФБО

Таблица 7.2 – Функциональные компоненты, сформулированные в явном виде расширенных (специальных) требований в Приложении А

Идентификатор компонента требований	Название компонента требований
FAU_GEN_EXT.1	Ассоциация защищаемой информации
FDP_DAR_EXT.1	Шифрование защищаемой информации приложения
FIA_IWS_EXT.1	Идентификация сессий веб-приложений
FMT_CFG_EXT.1	Конфигурация безопасности по умолчанию
FMT_MEC_EXT.1	Поддерживаемый механизм конфигурации
FPR_ANO_EXT.1	Согласие пользователей на обработку персональных данных (идентификационной информации)
FPT_AEX_EXT.1	Противодействие использованию уязвимостей безопасности
FPT_API_EXT.1	Использование поддерживаемых сервисов и прикладных программных интерфейсов
FPT_LIB_EXT.1	Использование сторонних библиотек
FPT_TUD_EXT.1	Целостность при установке и обновлении
FTP_DIT_EXT.1	Защита данных при передаче

7.1.1. 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) создание новых учетных записей и изменение прав доступа учетных записей;

в) неуспешные операции (например, ошибки аутентификации, недостаточные права доступа при выполнении операций, недоступность интерфейсов ОО);

г) срабатывание функций безопасности, направленных на противодействие компьютерным атакам (например, автоматическое блокирование учетных записей, автоматическое завершение сессий, поступление некорректных исходных данных на внешние интерфейсы ОО);

д) выполнение операций, предусмотренных моделью угроз в качестве составной части реализации угрозы;

е) все события, потенциально подвергаемые аудиту, на *детализированном* уровне аудита;

ж) события, приведенные в таблице 7.1.1;

з) [**назначение:** другие специально определенные события, потенциально подвергаемые аудиту].

и) все сеансы персонального доступа пользователей к защищаемой информации;

к) все действия, совершенные любым лицом с привилегиями суперпользователя (root) или администратора;

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 (если применимо) и результат события (успешный или неуспешный);

б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ/ЗБ, [**назначение**: другая относящаяся к аудиту информация].

Таблица 7.1.1– События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FIA_AFL.1 FIA_ATD.1 FIA_IWS_EXT.1 FIA_SOS.1 FIA_SOS.2 FIA_UAU.2 FIA_UAU.4 FIA_UAU.5 FIA_UAU.6FIA_UAU.7 FIA_UID.1	Запись аудита для событий, связанных с идентификацией и аутентификацией	Регистрируются успешные и неуспешные события, связанные с процессом идентификации и аутентификации
FDP_ACC.1 FDP_ACF.1 FDP_ETC.1 FDP_ITC.2 FDP_RIP.2 FDP_ROL.1 FDP_DAR_EXT.1 FTP_DIT_EXT.1	Запись аудита для событий, связанных с управлением доступом.	Регистрируются успешные и неуспешные события, связанные с процессами авторизации, правами доступа, управления потоками информации при импорте/ экспорте, защиты данных
FMT_MSA.1 FMT_MSA.3 FMT_MEC_EXT.1 FMT_CFG_EXT.1	Запись аудита для событий, связанных с управлением безопасности	Регистрируются успешные и неуспешные события, связанные с администрированием функций безопасности, настройкой параметров и конфигураций безопасности
FPT_AEX_EXT.1	Запись аудита для событий, связанных с противодействием компьютерным атакам	Например, автоматическое блокирование учетных записей, автоматическое

Компонент	Событие	Детализация
		завершение сессий, поступление некорректных исходных данных на внешние интерфейсы ППО
FPT_TST.1	Запись аудита для событий, связанных с выполнением и результатами самотестирования ФБО	
FPT_TUD_EXT.1	Запись аудита для событий, связанных с контролем целостности при установке и обновлении	
FTA_MCS.1	Запись аудита для событий, связанных с фиксацией числа параллельных сеансов пользователя, а также атрибутов безопасности этого пользователя	
FTP_DIT_EXT.1	Запись аудита для событий, связанных с нарушением конфиденциальности данных при передаче	

Зависимости: FPT_STM.1 Надежные метки времени.

Замечания по применению:

Записи аудита, генерируемые для событий безопасности, представляются на детализированном уровне, т. е. содержат информацию о любых изменениях конфигурации механизмов безопасности, включая параметры конфигурации до и после изменения.

Возможно использование нескольких уровней аудита, начиная от минимального, используемого в штатном режиме, заканчивая расширенным, предназначенным для выявления причин неисправностей. Переключение режима аудита не должно требовать перезапуска системы. Разработчик должен обеспечить регистрацию события переключения режима аудита в

записях аудита. Рекомендуется реализовать механизм очистки журналов аудита от защищаемой информации.

Производитель должен установить следующие требования к пользователю по эксплуатации:

FAU_GEN_EXT.1 Ассоциация защищаемой информации

FAU_GEN_EXT.1.1 ФБО не должны регистрировать в записях аудита защищаемую информацию, если иное не предусмотрено целями функционирования и техническими особенностями, а также ограничениями реализации АСБиФО: [выбор:

пароли пользователей;

полные номера платежных карт и критичные авторизационные данные;

закрытые криптографические ключи;

[**назначение**: *другая защищаемая информация*]

].

Зависимости: отсутствуют.

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 Для аудита событий, являющихся результатом действий идентифицированных пользователей, ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.

Зависимости: FAU_GEN.1 Генерация данных аудита

FIA_UID.1 Выбор момента идентификации

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.

FAU_SAR.2 Ограниченный просмотр аудита

FAU_SAR.2.1 ФБО должны запретить всем пользователям доступ к чтению записей аудита, за исключением пользователей, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_STG.1 Защищенное хранение журнала аудита

FAU_STG.1.1 ФБО должны защищать хранимые записи аудита в журнале аудита от несанкционированного удаления.

FAU_STG.1.2 ФБО должны быть способны [**выбор**, (выбрать одно из):

предотвращать;

выявлять

] несанкционированную модификацию хранимых записей аудита в журнале аудита.

Зависимости: FAU_GEN.1 Генерация данных аудита.

FAU_STG.3 Действия в случае возможной потери данных аудита

FAU_STG.3.1 ФБО должны выполнить [**назначение**: *действия, которые нужно предпринять в случае возможного сбоя хранения*

журнала аудита], если журнал аудита превышает [**назначение**: *принятое ограничение*].

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита.

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны [**выбор** (выбрать одно из):

игнорировать события, подвергающиеся аудиту;

записывать поверх самых старых хранимых записей аудита

] и [**назначение**: *другие действия, которые нужно предпринять в случае возможного сбоя хранения журнала аудита*] при переполнении журнала аудита.

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита.

7.1.2. Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять ПФБ [**выбор:**

управление доступом отсутствует;

дискреционное управление доступом;

ролевое управление доступом;

мандатное управление доступом

] для [**назначение**: *список субъектов, объектов и операций субъектов на объектах, на которые распространяется ПФБ*].

Зависимости: FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику управления доступом, определенную в FDP_ACC.1.1] к объектам, основываясь на [**назначение**: *список субъектов и объектов, находящихся под управлением указанной ПФБ, и для каждого из них — относящиеся к данной ПФБ атрибуты безопасности или именованные группы атрибутов безопасности*].

FDP_ACF.1.2 ФБО должны осуществлять следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: [**назначение**: *правила управления доступом управляемых субъектов к управляемым объектам с использованием управляемых операций на них*].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах: [**назначение**: *правила, основанные на атрибутах безопасности, которые явно разрешают доступ субъектов к объектам*].

FDP_ACF.1.4 ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах: [**назначение**: *правила, основанные на атрибутах безопасности, которые явно запрещают доступ субъектов к объектам*].

Зависимости: FDP_ACC.1 Ограниченное управление доступом

FMT_MSA.3 Инициализация статических атрибутов

Замечания по применению:

В качестве объектов доступа ПФБ следует в том числе рассматривать:

- сетевые соединения;
- устройства ввода-вывода информации;
- съемные носители информации;
- службы определения местоположения;
- хранилища защищаемой информации;
- другие аппаратные и программные ресурсы.

FDP_DAR_EXT.1 Шифрование защищаемой информации ОО

FDP_DAR_EXT.1.1 ФБО должны [**выбор**:

не хранить любую защищаемую информацию;

усилить предоставленную платформой функциональность для шифрования защищаемой информации;

реализовать функциональность для шифрования защищаемой информации;

определить необходимость шифрования защищаемой информации в высокопроизводительных системах с высокой критичностью по времени передачи данных;

использовать альтернативные методы зашиты защищаемой информации;

] в энергонезависимой памяти.

Зависимости: отсутствуют.

FDP_ETC.1 Экспорт данных пользователя без атрибутов безопасности

FDP_ETC.1.1 ФБО должны осуществлять [

проверку корректности выходных данных, в том числе:

- отсутствие возможности формирования серверными компонентами ППО исполняемых файлов и сценариев, на основе задаваемых пользователями исходных данных;
- отсутствие возможности включения в выходные данные, передаваемые между составными частями ППО, фрагментов, не соответствующих спецификациям протоколов взаимодействия и (или) используемых для эксплуатации типовых уязвимостей;

контроль отсутствия в видимых пользователями сообщениях об ошибках защищаемой информации (например, аутентификационных данных, сведений, идентифицирующих программное обеспечение составных частей ППО, диагностической информации, содержащей подобные данные);

контроль отсутствия защищаемой и аутентификационной информации в сообщениях HTTP любого типа

], при экспорте данных пользователя, контролируемом ПФБ, за пределы ОО.

FDP_ETC.1.2 ФБО должны экспортировать данные пользователя без атрибутов безопасности, ассоциированных с данными пользователя.

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или FDP_IFC.1 Ограниченное управление информационными потоками].

FDP_IFC.1 Ограниченное управление информационными потоками

FDP_IFC.1.1 ФБО должны осуществлять [назначение: ПФБ управления информационными потоками] для [назначение: список субъектов, информации и операций перемещения управляемой информации к управляемым субъектам и от них, на которые распространяется ПФБ].

Зависимости: FDP_IFF.1 Простые атрибуты безопасности.

FDP_IFF.1 Простые атрибуты безопасности

FDP_IFF.1.1 ФБО должны осуществлять [назначение: ПФБ управления информационными потоками], основанную на следующих типах атрибутов безопасности субъекта и информации: [назначение: список субъектов и типов информации, находящихся под управлением указанной ПФБ, и для каждого из них – атрибуты безопасности].

FDP_IFF.1.2 ФБО должны разрешать информационный поток между управляемым субъектом и управляемой информацией посредством управляемой операции, если выполняются следующие правила: [назначение: основанные на атрибутах безопасности отношения, которые необходимо поддерживать между атрибутами безопасности субъектов и информации (для каждой операции)].

FDP_IFF.1.3 ФБО должны осуществлять [назначение: дополнительные правила ПФБ управления информационными потоками].

FDP_IFF.1.4 ФБО должны явно разрешать информационный поток, основываясь на следующих правилах: [назначение: основанные на атрибутах безопасности правила, которые явно разрешают информационные потоки].

FDP_IFF.1.5 ФБО должны явно запрещать информационный поток, основываясь на следующих правилах: [назначение:

основанные на атрибутах безопасности правила, которые явно запрещают информационные потоки].

Зависимости: FDP_IFC.1 Ограниченное управление информационными потоками

FMT_MSA.3 Инициализация статических атрибутов

FDP_ITC.2 Импорт данных пользователя с атрибутами безопасности

FDP_ITC.2.1 ФБО должны осуществлять [

предварительную проверку корректности входных данных (в том числе проверку ограничений на длину текстовых строк, отсутствие в них недопустимых символов и комбинаций символов, соответствие числовых значений граничным условиям);

контроль наличия в параметрах веб-формы, предназначенных для ввода защищаемой информации, директив, запрещающих кеширование данных;

контроль наличия атрибута HTTPOnly у параметров cookie, значения которых не должны быть доступны сценариям, выполняемым веб-браузером;

контроль наличия атрибута secure у параметров cookie, содержащих защищаемую информацию;

контроль наличия директивы, определяющей используемую кодировку в заголовках сообщений HTTP, а также отсутствия использования разных кодировок для разных источников входных данных;

контроль корректности входных данных, предназначенных для последующей обработки программными модулями,

допускающими интерпретацию команд (SQL, XPath, LINQ, LDAP, командная оболочка ОС и т.п.);

преобразование специальных символов, предусмотренное спецификациями языка HTML (например, замена символов ‘<’ и ‘>’ специальными символами языка HTML);

[**назначение**: *другую ПФБ управления доступом и/или ПФБ управления информационными потоками*]

] при импорте данных пользователя, контролируемом ПФБ, из-за пределов ОО.

FDP_ITC.2.2 ФБО должны использовать атрибуты безопасности, ассоциированные с импортируемыми данными пользователя.

FDP_ITC.2.3 ФБО должны обеспечить, чтобы используемый протокол предусматривал однозначную ассоциацию между атрибутами безопасности и полученными данными пользователя.

FDP_ITC.2.4 ФБО должны обеспечить, чтобы интерпретация атрибутов безопасности импортируемых данных пользователя была такой, как предусмотрено источником данных пользователя.

FDP_ITC.2.5 ФБО должны осуществлять следующие правила при импорте данных пользователя, контролируемом ПФБ, из-за пределов ОО: [**назначение**: *дополнительные правила управления импортом*].

FDP_ITC.2.6 ФБО должны использовать встроенные средства проверки корректности входных параметров, реализованные в стандартных программных библиотеках.

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками].

[FTP_ITC.1 Доверенный канал передачи между ФБО или

FTP_TRP.1 Доверенный маршрут]

FPT_TDC.1 Базовая согласованность данных ФБО между ФБО.

FDP_RIP.2 Полная защита остаточной информации

FDP_RIP.2.1 ФБО должны обеспечить недоступность любого предыдущего информационного содержания ресурсов при [**выбор**:

распределение ресурса,

освобождение ресурса

] для всех объектов.

Зависимости: отсутствуют.

Замечания по применению:

Семейство FDP_RIP связано с необходимостью обеспечения последующей недоступности любых данных, содержащихся в ресурсе, если ресурс удален из одного объекта и перемещен в другой объект. Это семейство содержит требования защиты данных, содержащихся в ресурсе, которые были логически удалены или исключены из рассмотрения, но физически все еще могут присутствовать в контролируемом ФБО ресурсе, который, в свою очередь, может быть перемещен в другой объект.

Работы оценки

Оценщик должен исследовать представление реализации, с тем чтобы сделать вывод о том, что память, динамически выделяемая информационным объектам, освобождается после их использования и при этом процедура

освобождения памяти обеспечивает невозможность повторного использования освобождаемых объектов.

FDP_ROL.1 Базовый откат

FDP_ROL.1.1 ФБО должны осуществлять, при наличии технической возможности, [**назначение**: ПФБ управления доступом и/или ПФБ управления информационными потоками], чтобы разрешать откат [**назначение**: список операций] на [**назначение**: список объектов].

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками].

7.1.3. Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [**выбор**:

*[**назначение**: положительное целое число];*

*устанавливаемое администратором положительное целое число в пределах [**назначение**: диапазон допустимых значений]*

] неуспешных попыток аутентификации, относящихся к [назначение: *список событий аутентификации*].

FIA_AFL.1.2 При [**выбор**:

достижении;

превышении

] установленного числа неуспешных попыток аутентификации ФБО должны выполнить

[**выбор:**

блокирование доступа пользователя в ОО;

требование ввода пользователем дополнительной информации при невозможности ввода этой информации в автоматическом режиме

]

FIA_AFL.1.3 **При истечении [назначение: *интервал времени*] от момента блокирования доступа пользователя в ОО по неуспешным попыткам аутентификации ФБО должны выполнить автоматическое разблокирование доступа пользователя в ОО.**

Зависимости: FIA_UAU.2 Аутентификация до любых действий пользователя.

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности [**назначение**: *список атрибутов безопасности*].

Зависимости: отсутствуют.

FIA_IWS_EXT.1 Идентификация сессий веб-приложений

FIA_IWS_EXT.1.1 ФБО должны [*уточнение:*

определить минимальную длину идентификатора в размере 8 символов]

[**выбор**:

нет идентификации сессий веб-приложений;

исключать использование предсказуемых идентификаторов сессий;

исключать возможность повторного использования идентификатора сессии (в том числе использование одинаковых идентификаторов в нескольких сессиях одного пользователя, неизменность идентификатора сессии после повторной аутентификации пользователя);

исключать возможность использования идентификатора сессии после ее завершения;

исключать возможность раскрытия идентификаторов сессий, в том числе передачу идентификаторов в незашифрованном виде, а также включение идентификаторов в запись журналов регистрации событий, в сообщения об ошибках

].

Зависимости: отсутствуют.

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 ФБО должны предоставить механизм для верификации того, что секреты отвечают *[**назначение**: определенная метрика качества*].

Зависимости: отсутствуют.

Замечание по применению:

Под метрикой качества в том числе следует понимать:

- ограничения на использование в алгоритмах аутентификации сужающих преобразований аутентификационных данных (например, приведение букв идентификатора пользователя и (или) пароля к одному регистру, ограничение количества значащих символов пароля);
- принудительное ограничение на минимальную сложность паролей (например, ограничение минимальной длины пароля, наличие

символов различных классов, несовпадение пароля с идентификатором пользователя, несовпадение нового пароля с одним из ранее использовавшихся).

FIA_SOS.2 Генерация секретов ФБО

FIA_SOS.2.1 ФБО должны предоставить механизм генерации секретов, отвечающих [**выбор:**

нет генерации секретов

*[**назначение**: определенная метрика качества]*

].

FIA_SOS.2.2 ФБО должны ограничивать использование при генерации паролей единого первоначального пароля или формирование таких паролей по единому алгоритму, смену пароля пользователем без предварительной аутентификации, а также содержать механизм принудительной смены первоначального пароля при первом входе пользователя в ОО.

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны [**выбор:**

***не требовать**;*

требовать

], чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Зависимости: FIA_UID.1 Выбор момента идентификации.

FIA_UAU.4 Механизмы одноразовой аутентификации

FIA_UAU.4.1 ФБО должны предотвращать повторное применение аутентификационных данных, связанных с [**назначение***: идентифицированный механизм (механизмы) аутентификации*].

Зависимости: отсутствуют.

FIA_UAU.5 Сочетание механизмов аутентификации

FIA_UAU.5.1 ФБО должны предоставлять [**назначение**: *список сочетаемых механизмов аутентификации*] для поддержки аутентификации пользователя.

FIA_UAU.5.2 ФБО должны аутентифицировать представленный идентификатор пользователя согласно [**назначение**: *правила, описывающие, как сочетание механизмов аутентификации обеспечивает аутентификацию*].

Зависимости: отсутствуют.

Замечания по применению:

1. Компонент предназначен для задания требований к функциональным возможностям ОО по поддержке многофакторной (двухфакторной) аутентификации.

2. В FIA_UAU.5.1 разработчик ЗБ указывает механизмы аутентификации, поддерживаемые ОО при многофакторной (двухфакторной) аутентификации.

3. В FIA_UAU.5.2 разработчик ЗБ указывает поддерживаемые правила сочетания механизмов аутентификации при многофакторной (двухфакторной) аутентификации.

FIA_UAU.6 Повторная аутентификация

FIA_UAU.6.1 ФБО должны повторно аутентифицировать пользователя при [**назначение**: *список условий, при которых требуется повторная аутентификация*] во время выполнения аутентификации.

Зависимости: отсутствуют.

FIA_UAU.7 Аутентификация **с защищенной обратной связью**

FIA_UAU.7.1 ФБО должны предоставлять пользователю только [**назначение**: *список допустимой информации обратной связи*] во время выполнения аутентификации.

Зависимости: FIA_UAU.2 Аутентификация до любых действий пользователя.

Замечания по применению:

Во время ввода аутентификационной информации вводимые символы не должны отображаться. При конкретизации в ЗБ данного компонента указывается, что будет отображаться при вводе аутентификационной информации (условные знаки: точки, звездочки; количество введенных символов или др.).

FIA_UID.1 Выбор момента идентификации

FIA_UID.1.1 ФБО должны допускать [**назначение**: список действий, выполняемых при посредничестве ФБО] от имени пользователя прежде, чем он идентифицирован.

FIA_UID.1.2 ФБО должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого другого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Зависимости: отсутствуют.

7.1.4. Управление безопасностью (FMT)

FMT_CFG_EXT.1 Конфигурация безопасности по умолчанию

FMT_CFG_EXT.1.1 ФБО должны при установке новых учетных данных, когда конфигурируются с учетными данными по умолчанию или без учетных данных, предоставить [**назначение**: *уполномоченные пользователи*] только ограниченную функциональность.

FMT_CFG_EXT.1.2 ФБО должны запрещать создание технологических учетных записей со стандартными паролями и иными механизмами аутентификации, использующими стандартный секрет для аутентификации, задаваемыми автоматически при установке программного обеспечения.

Зависимости: FMT_SMF.1 Спецификация функций управления.

FMT_MEC_EXT.1 Поддерживаемый механизм конфигурации

FMT_MEC_EXT.1.1 ФБО должны защищать хранилища параметров конфигурации (настроек) ОО от несанкционированного доступа.

FMT_MEC_EXT.1.2 ФБО должны обеспечить возможность экспорта параметров конфигурации ОО в формат, пригодный для анализа пользователем.

FMT_MEC_EXT.1.3 ФБО должны использовать для хранения и установки параметров конфигурации ОО механизмы, предусмотренные платформой.

Зависимости: FMT_SMF.1 Спецификация функций управления.

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [**назначение**: *ПФБ управления доступом, ПФБ управления информационными потоками*], предоставляющую возможность [**выбор**:

изменять значения по умолчанию;

запрашивать;

модифицировать;

удалять;

*[**назначение**: другие операции]*

] атрибуты безопасности [**назначение**: *список атрибутов безопасности*] только [**назначение**: *уполномоченные идентифицированные роли*].

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками].

FMT_SMR.1 Роли безопасности.

FMT_SMF.1 Спецификация функций управления.

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [**назначение**: *ПФБ управления доступом, ПФБ управления информационными потоками*], предусматривающую [**выбор**:

ограничительные;

разрешающие;

другие свойства]

] значения по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ.

FMT_MSA.3.2 ФБО должны позволять [**назначение**: *уполномоченные идентифицированные роли*] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

Зависимости: FMT_MSA.1 Управление атрибутами безопасности

FMT_SMR.1 Роли безопасности

FMT_MTD.1 Управление данными ФБО

FMT_MTD.1.1 ФБО должны предоставлять возможность [**выбор**:

изменение значений по умолчанию;

запрос;

модификация;

удаление;

очистка;

формирование отчетов;

[назначение: другие операции]

] следующих данных [**назначение**: *данные о пользователях и их привилегиях, список других данных ФБО*] только [**назначение**: *уполномоченные идентифицированные роли*].

Зависимости: FMT_SMR.1 Роли безопасности

FMT_SMF.1 Спецификация функций управления

FMT_SMF.1 Спецификация функций управления

FMT_SMF.1.1 ФБО должны быть способны к выполнению следующих функций управления: [**назначение**: *список функций управления, предоставляемых ФБО*].

Зависимости: отсутствуют.

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли [**назначение**: *уполномоченные идентифицированные роли*].

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

Зависимости: отсутствуют.

7.1.5. Приватность (FPR)

FPR_ANO_EXT.1 Согласие пользователей на обработку персональных данных (идентификационной информации)

FPR_ANO_EXT.1.1 ФБО должны: [**выбор**:

не обрабатывать персональную идентификационную информацию;

запрашивать согласие пользователя на обработку его персональной идентификационной информации

], защита которой требуется в соответствии с законодательством.

Зависимости: отсутствуют.

7.1.6. Защита ФБО (FPT)

FPT_AEX_EXT.1 Противодействие использованию уязвимостей безопасности

FPT_AEX_EXT.1.1 ФБО не должны требовать отображения памяти с явными адресами, за исключением [**назначение**: *список явных исключений*].

FPT_AEX_EXT.1.2 ФБО должны [**выбор**:

не выделять никакую область памяти с разрешениями писать и выполнять;

выделять области памяти с разрешениями писать и выполнять только для [назначение: список функций, выполняющих компиляцию just-in-time]

].

FPT_AEX_EXT.1.3 ФБО должны [**выбор**:

запрещать запись пользовательской информации в системные директории;

разрешать запись пользовательской информации [назначение: список системных директорий]

].

FPT_AEX_EXT.1.4 В ФБО не должны использоваться элементы управления в графическом интерфейсе пользователя ППО, предназначенные для выполнения операций, права на выполнение которых у пользователя отсутствуют. Проверка прав на выполнение любых операций пользователя должна осуществляться таким образом, чтобы пользователь не мог повлиять на результаты такой проверки.

FPT_AEX_EXT.1.5 ФБО должны быть совместимы со средствами защиты, предоставляемыми поставщиком/разработчиком платформы.

FPT_AEX_EXT.1.6 ФБО не должны записывать модифицируемые пользователем файлы в директории, которые содержат исполняемые файлы, [**выбор:**

если делать так явно не предписано разработчиком

].

FPT_AEX_EXT.1.7 ФБО должны позволять смену пользователем пароля или иного используемого параметра аутентификации только после предварительной аутентификации.

FPT_AEX_EXT.1.8 ФБО должны обеспечивать предварительную инициализацию переменных и структур данных при выделении оперативной памяти.

FPT_AEX_EXT.1.9 ФБО должны исключать возможность просмотра содержимого каталогов веб-сайта в случаях, когда такой просмотр не является необходимым. Если такой просмотр и изменение необходимы, ФБО должны исключать возможность просмотра и изменения произвольного каталога веб-сайта и возможность изменения каталога веб-сайта, в котором может быть расположен исполняемый код.

FPT_AEX_EXT.1.10 ФБО [**выбор:**

не должны использовать при обработке данных в формате XML внешние сущности (External Entity), внешние параметры сущностей (External Parameter Entity) и внешние описания типа документа (External Doctype);

контролировать невозможность включения пользователем таких внешних сущностей, параметров и описаний типа документа, которые могут вызвать атаку типа XXE;

].

FPT_AEX_EXT.1.11 ОО не должен требовать для своего выполнения прав администратора операционной системы, за исключением случаев, когда такие права технически необходимы для корректного функционирования ОО.

FPT_AEX_EXT.1.12 ФБО должны предусматривать меры защиты от обратной разработки и меры по противодействию отладке ППО.

FPT_AEX_EXT.1.13 ФБО должны выполнять все значимые проверки первичных электронных документов таким образом, чтобы пользователь ППО не мог повлиять на результат проверки (например, проводить проверки реквизитов отправителя на стороне банка).

FPT_AEX_EXT.1.14 ФБО не должна использовать полученную от пользователя информацию для определения типа сущности ФБО, которая будет создана на основе полученной информации, без дополнительной проверки на допустимость создания такой сущности (противодействие атакам небезопасной десериализации).

FPT_AEX_EXT.1.15 В случае использования многопоточности в ФБО должна корректно обрабатывать конкурентный доступ к информации для предотвращения модификации информации в обход проверок доступа (противодействие уязвимостям типа «состояние гонки»).

Зависимости: отсутствуют.

FPT_API_EXT.1 Использование поддерживаемых сервисов и прикладных программных интерфейсов

FPT_API_EXT.1.1 ФБО должны использовать в программном продукте только задокументированные производителем сервисы и прикладные программные интерфейсы платформы. Выбор: [назначение: использовать в программном продукте задокументированные производителем сервисы.] [назначение: использовать доверенные самописные (сторонние) библиотеки функций противодействия использованию уязвимостей.]

FPT_API_EXT.1.2 ФБО должны использовать механизмы, предоставляемые архитектурой процессора, операционной системой и средствами компиляции кода (например, защиты от переполнения буфера, защиты от нарушения обработки исключений, защиты от исполнения кода в сегментах стека и данных, случайного размещения сегментов в адресном пространстве).

FPT_API_EXT.1.3 ФБО не должны использовать функции стандартных библиотек, уязвимых к атакам переполнения буфера, при наличии аналогичных функций со встроенной защитой.

Зависимости: отсутствуют.

FPT_LIB_EXT.1 Использование сторонних библиотек

FPT_LIB_EXT.1.1 ФБО должны использовать только [**назначение**: *список разрешенных сторонних библиотек*].

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 ФБО должны быть способны **[выбор:**

предоставлять;

не предоставлять

] *надежные метки времени.*

Зависимости: отсутствуют.

FPT_TDC.1 Базовая согласованность данных ФБО между ФБО

FPT_TDC.1.1 ФБО должны обеспечить способность согласованно интерпретировать [**назначение**: *список типов данных ФБО*], совместно используемые ФБО и другим доверенным продуктом ИТ.

FPT_TDC.1.2 ФБО должны использовать [**назначение**: *список правил интерпретации, применяемых ФБО*] при интерпретации данных ФБО, полученных от другого доверенного продукта ИТ.

Зависимости: отсутствуют.

FPT_TST.1 Тестирование ФБО

FPT_TST.1.1 ФБО должны выполнять пакет программ самотестирования [**выбор**:

при запуске;

периодически в процессе нормального функционирования;

по запросу уполномоченного пользователя;

*при условиях [**назначение**: условия, при которых следует предусмотреть самотестирование]*

] для демонстрации правильного выполнения [**выбор**:

*[**назначение**: части ФБО],*

ФБО

].

FPT_TST.1.2 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность, **корректность параметров конфигурации** [**выбор**:

*[**назначение**: данных частей ФБО];*

данных ФБО

].

FPT_TST.1.3 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность хранимого выполняемого кода ФБО.

FPT_TST.1.4 ФБО при выявлении нарушения целостности или некорректности параметров конфигурации должны:

[**выбор:**

- *перевести ОО в режим аварийного функционирования;*
- *предоставить уполномоченным пользователям возможность перевести ОО в режим аварийного функционирования]*,

отключить [**назначение**: *список функций безопасности ОО*],

сгенерировать диагностическую информацию.

Зависимости: отсутствуют.

FPT_TUD_EXT.1 Целостность при установке и обновлении

FPT_TUD_EXT.1.1 ФБО должны [**выбор**:

предоставлять возможность;

эффективно использовать платформу

], чтобы проверить обновление и установку патчей для ОО.

FPT_TUD_EXT.1.2 Программное обеспечение ОО должно распространяться с использованием формата, поддерживаемого платформой диспетчера пакетов. [**выбор:**

использовать средства по установке/удалению/обновлению программного обеспечения собственного производства;

использовать средства по установке/удалению/обновлению программного обеспечения стороннего производства.]

FPT_TUD_EXT.1.3 Программное обеспечение ОО должно быть упаковано таким образом, чтобы его удаление приводило к удалению всех его следов, за исключением параметров конфигурации, выходных файлов и контрольных/ регистрационных событий. [**выбор**:

использовать средства по установке/удалению/обновлению программного обеспечения собственного производства;

использовать средства по установке/удалению/обновлению программного обеспечения стороннего производства.]

FPT_TUD_EXT.1.4 Программное обеспечение ОО не должно загружать, изменять, заменять или обновлять [**выбор**:

при отсутствии автообновления

]

его собственный двоичный код.

FPT_TUD_EXT.1.5 Программное обеспечение ОО должно [**выбор**:

предоставлять возможность;

эффективно использовать платформу

], чтобы выяснить текущую версию прикладного программного обеспечения.

Зависимости: отсутствуют.

7.1.7. Доступ к ОО (FTA)

FTA_MCS.1 Базовое ограничение на параллельные сеансы

FTA_MCS.1.1 ФБО должны ограничить максимальное число параллельных сеансов, предоставляемых одному и тому же пользователю.

FTA_MCS.1.2 ФБО должны задать по умолчанию ограничение [**назначение**: *задаваемое по умолчанию число*] сеансов пользователя.

Зависимости: FIA_UID.1 Выбор момента идентификации.

7.1.8. Доверенный маршрут/канал (FTP)

FTP_DIT_EXT.1 Защита данных при передаче

FTP_DIT_EXT.1.1 ФБО должны [**выбор**:

не передавать любые данные;

не передавать любую защищаемую информацию;

шифровать всю передаваемую защищаемую информацию;

реализовать функциональность для шифрования защищаемой информации

] между ОО и другими доверенными продуктами ИТ.

Зависимости: отсутствуют.

FTP_ITC.1 Доверенный канал передачи между ФБО

FTP_ITC.1.1 ФБО должны предоставлять канал связи между собой и другим доверенным продуктом ИТ, который логически отличим от других каналов связи и обеспечивает уверенную

идентификацию его конечных сторон, а также защиту данных канала от модификации или раскрытия.

FTP_ITC.1.2 ФБО должны позволить [**выбор**:

ФБО,

другой доверенный продукт ИТ

] инициировать связь через доверенный канал.

FTP_ITC.1.3 ФБО должны инициировать связь через доверенный канал для выполнения [**назначение:** список функций, для которых требуется доверенный канал].

Зависимости: отсутствуют.

7.2. Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» с учетом положений ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» и образуют ОУД4, усиленный дополнительными компонентами (см. таблицу 7.2).

Таблица 7.2 – Требования доверия к безопасности ОО

Классы доверия	**Идентификаторы компонентов доверия**	**Названия компонентов доверия**
Разработка	ADV_ARC.1	Описание архитектуры безопасности
	ADV_FSP.4	Полная функциональная спецификация
	ADV_IMP.2*	Полное отображение представления реализации ФБО
	ADV_IMP_EXT.3*	Реализация ОО
	ADV_TDS.3	Базовый модульный проект
	ADV_TDS_EXT.3	Разработка, уточнение и анализ архитектуры программного обеспечения ОО
Руководства	AGD_OPE.1	Руководство пользователя по эксплуатации
	AGD_OPE_EXT.1	Правила кодирования
	AGD_PRE.1	Подготовительные процедуры
Поддержка жизненного цикла	ALC_CMC.4**	Поддержка генерации, процедуры приемки и автоматизация
	ALC_CMS.4	Охват УК отслеживания проблем
	ALC_DEL.1	Процедуры поставки

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
	ALC_DEL_EXT.1	Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок
	ALC_DVS.1	Идентификация мер безопасности
	ALC_DVS_EXT.1	Моделирование угроз и разработка описания поверхности атаки
	ALC_DVS_EXT.2	Обеспечение безопасности сборочной среды программного обеспечения
	ALC_DVS_EXT.3	Управление доступом и контроль целостности кода при разработке программного обеспечения
	ALC_FLR.2	Процедуры сообщений о недостатках
	ALC_FPU_EXT.1	Процедуры обновления программного обеспечения
	ALC_LCD.1	Определенная заявителем модель жизненного цикла
	ALC_LCD_EXT.3	Определенные разработчиком сроки поддержки
	ALC_TAT.1	Полностью определенные инструментальные средства разработки
	ALC_TAT_EXT.1	Статический анализ исходного кода
	ALC_TAT_EXT.2	Динамический анализ кода программы
Оценка задания по безопасности	ASE_CCL.1	Утверждения о соответствии
	ASE_ECD.1	Определение расширенных компонентов
	ASE_INT.1	Введение ЗБ
	ASE_OBJ.2	Цели безопасности
	ASE_REQ.2	Производные требования безопасности
	ASE_SPD.1	Определение проблемы безопасности
	ASE_TSS.1	Краткая спецификация ОО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.2	Тестирование: модули обеспечения безопасности
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
	ATE_IND.EXT.1	Нефункциональное тестирование
Оценка уязвимостей	AVA_VAN.5	Усиленный методический анализ
	AVA_VAN_EXT.1	Реагирование на информацию об уязвимостях
	AVA_CCA_EXT.1	Анализ скрытых каналов
Композиция***	ACO_DEV.1	Функциональное описание
	ACO_REL.1	Базовая информация о зависимостях
	ACO_VUL.2	Анализ уязвимостей композиции
Обновление ОО	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность ОО

Примечания:

* – Отмечены компоненты, конкретизированные в настоящем ПЗ для обеспечения унификации с действующими ПЗ ФСТЭК России и преемственности требований по контролю отсутствия недекларированных возможностей руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации: Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999).

** – Требования доверия настоящего ПЗ основаны на ОУД4, усиленном, с учетом предыдущего примечания, компонентом ADV_IMP.2, для которого по зависимости требуется компонент ALC_CMC.5. Однако для исключения чрезмерного завышения требований в настоящем ПЗ сохранен компонент ALC_CMC.4, который входит в состав ОУД4.

*** – Отмечены компоненты, конкретизированные в настоящем ПЗ для обеспечения унификации с требованиями раздела 5.16 «Использование инструментов композиционного анализа» ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

7.2.1. Разработка (ADV)

Требования данного класса определяют необходимость предоставления заявителем информации об ОО в виде совокупности свидетельств, содержащих проектные материалы по разработке ОО.

Оформление и содержание свидетельств должно соответствовать требованиям национальных стандартов Российской Федерации.

ADV_ARC.1 Описание архитектуры безопасности

В «Описании архитектуры безопасности» должно объясняться, как в ФБО реализуются свойства собственной защиты, разделения доменов и невозможности обхода ФБО. Оно должно содержать описание механизмов определения и разделения доменов посредством ФБО; мер защиты ФБО от несанкционированного доступа и модификации со стороны недоверенных процессов; а также описание мер, обеспечивающих надлежащую защиту всех ресурсов под контролем ФБО и выполнение ФБО роли посредника в действиях, связанных с ФТБ. Также в «Описании архитектуры безопасности» должна объясняться роль среды в любом из этих процессов.

Зависимости: ADV_FSP.1 Базовая функциональная спецификация;

ADV_TDS.1 .Базовый проект

Элементы действий разработчика

ADV_ARC.1.1D Разработчик должен спроектировать ОО и обеспечить реализацию проекта таким образом, чтобы свойства безопасности ФБО невозможно было обойти.

ADV_ARC.1.2D Разработчик должен спроектировать ФБО и обеспечить их реализацию таким образом, чтобы ФБО обеспечивали собственную защиту от вмешательства недоверенных сущностей.

ADV_ARC.1.3D Разработчик должен предоставить «Описание архитектуры безопасности» ФБО.

Элементы содержания и представления документированных материалов

ADV_ARC.1.1C Уровень детализации «Описания архитектуры безопасности» должен соответствовать представленному в проектной документации по ОО описанию абстракций (элементов представления ОО), осуществляющих выполнение ФТБ.

ADV_ARC.1.2C В «Описание архитектуры безопасности» должно быть включено описание доменов безопасности, обеспеченных согласованностью ФБО с ФТБ.

ADV_ARC.1.3C «Описание архитектуры безопасности» должно предоставлять информацию о том, насколько процесс инициализации ФБО является защищенным.

ADV_ARC.1.4C В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО обеспечивают собственную защиту от вмешательства.

ADV_ARC.1.5C В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО не допускают возможности обхода функциональных возможностей, осуществляющих выполнение ФТБ.

Элементы действий оценщика

ADV_ARC.1.1E Оценщик должен подтвердить, что информация, представленная разработчиком в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в ADV_ARC.1.1C – ADV_ARC.1.5C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 10.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности.

Методология оценки безопасности информационных технологий».

Архитектура безопасности должна обеспечивать, чтобы ОО не имел каналов связи, обеспечивающих доступ (в том числе внеполосный) в обход заданных правил управления доступом к ОО (его программному обеспечению и настройкам), а также правил контроля и фильтрации сетевого трафика (сетевых потоков).

Оценщик должен изучить представленные документированные материалы в совокупности с другими документированными материалами по ОО и ФБО и вынести заключения о том, достигается ли реализация заявленных свойств.

ADV_FSP.4 Полная функциональная спецификация

В функциональной спецификации описываются интерфейсы ФБО (ИФБО). ИФБО включают в себя все способы, которыми пользователи могут вызвать тот или иной сервис ФБО (путем предоставления информации, которая обрабатывается ФБО), и соответствующую реакцию на запросы на обслуживание. Определены три категории ИФБО в зависимости от степени значимости тех сервисов, к которым эти интерфейсы предоставляют доступ для заявленных ФТБ:

если сервис, доступ к которому предоставляется интерфейсом, может быть сопоставлен с одним из ФТБ, предъявляемых к ФБО, тогда данный интерфейс относится к категории ***осуществляющих выполнение ФТБ***;

интерфейсы сервисов, от которых зависят функциональные возможности, осуществляющие выполнение ФТБ, но при этом от них для осуществления политик безопасности ОО требуется только правильное функционирование, относятся к категории ***поддерживающих выполнение ФТБ***;

интерфейсы сервисов, от которых никак не зависят функциональные возможности, осуществляющие выполнение ФТБ, относятся к ***не влияющим на выполнение ФТБ***.

Интерфейсы специфицируются в терминах назначения интерфейса, метода использования, параметров, описаний параметров и сообщений об ошибках.

Зависимости: ADV_TDS.1 .Базовый проект.

Элементы действий разработчика

ADV_FSP.4.1D Разработчик должен представить функциональную спецификацию.

ADV_FSP.4.2D Разработчик должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления документированных материалов

ADV_FSP.4.1C В функциональной спецификации должны быть полностью представлены ФБО.

ADV_FSP.4.2C В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

Замечания по применению:

Назначение ИФБО – это общее утверждение, кратко описывающее функциональные возможности, предоставляемые интерфейсом.

Если действие, доступное через интерфейс, играет роль в осуществлении какой-либо политики безопасности ОО (то есть, если одно из действий интерфейса может быть прослежено к одному из ФТБ, предъявляемых к ФБО), то этот интерфейс – осуществляющий ФТБ. Это относится не только к политикам управления доступом, но также и к любым функциям, определенным одним из ФТБ, содержащихся в ЗБ. Следует отметить, что у интерфейса могут быть различные действия и результаты его вызова, некоторые из которых могут быть осуществляющими ФТБ, а некоторые – нет.

Интерфейсы (или действия, доступные через связанный с ними интерфейс), от которых зависят функции, осуществляющие выполнение ФТБ, от которых требуется только правильное функционирование для поддержания выполнения политик безопасности ОО, являются интерфейсами, поддерживающими выполнение ФТБ. Интерфейсы, от которых никак не зависят функции, осуществляющие выполнение ФТБ, не относятся к ИФБО.

Следует отметить, что для того, чтобы интерфейс был отнесен к поддерживающим или не влияющим на выполнение ФТБ, он не должен включать в себя действия и результаты, осуществляющие выполнение ФТБ. Напротив, осуществляющий выполнение ФТБ интерфейс может включать поддерживающие выполнение ФТБ действия.

ADV_FSP.4.3C В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV_FSP.4.4C В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.

ADV_FSP.4.5C Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.

ADV_FSP.4.6C В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий оценщика

ADV_FSP.4.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_FSP.4.1C – ADV_FSP.4.6C.

ADV_FSP.4.2E Оценщик должен сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 10.4.4 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ADV_IMP.2 Полное отображение представления реализации ФБО

Зависимости: ADV_TDS.3 Базовый модульный проект;

ALC_TAT.1 Полностью определенные инструментальные средства разработки;

ALC_CMC.4 Поддержка генерации, процедуры приемки и автоматизация.

Элементы действий разработчика

ADV_IMP.2.1D Разработчик должен обеспечить доступ к представлению реализации для всех ФБО.

Замечания по применению:

Доступ к представлению реализации должен быть предоставлен на уровне исходных текстов всего программного обеспечения, входящего в состав ОО.

Доступ ко всему представлению реализации должен быть предоставлен для того, чтобы обеспечить уверенность в том, что действия по анализу не будут сокращены вследствие недостаточности информации.

Разработчик должен сделать доступным представление реализации ОО в форме, которая может быть проанализирована оценщиком.

ADV_IMP.2.2D Разработчик должен обеспечить прослеживание всего представления реализации к описанию проекта ОО.

ADV_IMP.2.3D Разработчик должен провести контроль представления реализации ОО.

Замечания по применению:

Контроль представления реализации – мероприятия, осуществляемые в отношении определенных частей исходного текста (исходного кода) ПО, созданного одним или несколькими разработчиками, другим (не создававшим эту часть кода) разработчиком или назначенным в установленном порядке иным имеющим требуемую подготовку специалистом и состоящие в детальной проверке (изучении, анализе, исследовании) соответствующих исходных кодов с целью выявления неизвестных уязвимостей, в том числе связанных с ошибками программирования, нарушений установленных требований, а также иных существенных дефектов.

Контроль исходного кода может осуществляться лицом, проверяющим код, как вручную, в том числе с использованием приемов эффективного чтения программного кода, так и с применением методов и средств автоматизированного анализа исходного кода, в том числе обеспечивающих статический анализ кода.

Контроль (проверка) исходного кода вручную обеспечивается просмотром, изучением и оценкой кода лицом, отличным от его разработчика. Является альтернативным методом оценки. Оценка кода может включать в себя:

а) оценку соответствия кода требованиям, предъявляемым к структурированию и оформлению кода, именованию объектов, разделению на модули, использованию специальных средств обеспечения качества кода, предусмотренных используемыми языками программирования и средствами разработки;

б) оценку полноты и качества документирования кода, включая документирование заголовков программных модулей, прототипов функций и структур данных, комментарии к выполнению существенных операций;

в) оценку соответствия алгоритмов, реализованных в исходном коде, программной документации, в том числе выявление явных недекларированных возможностей (программных закладок), ошибок программного кода, попыток запутывания (обфускации) программного кода и использования иных приемов, затрудняющих проведение контроля.

Примечание: *недекларированные возможности* – функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Статический анализ кода проводится с использованием автоматизированных средств (программных инструментов) и направлен на идентификацию потенциально опасных фрагментов кода, в том числе:

а) вызовов функциональных объектов (функций, методов, процедур) с передачей им в качестве аргументов данных, вводимых пользователем или принимаемых из внешних источников;

Примечание: *функциональный объект* – элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы. Функциональные объекты, в частности, могут быть

представлены в виде функций (процедур, подпрограмм), используемых в процедурно-ориентированных языках программирования, методов, используемых в объектно-ориентированных языках программирования, отдельных фрагментов в программном коде, процессов в языках описания аппаратных средств и т.п.;

б) текстов функциональных объектов преобразования форматов данных;

в) вызовов системных функциональных объектов и функциональных объектов обеспечения ИБ разделяемых обеспечивающих компонентов ППО, в том числе функциональных объектов обеспечения ИБ операционной системы, функциональных объектов ввода/вывода, управления памятью и системными ресурсами;

г) текстов функциональных объектов, осуществляющих проверку прав доступа и принятие решений, основанных на значениях атрибутов безопасности;

д) текстов функциональных объектов, самостоятельно реализующих функциональность обеспечения ИБ, в том числе криптографические функции, аутентификацию пользователей и проверку прав доступа, генерацию данных мониторинга ИБ;

е) текстов функциональных объектов, предусматривающих установление соединения с внешними компонентами с передачей им аутентификационных данных;

ж) текстов функциональных объектов обработчиков ошибок и исключений.

В ходе статического анализа кода необходимо проводить поиск типовых ошибок программирования (недостаточная проверка входных параметров функций, включение аутентификационных данных непосредственно в текст программ, некорректное преобразование типов, недостаточная обработка ошибок и исключений), а также определять статические пути исполнения программы.

В программном коде ОО должны отсутствовать аутентификационные данные, необходимые для доступа компонентов ППО к прочим ППО организации БС Российской Федерации.

Элементы содержания и представления документированных материалов

ADV_IMP.2.1C Представление реализации должно определить ФБО на таком уровне детализации, чтобы ФБО могли быть созданы без дополнительных проектных решений.

ADV_IMP.2.2C Представление реализации должно быть изложено в том виде, который используется персоналом, занимающимся разработкой.

Замечания по применению:

Представление реализации должно быть выполненным разработчиком таким образом, чтобы потом была возможность фактической реализации этого представления. Например, разработчик может работать с файлами, содержащими исходный текст программ, который потом будет скомпилирован и станет частью ФБО. Разработчик также может использовать в представлении реализации элементы, для которых исходные тексты недоступны, или элементы, не предполагающие проведения компиляции из

исходных текстов для генерации ФБО. Однако разработчик обязательно должен сделать доступным представление реализации в той форме, в какой он его использует. Это также увеличивает уверенность в том, что оцениваемое представление реализации является именно тем, которое используется при производстве ФБО (в отличие от того случая, когда оно сопровождается альтернативным форматом представления, например, документом текстового процессора). Разработчик может использовать различные формы представления реализации, которые также должны прилагаться. Основная цель – снабдить оценщика такой информацией, которая позволила бы максимизировать эффективность его усилий по анализу.

Разработчик ОО может применять в представлении реализации некие программы по сокрытию или запутыванию кода, например, обфускация, шифрование и т.п. Несмотря на то, что представление со скрытыми участками кода является именно тем, которое будет в дальнейшем подвергнуто компиляции, а потому может быть даже ближе к реализации (по структуре), чем оригинальная версия, предоставление оценщику запутанного программного кода может привести к значительному увеличению времени проведения анализа представления реализации и (или) невозможности получения положительного заключения. При подобных формах представления реализации разработчиком дополнительно должны быть представлены материалы по представлению реализации до применения сокрытия участков кода, а также применяемые средства/алгоритмы сокрытия для получения оценщиком уверенности в том, что процесс сокрытия

участков кода не нарушил выполнения каких-либо функциональных возможностей безопасности.

Для всех файлов с исходными текстами ПО в документации должны быть приведены значения контрольных сумм файлов.

ADV_IMP.2.3C В прослеживании между всем представлением реализации и описанием проекта ОО должно быть продемонстрировано их соответствие.

Замечания по применению:

Соответствие между всем представлением реализации и описанием проекта ОО должно быть продемонстрировано для всех модулей, отнесенных к осуществляющим или поддерживающим выполнение ФТБ.

Для модулей ОО, определенных как «не влияющие на выполнение ФТБ», должно быть предоставлено соответствующее обоснование.

ADV_IMP.2.4C Результаты контроля представления реализации разработчиком должны быть оформлены в виде протоколов контроля представления реализации.

Замечания по применению:

Результаты контроля должны быть подписаны разработчиками – непосредственными исполнителями разработки проверенного исходного кода и лицами, участвовавшими в его проверке (контролерами кода), с отражением в протоколе сведений о дате мероприятия, проверенной части исходных кодов, выявленных недостатках (при наличии), повторном контроле кодов с подтверждением устранения выявленных недостатков. Протокол необходимо оформлять в виде информации в электронной форме, созданной, переданной и надежно сохраненной в предусмотренной для данного вида информации системе электронного документооборота с реквизитами, позволяющими при аудите предъявлять ее в качестве электронного документа, подписанного простыми электронными подписями, а также при необходимости изготавливать и заверять ее копии на бумажном носителе.

Элементы действий оценщика

ADV_IMP.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_IMP.2.1C – ADV_IMP.2.4C**.**

ADV_IMP.2.2E Оценщик должен провести контроль соответствия всего представления реализации описанию проекта ОО, включая:

а) контроль исходного состояния ОО;

б) контроль полноты представления реализации на уровне исходных модулей программ;

в) контроль отсутствия избыточности представления реализации на уровне исходных модулей программ;

г) контроль полноты представления реализации на уровне функциональных объектов;

д) контроль отсутствия избыточности представления реализации на уровне функциональных объектов;

е) контроль связей функциональных объектов представления реализации по управлению;

ж) контроль связей функциональных объектов представления реализации по информации.

Работы оценки:

1. Оценщик должен выполнить действия в соответствии с пунктом 10.5.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» для всего представления реализации.

2. Исследование представления реализации должно выполняться с использованием методов статического и динамического анализа исходных модулей программ.

Под исходным модулем понимается программный модуль на исходном языке, обрабатываемый транслятором и представляемый для него как целое, достаточное для проведения трансляции. В зависимости от особенностей используемой среды разработки программ исходный модуль может быть представлен как файл с исходным текстом, запись в базе данных (например, хранимая процедура), активное содержимое документа (например, исполняемый код в файле документа с гипертекстовой разметкой) и т.п. К

исходным модулям относятся также и интерпретируемые исполняемые модули, для которых не предусмотрена компиляция, преобразование в объектный или исполняемый код.

Исследование представления реализации должно выполняться с использованием методов контроля (не)соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных модулей программ и сопоставлением с фактическими маршрутами выполнения функциональных объектов. Оценщик должен исследовать представление реализации и сделать заключение о том, является ли оно пригодным для проведения оценки. Если в представлении реализации используются механизмы, препятствующие проведению исследований его внутренней структуры, например, обфускация, шифрование и т.п., то вердикт не может быть положительным.

3. Оценщик должен выполнить контроль исходного состояния ОО. Контроль заключается в фиксации исходного состояния ОО и сравнении полученных результатов с приведенными в документации. Результатами контроля исходного состояния ОО должны быть рассчитанные уникальные значения контрольных сумм всех модулей, входящих в состав ПО.

4. Оценщик должен выполнить контроль полноты представления реализации на уровне исходных модулей.

Оценщик должен исследовать проект ОО, чтобы сделать заключение о том, что описание назначения каждого осуществляющего выполнение ФТБ модуля является полным и точным. В описании назначения исходного модуля должны приводиться выполняемые исходным модулем функции. Оно должно обеспечивать понимание функционирования исходного модуля таким образом, чтобы можно было сделать заключение о достаточности представления реализации для выполнения ФТБ.

Оценщик должен исследовать исходные модули, входящие в представление реализации, для того чтобы сделать заключение о соответствии их назначения описанию назначения, представленному в проекте ОО, и о достаточности представления реализации для выполнения ФТБ.

Если в результате исследования установлено, что для ФТБ отсутствует представление реализации или оно представлено только частично, то такому этапу исследования не может быть дана положительная оценка.

5. Оценщик должен выполнить контроль отсутствия избыточности представления реализации на уровне исходных модулей.

Оценщик должен исследовать проект ОО, с тем чтобы вынести заключение о том, что в описание всех исходных модулей ОО включена информация, соответствующая их роли в ОО (осуществляющие, поддерживающие выполнение ФТБ, не влияющие на выполнение ФТБ и т.д.). Описание должно указывать на выполняемые исходным модулем функции. Оно должно обеспечивать понимание функционирования исходного модуля таким образом, чтобы можно было сделать заключение о выполнении ФТБ, поддержке выполнения ФТБ или об отсутствии влияния на ФТБ.

Оценщик должен исследовать представление реализации чтобы сделать заключение в отношении каждого исходного модуля как осуществляющего выполнение ФТБ, поддерживающего выполнение ФТБ или не влияющего на выполнение ФТБ. В составе представления реализации могут находиться исходные модули, которые не используются в процессе его преобразования для создания фактической реализации ОО. Факт неиспользования таких модулей при преобразовании должен быть верифицирован оценщиком. Такие модули вне зависимости от наличия описания в проекте ОО могут быть признаны оценщиком с учетом результатов верификации не влияющими на выполнение ФТБ.

Оценщик при контроле отсутствия избыточности исходных модулей должен:

- в части исходных модулей, осуществляющих и поддерживающих выполнение ФТБ, – исследовать (основываясь на структурном анализе и декомпозиции) эти модули, чтобы сделать заключение об отсутствии в исходных модулях функциональных возможностей безопасности, не предусмотренных проектом и ФТБ;
- в части исходных модулей, заявленных как «не влияющие на выполнение ФТБ», – проанализировать эти модули с глубиной, достаточной для подтверждения их невлияния на выполнение ФТБ.

Исходные модули, назначение которых не описано в документации, признаются избыточными, а по шагу оценивания в целом выносится отрицательная оценка.

6. Оценщик должен выполнить контроль полноты представления реализации на уровне функциональных объектов.

Оценщик должен исследовать документированные материалы разработчика ОО, чтобы сделать вывод о том, что все аспекты ФТБ реализованы на уровне интерфейсов исходных модулей и связанных с ними определений функциональных объектов.

Оценщик должен исследовать функциональные объекты, входящие в представление реализации, с тем чтобы сделать заключение о соответствии их назначения описанию назначения, представленному в проекте ОО, и о достаточности содержащихся в представлении реализации функциональных объектов для выполнения ФТБ.

7. Оценщик должен выполнить контроль отсутствия избыточности представления реализации на уровне функциональных объектов.

Оценщик должен исследовать представление реализации, чтобы сделать заключение в отношении каждого функционального объекта как обеспечивающего выполнение ФТБ, поддерживающего выполнение ФТБ или не влияющего на выполнение ФТБ.

Функциональные объекты, назначение которых не описано в документации, признаются избыточными, по шагу оценивания в целом выносится отрицательная оценка.

В составе представления реализации могут находиться функциональные объекты, которые не используются в процессе его преобразования для создания фактической реализации ОО. Факт неиспользования таких функциональных объектов при преобразовании должен быть верифицирован оценщиком. Такие функциональные объекты вне зависимости от наличия описания в проекте ОО могут быть признаны оценщиком с учетом результатов верификации не влияющими на выполнение ФТБ.

8. Оценщик должен выполнить контроль связей функциональных объектов представления реализации по управлению.

Связи функциональных объектов по управлению могут быть как статическими (например, при вызове в исходном тексте явно указываются имя функции и значения ее фактических параметров), так и динамическими, реализуемыми только при выполнении программы (например, вызов функционального объекта по вычисляемому значению адреса в оперативной памяти, динамическое создание и вызов методов экземпляра объекта в объектно-ориентированном программировании, получение содержимого объекта, содержащего код и данные, по каналу связи от веб-сервера и т.п.). Динамические связи функций по управлению не всегда могут быть определены на основе анализа представления реализации без исполнения программы или ее фрагментов, например, под управлением отладчика.

Оценщик должен исследовать связи функциональных объектов представления реализации по управлению, с тем чтобы сделать заключение о том, что они не допускают возможности обхода механизмов, осуществляющих выполнение ФТБ. Если в отношении какого-либо функционального объекта не может быть сделано положительное заключение, то по шагу оценивания выносится отрицательная оценка.

При проведении исследования следует учитывать, что применение только одного метода статического анализа представления реализации для контроля связей функциональных объектов по управлению может оказаться недостаточным. Методу статического анализа присуще ограничение, связанное с принципиальной невозможностью определения связей функциональных объектов и интерфейсов модулей, а также связей функциональных объектов по управлению между собой, реализуемых динамически во время исполнения программы.

При обнаружении невозможности исследовать связи функциональных объектов по управлению только с использованием метода статического анализа оценщик должен использовать в дополнение к нему метод динамического анализа представления реализации.

9. Оценщик должен выполнить контроль связей функциональных объектов (модулей, процедур, функций) по информации.

Связи функциональных объектов по информации осуществляются путем использования функциональными объектами общих информационных объектов.

Информационный объект – элемент программы, содержащий фрагменты информации, циркулирующей в программе. В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, области оперативной памяти, потоки, именованные каналы, очереди, стеки и т.п.

Важным условием наличия связи функциональных объектов по информации являются определенные права доступа к совместно используемому информационному объекту. Связи функциональных объектов по информации могут осуществляться как явно, путем передачи фактических параметров при вызове функционального объекта из другого функционального объекта, так и неявно – за счет совместного использования некоторого общего глобального информационного объекта. В первом случае

связи функциональных объектов по информации могут быть прослежены при выполнении контроля связей функциональных объектов по управлению. Во втором случае предположение о наличии связи функциональных объектов по информации, основанное только на факте совместного использования общего информационного объекта, требует подтверждения на основе детального анализа как структуры самого информационного объекта, так и алгоритмов обработки информации, реализованных в функциональных объектах. В отличие от связей функциональных объектов по управлению связи по информации не всегда могут быть представлены в виде маршрутов выполнения функциональных объектов. Однако такие маршруты позволяют судить об информационных потоках, связанных с некоторым рассматриваемым информационным объектом.

При проведении исследования должны быть четко определены защищаемые ФБО информационные объекты и проанализированы все возможные обращения к ним из функциональных объектов, как непосредственные, так и через последовательность вызовов функциональных объектов.

Оценщик должен исследовать связи функциональных объектов по информации, с тем чтобы сделать заключение о том, что они не допускают возможности обхода механизмов, осуществляющих выполнение ФТБ.

ADV_IMP_EXT.3 Реализация ОО

Зависимости: ADV_IMP.2 Полное отображение представления реализации ФБО.

Элементы действий разработчика

ADV_IMP_EXT.3.1D Разработчик должен предоставить реализацию ОО.

ADV_IMP_EXT.3.2D Разработчик должен обеспечить прослеживание реализации ОО к представлению реализации ФБО.

Элементы содержания и представления документированных материалов

ADV_IMP_EXT.3.1C В документации должны быть указаны состав и значения контрольных сумм элементов реализации ПО [**выбор**:

загрузочные модули ПО;

*[**назначение**: иные типы элементов реализации ПО]*

].

ADV_IMP_EXT.3.2C В прослеживании между реализацией ОО и представлением реализации должно быть продемонстрировано соответствие между реализацией ПО [**выбор***:*

загрузочные модули ПО,

*[**назначение**: иные типы элементов реализации ПО]*

] *и их представлением реализации* [**выбор***:*

исходные тексты ПО,

*[**назначение**: иные формы представления реализации]*

].

Элементы действий оценщика

ADV_IMP_EXT.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_IMP_EXT.3.1C и ADV_IMP_EXT.3.2C.

Работы оценки

1. Оценщик должен верифицировать представленное разработчиком прослеживание между элементами представления реализации и элементами

фактической реализации ОО.

2. Оценщик должен выполнить контроль соответствия представления реализации ОО фактической реализации ОО.

Оценщик должен исследовать представление реализации, с тем чтобы сделать заключение о том, что представление реализации с использованием описанных инструментальных средств разработки может быть преобразовано в фактическую реализацию ОО.

Оценщик должен исследовать документированные процедуры, применяемые разработчиком для преобразования представления реализации в фактическую реализацию ОО, для того, чтобы сделать вывод о возможности выполнения преобразования.

Оценщик должен выполнить в соответствии с документированными процедурами разработчика с использованием инструментальных средств разработчика (или с использованием инструментальных средств, идентичных инструментальным средствам разработчика) преобразование представления реализации в фактическую реализацию ОО.

Оценщик должен провести верификацию соответствия фактической реализации ОО, полученной в процессе выполнения преобразования, с реализацией ОО, представленного для оценки.

Верификация соответствия фактической реализации ОО, полученной в процессе выполнения преобразования, с реализацией ОО, представленного для оценки может быть выполнена, в том числе, следующими методами:

- сравнение контрольных сумм фактической реализации ОО, полученной в процессе выполнения преобразования, с реализацией ОО, представленного для оценки;

- сравнение двоичного кода фактической реализации ОО, полученной в процессе выполнения преобразования, с реализацией ОО, представленного для оценки.

ADV_TDS.3 Базовый модульный проект

Зависимости: ADV_FSP.4 Полная функциональная спецификация.

Элементы действий разработчика

ADV_TDS.3.1D Разработчик должен представить проект ОО.

Замечания по применению:

Проектная документация должна предоставлять возможность проведения контроля полноты и корректности реализации функций обеспечения ИБ в реализованных проектных решениях.

При разработке проекта ОО должны учитываться положения руководящего документа РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов», а также ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

ADV_TDS.3.2D Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

Элементы содержания и представления документированных материалов

ADV_TDS.3.1C В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV_TDS.3.2C В проекте должно приводиться описание структуры ОО на уровне модулей.

ADV_TDS.3.3C В проекте должны быть идентифицированы все подсистемы ФБО.

ADV_TDS.3.4C В проекте должно приводиться описание каждой из подсистем ФБО.

ADV_TDS.3.5C В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV_TDS.3.6C В проекте должно быть осуществлено прослеживание подсистем ФБО с модулями ФБО.

ADV_TDS.3.7C В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV_TDS.3.8C В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.

ADV_TDS.3.9C В проекте должен быть описан каждый поддерживающий и не влияющий на выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV_TDS.3.10C В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий оценщика

ADV_TDS.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_TDS.3.1C – ADV_TDS.3.10C.

ADV_TDS.3.2E Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

Работы оценки

Оценщик должен выполнить действия по оценке в соответствии с пунктом 10.8.3 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ADV_TDS_EXT.3 Разработка, уточнение и анализ архитектуры программного обеспечения ОО

Зависимости: ADV_TDS.3 Базовый модульный проект

Элементы действий разработчика

ADV_TDS_EXT.3.1D Разработчик должен определить требования безопасности к принципам проектирования архитектуры ПО, направленным на снижение количества возможных недостатков в разрабатываемом ПО.

ADV_TDS_EXT.3.2D Разработчик должен выполнить первичное проектирование архитектуры ПО.

ADV_TDS_EXT.3.3D Разработчик должен установить критерии необходимости уточнения архитектуры ПО.

ADV_TDS_EXT.3.4D Разработчик должен выполнять уточнение архитектуры ПО в процессе разработки кода и его изменений с установленной периодичностью или при наступлении определенных событий.

Элементы содержания и представления документированных материалов

ADV_TDS_EXT.3.1C Требования к принципам проектирования архитектуры ПО должны содержать информацию, позволяющую на начальном этапе проектирования ПО получить представление о принятых подходах и принципах проектирования архитектуры ПО (например, инкапсуляция, уникальность, разделение задач, применение заимствованных компонентов и т.п.), в том числе с точки зрения безопасности («нулевое доверие», «протоколирование событий», «резервное копирование», «формирование перечня недопустимых событий», «приоритетное использование языков с безопасной моделью памяти» и т.п.).

ADV_TDS_EXT.3.2C Описание архитектуры ПО должно включать, как минимум, следующую информацию:

- назначение ПО и сценарии его использования;
- описание среды функционирования;
- ограничения и указания по применению;
- проект ПО на уровне подсистем (модулей), включающий описание их назначения, структуры, особенностей реализации, применяемых языков программирования, взаимодействия друг с другом и другим ПО с указанием соответствующих интерфейсов, сетевых портов, протоколов.

ADV_TDS_EXT.3.3C Критерии необходимости уточнения архитектуры ПО должны содержать информацию о периодичности пересмотра (уточнения) архитектуры ПО в процессе

разработки ПО или о событиях, при наступлении которых необходимо уточнять архитектуру ПО.

ADV_TDS_EXT.3.4C Архитектура ПО, уточненная по результатам выполнения требования ADV_TDS_EXT.3.4D, должна содержать информацию об особенностях реализации ПО в процессе разработки ПО, принятых решениях по корректировкам архитектурных решений в процессе разработки, в том числе связанных с безопасностью, и причинах, их вызвавших.

Элементы действий оценщика

ADV_TDS_EXT.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_TDS_EXT.3.1C – ADV_TDS_EXT.3.4C.

Работы оценки

Оценщик должен выполнить действия по оценке в соответствии с пунктом 10.8.3 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.2. Руководства (AGD)

AGD_OPE.1 Руководство пользователя по эксплуатации

Зависимости: ADV_FSP.1 Базовая функциональная спецификация.

Элементы действий разработчика

AGD_OPE.1.1D Разработчик должен представить руководство пользователя по эксплуатации.

Элементы содержания и представления документированных материалов

AGD_OPE.1.1C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений.

AGD_OPE.1.2C В руководстве пользователя по эксплуатации в рамках каждой пользовательской роли должно быть представлено описание принципов безопасной работы с предоставленными в ОО интерфейсами.

AGD_OPE.1.3C В руководстве пользователя по эксплуатации должно быть представлено описание доступных для каждой пользовательской роли функций и интерфейсов, особенно всех параметров безопасности под управлением пользователя, с указанием безопасных значений, если это уместно.

AGD_OPE.1.4C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть четкое представление каждого типа имеющих значение для безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением ФБО.

AGD_OPE.1.5C В руководстве пользователя по эксплуатации должны быть идентифицированы все возможные режимы работы ОО (включая операции после сбоев и ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования.

AGD_OPE.1.6C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть **приведено** описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ**, имеющих отношение к пользователю**.

AGD_OPE.1.7C Руководство пользователя по эксплуатации должно быть четким и обоснованным.

AGD_OPE.1.8C Руководство пользователя по эксплуатации должно содержать описание состава функций безопасности в привязке к компонентам ОО.

AGD_OPE.1.9C Руководство пользователя по эксплуатации должно содержать типовые параметры настройки ОО (стандарты конфигурации), обеспечивающие безопасное функционирование ОО в установленных средах и режимах функционирования.

AGD_OPE.1.10C Руководство пользователя по эксплуатации должно содержать параметры настройки ОО, устанавливаемые по умолчанию, при которых пользователю будет предоставляться только ограниченная функциональность ОО. Параметры, определяющие защиту ОО от несанкционированного доступа, должны по умолчанию устанавливаться такими, которые будут обеспечивать требуемый уровень защиты от НСД.

AGD_OPE.1.11C Руководство пользователя по эксплуатации должно содержать описание правил использования функций безопасности ОО, включая правила обновления, управления и контроля их применения, в том числе параметров их настройки.

AGD_OPE.1.12C Руководство пользователя по эксплуатации должно содержать перечень и эталонные значения конфигурационных параметров, а также описание процедур контроля соответствия фактических значений параметров конфигурации их эталонным значениям.

AGD_OPE.1.13C В руководстве пользователя по эксплуатации должны быть определены требования к кадровому обеспечению подсистемы ИБ.

AGD_OPE.1.14C В руководстве пользователя по эксплуатации должны быть определены требования по назначению ролей эксплуатационного персонала и его обучению, информированию и повышению осведомленности эксплуатационного персонала и пользователей, необходимых к проведению для обеспечения развертывания и эксплуатации подсистемы ИБ.

AGD_OPE.1.15C В руководстве пользователя по эксплуатации должно быть регламентировано использование компонентов ОО на стороне клиента:

- порядок реализации мер, принимаемых для обеспечения целостности ППО и компонентов ОО, передаваемых на стороне клиента;
- требования к составу, версиям, обновлению и настройкам технических защитных мер, применяемых на стороне клиента.

AGD_OPE.1.1**6**C В руководстве пользователя по эксплуатации должны быть определены требования к использованию функции расширенного аудита, указанию порядка переключения режима аудита, контролю переключения режима аудита.

Элементы действий оценщика

AGD_OPE.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AGD_OPE.1.1C – AGD_OPE.1.16C.

Работы оценки

Оценщик должен выполнить действия по оценке в соответствии с пунктом 11.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

AGD_OPE_EXT.1 Правила кодирования

Зависимости: отсутствуют

Элементы действий разработчика

AGD_OPE_EXT.1.1D Разработчик должен принять и использовать в процессе разработки кода ПО регламент оформления исходного кода и безопасного кодирования для используемых разработчиком языков программирования.

Замечание по применению.

Под безопасным кодированием здесь и далее понимаются практики разработки ПО в соответствии с предъявляемыми

в указанном выше регламенте требованиями по безопасности.

AGD_OPE_EXT.1.2D Разработчик должен учитывать при разработке регламента оформления исходного кода и безопасного кодирования примеры опасных и безопасных конструкций для используемых в ПО языков программирования.

AGD_OPE_EXT.1.3D Разработчик должен учитывать при разработке регламента оформления исходного кода и безопасного кодирования общепринятые стандарты и рекомендации разработчиков (экспертов, специалистов) для соответствующих языков программирования.

AGD_OPE_EXT.1.4D Разработчику рекомендуется при разработке ПО использовать программные средства автоматической проверки правил кодирования.

Элементы содержания и представления документированных материалов

AGD_OPE_EXT.1.1C Регламент оформления исходного кода и безопасного кодирования должен содержать информацию о способах оформления исходного кода.

AGD_OPE_EXT.1.2C Регламент оформления исходного кода и безопасного кодирования должен содержать перечень запрещенных способов кодирования, конструкций и т.п. (например, указание паролей в исходном коде ПО в явном виде, использование «магических чисел» и т.п.).

AGD_OPE_EXT.1.3C Регламент оформления исходного кода и безопасного кодирования должен содержать примеры опасных и безопасных конструкций для используемых языков программирования.

AGD_OPE_EXT.1.4C Регламент оформления исходного кода и безопасного кодирования должен содержать область применения правил кодирования.

AGD_OPE_EXT.1.5C Регламент оформления исходного кода и безопасного кодирования должен содержать порядок проверки выполнения правил кодирования для вносимых изменений в исходный код ПО.

AGD_OPE_EXT.1.6C Регламент оформления исходного кода и безопасного кодирования должен содержать рекомендации разработчиков языков программирования по использованию стандартов кодирования (языков программирования, в т.ч. собственной разработки), принятые разработчиком ПО.

Элементы действий оценщика

AGD_OPE_EXT.1.1E Оценщик должен подтвердить, что регламент, представленный заявителем, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AGD_OPE_EXT.1.1C – AGD_OPE_EXT.1.6C.

Работы оценки

Оценщик должен выполнить действия по оценке в соответствии с пунктом 11.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

AGD_PRE.1 Подготовительные процедуры

Зависимости: отсутствуют.

Элементы действий разработчика

AGD_PRE.1.1D Разработчик должен предоставить ОО вместе с подготовительными процедурами.

Элементы содержания и представления документированных материалов

AGD_PRE1.1C В подготовительных процедурах должны описываться все шаги, необходимые для безопасной приемки поставленного ОО в соответствии с процедурами поставки заявителя (разработчика, производителя).

AGD_PRE1.2C В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки и настройки ОО и безопасной подготовки среды функционирования в соответствии с целями безопасности для среды функционирования, описанными в ЗБ.

AGD_PRE1.3C В подготовительных процедурах должны описываться все необходимые шаги для контроля корректности версий и целостности ОО.

Элементы действий оценщика

AGD_PRE.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AGD_PRE1.1C и AGD_PRE1.3C.

AGD_PRE.1.2E Оценщик должен использовать подготовительные процедуры для подтверждения того, что ОО может быть безопасно подготовлен к работе.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 11.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.3. Поддержка жизненного цикла (ALC)

ALC_CMC.4 Поддержка генерации, процедуры приемки и автоматизация

Управление конфигурацией – один из способов увеличения доверия к тому, что ОО соответствует ФТБ. УК устанавливает это посредством предъявления требований к организационному порядку и управлению процессами усовершенствования и модификации ОО и связанной с ним информации. Системы УК реализуются для того, чтобы удостовериться в целостности частей ОО, подвергающихся контролю со стороны этих систем, путем отслеживания любых изменений, а также обеспечения санкционированности всех изменений.

Зависимости: ALC_CMS.1 Охват УК ОО;

ALC_DVS.1 Идентификация мер безопасности;

ALC_LCD.1 Определенная разработчиком модель жизненного цикла.

Элементы действий разработчика

ALC_CMC.4.1D Разработчик должен предоставить ОО и маркировку для ОО.

ALC_CMC.4.2D Разработчик должен предоставить документацию УК.

ALC_CMC.4.3D Разработчик должен использовать систему УК.

Элементы содержания и представления документированных материалов

ALC_CMC.4.1C ОО должен быть помечен уникальной маркировкой.

ALC_CMC.4.2C В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации **(в том числе файлов исходного кода, ресурсных файлов, файлов документации)**.

ALC_CMC.4.3C В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.

ALC_CMC.4.4C В системе УК должны быть предусмотрены такие автоматизированные меры, при применении которых в элементы конфигурации могут быть внесены только санкционированные изменения.

ALC_CMC.4.5C Система УК должна поддерживать производство ОО автоматизированными средствами.

ALC_CMC.4.6C Документация УК должна включать в себя план УК.

ALC_CMC.4.7C В плане УК должно быть описание того, каким образом система УК используется для разработки ОО.

ALC_CMC.4.8C План УК должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации.

ALC_CMC.4.9C В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.

ALC_CMC.4.10C В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.

Элементы действий оценщика

ALC_CMC.4.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию

и представлению документированной информации, изложенным в ALC_CMC.4.1C – ALC_CMC.4.10C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 12.2.4 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_CMS.4 Охват УК отслеживания проблем

Компонент ALC_CMS.4 содержит требование о том, что недостатки безопасности должны быть включены в список элементов конфигурации и, следовательно, должны находиться под УК в соответствии с требованиями УК семейства ALC_CMC «Возможности УК». Согласно этому требованию должно обеспечиваться сопровождение не только детальной информации о возникавших ранее недостатках и методах их устранения, но и об имеющихся в настоящий момент недостатках безопасности.

Включение недостатков безопасности в контроль системы УК не позволяет пропустить или проигнорировать сообщения о недостатках защиты, давая возможность разработчику отслеживать недостатки безопасности вплоть до их устранения.

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_CMS.4.1D Разработчик должен представить список элементов конфигурации для ОО.

Элементы содержания и представления документированных материалов

ALC_CMS.4.1C Список элементов конфигурации должен включать следующее: сам ОО; свидетельства оценки, необходимые по требованиям доверия к безопасности; представление реализации; сведения о недостатках безопасности и стадии их устранения.

ALC_CMS.4.2C Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

ALC_CMS.4.3C Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.

Элементы действий оценщика

ALC_CMS.4.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_CMS.4.1C – ALC_CMS.4.3C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 12.3.4 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_DEL.1 Процедуры поставки

Требования к поставке предусматривают такие средства и процедуры системы контроля и распространения, которые конкретизируют меры, необходимые для обеспечения доверия к тому, что безопасность ОО поддерживается во время передачи ОО пользователю.

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_DEL.1.1D Разработчик должен задокументировать процедуры поставки ОО или его частей потребителю.

ALC_DEL.1.2D Разработчик должен использовать процедуры поставки.

Элементы содержания и представления документированных материалов

ALC_DEL.1.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержания безопасности при распространении версий ОО потребителю.

Замечания по применению:

В процедурах поставки должны затрагиваться следующие вопросы:

а) обеспечение точного соответствия между ОО, полученным потребителем, и прошедшим оценку ОО;

б) избежание/обнаружение какой-либо подделки актуальной версии ОО;

в) предотвращение поставки фальсифицированной версии ОО;

г) избежание нежелательной утечки информации о распространении ОО потребителю; возможны случаи, при которых потенциальным нарушителям не следует знать о том, когда и каким образом поставляется ОО;

д) избежание/обнаружение перехвата ОО во время поставки;

е) избежание задержки поставки или невыполнения поставки ОО.

Элементы действий оценщика

ALC_DEL.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DEL.1.1C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 12.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_DEL_EXT.1 Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок

Зависимости: ADV_TDS.3 Базовый модульный проект, ALC_DVS_EXT.1 Моделирование угроз и разработка описания поверхности атаки.

Элементы действий разработчика

ALC_DEL_EXT.1.1D Разработчик должен осуществлять контроль зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков; компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков).

ALC_DEL_EXT.1.2D Разработчик должен осуществлять контроль договорных обязательств со сторонними поставщиками.

ALC_DEL_EXT.1.3D Разработчик должен осуществлять выявление элементов инфраструктуры разработчика, воздействие на которые может повлиять на возникновение недекларированных возможностей в ПО.

ALC_DEL_EXT.1.4D Разработчик должен осуществлять контроль использования предсобранного поставщиком ПО (кода, для которого отсутствуют исходные тексты).

ALC_DEL_EXT.1.5D Разработчик должен осуществлять анализ кода ПО, полученного через цепочки поставок, на предмет внедрения вредоносного программного обеспечения.

Элементы содержания и представления документированных материалов

ALC_DEL_EXT.1.1C Перечень процессов, компонентов инфраструктуры, частей разрабатываемого ПО, зависящих от сторонних поставщиков, должен содержать следующие сведения:

- описание внутренних процессов, зависящих от сторонних поставщиков;
- описание компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков;
- описание компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков.

ALC_DEL_EXT.1.2C Сведения о договорных обязательствах со сторонними поставщиками могут включать следующую информацию:

- перечень поставщиков с указанием поставляемых продуктов (услуг);
- сведения о заключенных договорах со сторонними поставщиками, включающие информацию о поставляемых продуктах (услугах), сроках начала и окончания договоров, иную информацию.

ALC_DEL_EXT.1.3C Сведения о критичных и вероятных с точки зрения внедрения недекларированных возможностей элементах инфраструктуры (компонентах инфраструктуры разработки ПО, зависящих от сторонних поставщиков) должны содержать следующую информацию:

- перечень элементов инфраструктуры разработчика, воздействие на которые может повлиять на возникновение недекларированных возможностей в ПО;
- информацию о поставщиках продуктов (услуг) для указанных в перечне элементов инфраструктуры разработчика.

ALC_DEL_EXT.1.4C Результаты контроля использования предсобранного поставщиком ПО должны содержать информацию, позволяющую определить наличие предсобранных поставщиком ПО компонентов и осуществить их идентификацию (по свойствам файлов, контрольным суммам файлов и т.п.).

ALC_DEL_EXT.1.5C Результаты анализа кода ПО, полученного через цепочки поставок, на предмет внедрения вредоносного программного обеспечения должны содержать, как минимум, отчеты сканирования средств антивирусной защиты.

Элементы действий оценщика

ALC_DEL_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DEL_EXT.1.1C - ALC_DEL_EXT.1.5C.

Работы оценки

Оценщик должен выполнить действия по оценке в соответствии с пунктом 12.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_DVS.1 Идентификация мер безопасности

Безопасность разработки связана с физическими, процедурными, организационными и другими мерами безопасности, которые могут применяться в среде разработки для защиты ОО и его частей. К этому относится и физическая защита места разработки и любые процедуры, связанные с отбором персонала, занимающегося разработкой.

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_DVS.1.1D Разработчик должен представить документацию по безопасности разработки.

Элементы содержания и представления документированных материалов

ALC_DVS.1.1C Документация по безопасности разработки должна содержать описание всех физических, процедурных, организационных и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.

ALC_DVS.1.2C Для противодействия угрозам разработчик должен принять и задокументировать меры защиты, включающие:

а) обеспечение контроля физического доступа к средствам вычислительной техники, используемым на этапах

разработки и тестирования ОО;

б) выделение сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые на этапе разработки ОО специализированных банковских приложений (специализированного ПО) финансовых организаций;

в) выделение сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые на этапе тестирования ОО специализированных банковских приложений (специализированного ПО) финансовых организаций;

г) организацию и контроль изоляции и информационного взаимодействия сегмента разработки, сегмента тестирования и сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые для реализации банковских технологических процессов, технологических процессов финансовой организации;

д) управление доступом к ресурсам, средствам разработки и тестирования ОО специализированных банковских приложений (специализированного ПО) финансовых организаций, в том числе исходным файлам;

е) регистрацию и контроль действий с исходными файлами ОО специализированных банковских приложений (специализированного ПО) финансовых организаций;

ж) организацию антивирусной защиты;

з) контроль использования коммуникационных портов средств вычислительной техники.

Элементы действий оценщика

ALC_DVS.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS.1.1C.

ALC_DVS.1.2E Оценщик должен подтвердить, что меры безопасности применяются **и направлены на снижение вероятности возникновения в ОО уязвимостей и других недостатков**.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 12.5.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_DVS_EXT.1 Моделирование угроз и разработка описания поверхности атаки

Зависимости: ALC_DVS.1 Идентификация мер безопасности.

Элементы действий разработчика

ALC_DVS_EXT.1.1D Разработчик должен выполнить первичное моделирование угроз для ПО (разработать модель угроз безопасности информации ОО); для выявленных угроз безопасности информации составить перечень мер по их нейтрализации (снижению вероятности возникновения).

ALC_DVS_EXT.1.2D Разработчик должен выполнить первичное описание поверхности атаки.

ALC_DVS_EXT.1.3D Разработчик должен сформировать перечень целей (функциональных подсистем, модулей (компонентов) ПО и их интерфейсов) для проведения дальнейших исследований безопасности ПО (например, фаззинг-тестирования) с учетом архитектуры ПО, результатов моделирования угроз и выполнения анализа поверхности атаки.

ALC_DVS_EXT.1.4D Разработчик должен выполнять уточнение модели угроз ПО для изменяемого в ходе разработки ПО кода с определенной периодичностью или при наступлении определенных событий.

ALC_DVS_EXT.1.5D Разработчик должен выполнять уточнение описания поверхности атаки для изменяемого в ходе разработки ПО кода с определенной периодичностью или при наступлении определенных событий.

ALC_DVS_EXT.1.6D Разработчик должен при уточнении описания поверхности атаки выполнять анализ поверхности атаки методом идентификации интерфейсов ПО.

Замечание по применению.

Используемые методы анализа сетевых интерфейсов способствуют получению информации об узлах сети, именах устройств, IP-адресах, операционных системах, запущенных программах и службах, именах пользователей, группах и открытых портах и могут включать анализ локальных и сетевых интерфейсов взаимодействия пользователя с ПО (модулями ПО, компонентами ПО) и взаимодействий модулей (компонентов) ПО между собой, средой функционирования и внешними объектами при их наличии.

ALC_DVS_EXT.1.7D Разработчик должен уточнять перечень целей (функциональных подсистем, модулей (компонентов) ПО и их интерфейсов) для проведения дальнейших исследований безопасности ПО (например, фаззинг-тестирования) с учетом уточненной архитектуры ПО, результатов моделирования угроз и выполнения анализа поверхности атаки для разработанного кода ПО.

Элементы содержания и представления документированных материалов

ALC_DVS_EXT.1.1C Модель угроз безопасности информации ОО должна включать совокупность угроз безопасности, актуальных для разрабатываемого ПО. Каждая угроза безопасности представляется в виде совокупности свойств (характеристик), включающей, как минимум, краткое описание угрозы, предполагаемый объект воздействия и возможные последствия реализации угрозы.

Замечание по применению.

При составлении перечня угроз безопасности и их описания рекомендуется учитывать положения ГОСТ Р 58412-2019, а также угрозы безопасности информации Банка данных угроз безопасности информации ФСТЭК России, других источников В модели угроз рекомендуется указывать использованную при моделировании методологию, в том числе в случае ее собственной разработки.

ALC_DVS_EXT.1.2C Перечень мер по нейтрализации (снижению вероятности возникновения) угроз безопасности информации содержит перечень необходимых действий (доработок ПО, иных мер). Перечень мер по нейтрализации (снижению вероятности возникновения) угроз безопасности информации должен быть приоритизирован с точки зрения критичности возможного ущерба от реализации угроз безопасности информации.

ALC_DVS_EXT.1.3C Описание поверхности атаки должно включать совокупность потенциальных областей воздействия на информационную (автоматизированную) систему с использованием разрабатываемого ПО, которые могут быть использованы нарушителем для проведения компьютерной атаки. Описание поверхности атаки может быть частью модели угроз.

ALC_DVS_EXT.1.4C Перечень целей должен включать список функциональных подсистем, модулей (компонентов) ПО и их интерфейсов, составляющих поверхность атаки, подлежащих дополнительному анализу с точки зрения безопасности.

ALC_DVS_EXT.1.5C Модель угроз безопасности информации ОО должна дополнительно (в случае применимости) содержать угрозы безопасности ПО, актуальные для выполненных изменений.

ALC_DVS_EXT.1.6C Описание поверхности атаки должно включать перечень функциональных подсистем, модулей (компонентов) ПО и их интерфейсов, составляющих поверхность атаки, актуальных для разработанного кода ПО.

ALC_DVS_EXT.1.7C Перечень целей для проведения дальнейших исследований безопасности ПО должен содержать описание функциональных подсистем, модулей (компонентов) ПО, их интерфейсов, для которых предполагаются дальнейшие исследования в части безопасности при реализации других процессов РБПО.

Элементы действий оценщика

ALC_DVS_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS_EXT.1.1C - ALC_DVS_EXT.1.7C.

Работы оценки

Оценщик должен выполнить действия по оценке в соответствии с пунктом 12.5.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_DVS_EXT.2 Обеспечение безопасности сборочной среды программного обеспечения

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_DVS_EXT.2.1D Разработчик должен разработать регламент обеспечения безопасности сборочной среды.

ALC_DVS_EXT.2.2D Разработчик должен зафиксировать описание ожидаемых результатов сборки ПО, прав доступа к среде

сборки ПО и хранилищу результатов сборки ПО и ролей пользователей, участвующих в процессе сборки ПО.

ALC_DVS_EXT.2.3D Разработчик должен разработать схему сборочной среды.

ALC_DVS_EXT.2.4D Разработчик должен обеспечивать регистрацию всех выполняемых действий при сборке ПО в журналах аудита; журналы аудита должны храниться способом, обеспечивающим их целостность; сроки хранения журналов аудита должны быть зафиксированы в регламенте обеспечения безопасности сборочной среды

ALC_DVS_EXT.2.5D Разработчик должен обеспечивать хранение результатов сборки ПО в выделенном хранилище – хранилище результатов сборки ПО.

ALC_DVS_EXT.2.6D Разработчик должен обеспечивать повторяемость сборки ПО (если применимо).

Замечание по применению

Под повторяемостью сборки имеется в виду обеспечение предсказуемости результатов сборок, обеспечение полного бинарного соответствия результатов повторных сборок не требуется.

ALC_DVS_EXT.2.7D Разработчик должен обеспечивать управление доступом к среде сборки ПО и хранилищу результатов сборки ПО на основе ролей пользователей.

ALC_DVS_EXT.2.8D Разработчик должен обеспечивать защиту каналов связи с внешними источниками данных для обеспечения конфиденциальности информации, обрабатываемой в сборочной среде.

Элементы содержания и представления документированных материалов

ALC_DVS_EXT.2.1C Регламент обеспечения безопасности сборочной среды должен содержать следующие сведения:

- обязанности сотрудников и их роли при проведении сборок ПО;
- порядок регистрации событий безопасности при реализации сборок ПО в журналах аудита;
- сроки хранения журналов аудита;
- описание мер безопасности, необходимых для реализации в сборочной среде.

ALC_DVS_EXT.2.2C Информация о безопасности сборочной среды должна содержать:

- описание ожидаемых результатов сборки ПО;
- описание прав доступа к сборочной среде и хранилищу результатов сборки ПО, а также ролей пользователей, участвующих в процессе сборки ПО.

ALC_DVS_EXT.2.3C Схематическое изображение сборочной среды должно содержать:

- элементы сборочной среды (серверы, узлы, виртуальные узлы, элементы среды контейнеризации и т.п.);
- связи между элементами сборочной среды, позволяющие отследить порядок (очередность) выполнения сборочных действий;
- компоненты сборочной среды, реализующие отдельные функции, в том числе меры безопасности

(средства защиты информации, инструменты статического анализа и др.).

ALC_DVS_EXT.2.4C Журналы аудита процессов сборки ПО должны содержать следующую информацию:

- дату и время начала и завершения сборки ПО;
- информацию о версии собираемого ПО (модуля ПО, компонента ПО);
- информацию об используемой конфигурации сборки ПО;
- информацию о шагах сборки ПО;
- информацию о событиях безопасности в соответствии с регламентом обеспечения безопасности сборочной среды.

ALC_DVS_EXT.2.5C В качестве артефакта реализации требований, подтверждающих хранение результатов сборки ПО в выделенном хранилище, может использоваться журнал аудита сборки ПО, в котором указано место сохранения собранного модуля (компонента) ПО, результаты контрольного суммирования файлов, скачанных из хранилища результатов сборки ПО, и последующего сравнения их с контрольными суммами, указанными в журнале аудита сборки ПО или в графическом интерфейсе системы хранения результатов сборки ПО.

ALC_DVS_EXT.2.6C В качестве артефактов реализации требований, подтверждающих повторяемость сборки ПО, могут использоваться журналы аудита выполненных сборок, сравненные друг с другом; результаты контрольного суммирования файлов, полученных при разных запусках сборок, и последующего их сравнения (по контрольным

суммам, по бинарному представлению, по наименованию и размеру и др.).

Элементы действий оценщика

ALC_DVS_EXT.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS_EXT.2.6C.

Работы оценки

Оценщик должен выполнить действия по оценке в соответствии с пунктом 12.5.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_DVS_EXT.3 Управление доступом и контроль целостности кода при разработке программного обеспечения

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_DVS_EXT.3.1D Разработчик должен разработать регламент доступа к исходному коду ПО и обеспечения его целостности.

Замечание по применению

При разработке и реализации регламента доступа к исходному коду ПО рекомендуется руководствоваться принципами минимизации привилегий и разделения полномочий.

ALC_DVS_EXT.3.2D Разработчик должен осуществлять управление доступом к исходному коду ПО на основе выбранной модели управления доступом.

ALC_DVS_EXT.3.3D Разработчик должен осуществлять контроль целостности собственного исходного кода.

Элементы содержания и представления документированных материалов

ALC_DVS_EXT.3.1C Регламент доступа к исходному коду ПО и обеспечения его целостности должен содержать следующие сведения:

- обязанности сотрудников, их права и роли при разработке ПО;
- правила хранения исходного кода ПО, включая правила резервного копирования исходного кода ПО;
- правила внесения изменений (модификации, добавления, удаления) в исходный код ПО;
- критерии выбора способов и инструментов контроля целостности ПО;
- критерии выбора модулей (компонентов) ПО, подлежащих контролю целостности;
- описание процедуры контроля целостности исходного кода ПО.

ALC_DVS_EXT.3.2C Описание модели управления доступом к исходному коду ПО должно включать:

- перечень сотрудников, их права и обязанности при разработке ПО;
- описание выбранной модели управления доступом и используемых инструментов управления доступом.

ALC_DVS_EXT.3.3C Результаты выполнения контроля целостности собственного исходного кода должны обеспечивать соответствие требованиям регламента доступа к исходному коду ПО и обеспечения его целостности и позволять сделать однозначный вывод о целостности собственного исходного кода.

Элементы действий оценщика

ALC_DVS_EXT.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS_EXT.3.1C - ALC_DVS_EXT.3.3C.

Работы оценки

Оценщик должен выполнить действия по оценке в соответствии с пунктом 12.5.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_FLR.2 Процедуры сообщений о недостатках

В процедурах устранения недостатков следует описать методы реагирования на все типы выявленных недостатков. Об этих недостатках могут сообщить разработчик ОО, пользователи ОО, другие стороны, знакомые с ОО. Некоторые недостатки не могут быть исправлены немедленно. Не исключено, что недостаток вообще не может быть исправлен, и необходимо применить другие (например, процедурные) меры. В представленной документации следует охватывать процедуры по обеспечению исправлений в местах эксплуатации, а также предоставлять информацию о недостатках, для

которых исправление отложено или невозможно (с описанием того, что следует делать в этой ситуации).

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_FLR.2.1D Разработчик должен предоставить процедуры устранения недостатков, предназначенные для заявителей (разработчиков, производителей) ОО.

ALC_FLR.2.2D Разработчик должен установить процедуру получения и отработки всех сообщений пользователей о недостатках безопасности и запросов на исправление этих недостатков.

ALC_FLR.2.3D Разработчик должен предоставить руководство по устранению недостатков, предназначенное для пользователей ОО.

Элементы содержания и представления документированных материалов

ALC_FLR.2.1C Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

ALC_FLR.2.2C Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.

ALC_FLR.2.3C Процедуры устранения недостатков должны содержать требование к тому, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.

ALC_FLR.2.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

ALC_FLR.2.5C Процедуры устранения недостатков должны описывать средства, посредством которых разработчик получает от пользователей ОО сообщения и запросы о предполагаемых недостатках безопасности в ОО.

ALC_FLR.2.6C Процедуры обработки ставших известными недостатков безопасности должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а для пользователей ОО выпущены процедуры по исправлению.

ALC_FLR.2.7C Процедуры обработки ставших известными недостатков безопасности должны обеспечить такие защитные меры, чтобы любые исправления этих недостатков не приводили к появлению новых недостатков.

ALC_FLR.2.8C Руководство по устранению недостатков должно описывать средства, посредством которых пользователи ОО могут сообщать разработчикам о любых предполагаемых недостатках безопасности в ОО.

Элементы действий оценщика

ALC_FLR.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_FLR.2.1C – ALC_FLR.2.8C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 12.6.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_FPU_EXT.1 Процедуры обновления программного обеспечения

Элементы действий разработчика

ALC_FPU_EXT.1.1D Разработчик должен разработать и реализовать технологию обновления ОО для [**выбор**:

обновление, направленное на устранение уязвимостей ОО;

иное обновление, оказывающее влияние на безопасность ОО;

обновление, не оказывающее влияния на безопасность ОО

].

ALC_FPU_EXT.1.2D Разработчик должен разработать и поддерживать регламент обновления программного обеспечения.

ALC_FPU_EXT.1.3D Разработчик должен разработать и реализовать процедуру уведомления потребителей о выпуске обновлений ОО, основанную на [назначение: *способы уведомления*].

ALC_FPU_EXT.1.4D Разработчик должен разработать и реализовать процедуру предоставления обновлений потребителям ОО, основанную на [назначение: *способы предоставления обновлений*].

ALC_FPU_EXT.1.5D Разработчик должен разработать и реализовать процедуру предоставления обновлений оценщику для проведения внешнего контроля, основанную на [назначение: *способы предоставления обновлений для контроля*].

Элементы содержания и представления документированных материалов

ALC_FPU_EXT.1.1C Документация ОО должна содержать описание технологии выпуска обновлений ОО.

ALC_FPU_EXT.1.2C Документация ОО должна содержать регламент обновления ОО, включающий:

а) идентификацию типов выпускаемых обновлений;

б) описание процедуры уведомления потребителей о выпуске обновлений;

в) описание процедуры предоставления обновлений потребителям;

г) описание содержания эксплуатационной документации на выпускаемые обновления;

д) [назначение: *иная информация*].

ALC_FPU_EXT.1.3C Регламент обновления ОО должен предусматривать включение в эксплуатационную документацию на выпускаемые обновления описания следующих процедур:

а) процедуры получения обновления;

б) процедуры контроля целостности обновления;

в) типовой процедуры тестирования обновления;

г) процедуры установки и применения обновления;

д) процедуры контроля установки обновления;

е) процедуры верификации (проверки) применения обновления.

ALC_FPU_EXT.1.4C Документация процедуры предоставления обновлений для проведения внешнего контроля должна содержать:

а) описание процедуры предоставления обновлений для внешнего контроля;

б) требования к предоставлению и содержанию методики тестирования обновления разработчиком;

в) требования к оформлению и предоставлению результатов тестирования обновления разработчиком;

г) [**назначение**: *иная информация*].

Элементы действий оценщика

ALC_FPU_EXT.1.1E Оценщик должен подтвердить, что информация, предоставленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в ALC_FPU_EXT.1.1C - ALC_FPU_EXT.1.4C.

ALC_FPU_EXT.1.2E Оценщик должен проверить, что процедура предоставления обновлений для проведения внешнего контроля позволяет организовать и проводить их внешний контроль.

Замечания по применению:

В качестве типов обновлений рассматриваются: обновления, направленные на устранение уязвимостей ОО; иные обновления, оказывающие влияние на безопасность ОО; обновления, не оказывающие влияния на безопасность ОО.

ALC_LCD.1 Определенная разработчиком модель жизненного цикла

Модель жизненного цикла объединяет в себе процедуры, инструментальные средства и методы, используемые для разработки и сопровождения ОО. Аспекты процесса, которые могут быть охвачены такой моделью, включают методы проектирования, процедуры просмотра, средства управления проектом, процедуры управления изменениями, методы тестирования и процедуры приемки. Эффективная модель жизненного цикла позволит включить аспекты процесса разработки и сопровождения в общую структуру управления, которая устанавливает обязанности и контролирует ход процессов.

Важно, чтобы модель разработки и сопровождения ОО была установлена как можно раньше в жизненном цикле ОО.

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_LCD.1.1D Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении ОО.

ALC_LCD.1.2D Разработчик должен представить документацию по определению жизненного цикла.

Элементы содержания и представления документированных материалов

ALC_LCD.1.1C Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.

Замечания по применению:

Модель жизненного цикла ОО должна содержать следующие этапы:

1) проектирование;

2) создание и тестирование;

3) приемка и ввод в действие;

4) сопровождение и модернизация;

5) вывод из эксплуатации.

ALC_LCD.1.2C Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением ОО.

Замечания по применению:

На каждом этапе жизненного цикла формируется собственный набор свидетельств доверия, по результатам оценки которых может быть принято решение о полноте и корректности реализации требований к обеспечению ИБ, предъявляемых к ОО.

В качестве документированных материалов рекомендуется рассматривать:

а) регламенты, используемые для организации деятельности по обеспечению ИБ на этапах жизненного цикла ОО:

- регламент приемки ПО, который должен содержать обязанности сотрудников и их роли при проведении приемки ПО, описание типовых сценариев приемки ПО перед предоставлением его пользователям;
- регламент обеспечения целостности ПО, передаваемого пользователям, который должен содержать перечень мер, реализуемых разработчиком ПО с целью обеспечения возможности проверки целостности ПО пользователями, порядок применения мер по обеспечению возможности проверки целостности ПО пользователями, порядок информирования

пользователей ПО о механизмах проверки целостности ПО;

- регламент вывода ПО из эксплуатации, который должен содержать описание условий, при которых ПО (версию ПО) необходимо выводить из эксплуатации, обязанности сотрудников и их роли при осуществлении вывода ПО из эксплуатации ПО и порядок оповещения пользователей о планах прекращения технической поддержки ПО (версии ПО).

б) документированные результаты выполнения деятельности по обеспечению ИБ на этапах жизненного цикла ОО.

На этапе «Приемка и ввод в действие» необходимо проводить анализ степени влияния на безопасность ПО неустраненных ошибок. Информация о неустраненных ошибках выпускаемого ПО должна быть зафиксирована (например, в системе управления изменениями, системе отслеживания ошибок и т.п.).

На этапе «Вывод из эксплуатации» необходимо информировать пользователя о планах прекращения технической поддержки ПО (версии ПО) и своевременно уведомлять об этом.

Элементы действий оценщика

ALC_LCD.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_LCD.1.1C и ALC_LCD.1.2C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 12.7.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_LCD_EXT.3 Определенные разработчиком сроки поддержки

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_LCD_EXT.3.1D Заявитель, разработчик, производитель должны установить в совместной декларации срок [**назначение**: срок], в течение которого они обязуются выполнять все необходимые действия по поддержке ОО, направленные на обеспечение поддержания сертификата соответствия ОО требованиям безопасности информации.

ALC_LCD_EXT.3.2D Заявитель, разработчик, производитель должны обеспечить представление совместной декларации о сроке поддержки ОО вместе с заявкой на сертификацию ОО.

Элементы содержания и представления документированных материалов

ALC_LCD_EXT.3.1C Декларация о сроке поддержки ОО должна содержать план поддержки ОО на весь задекларированный срок, включающий описание всех предпринимаемых действий по обеспечению поддержания сертификата соответствия ОО требованиям безопасности информации.

ALC_LCD_EXT.3.2C Декларация о сроке поддержки ОО должна содержать сведения о поддерживаемой версии ОО.

Элементы действий оценщика

ALC_LCD_EXT.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_LCD_EXT.3.1C и ALC_LCD_EXT.3.2C.

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Данные требования связаны с выбором инструментальных средств, используемых для разработки, анализа и реализации ОО. Они направлены на предотвращение использования плохо определенных, несогласованных или неверных инструментальных средств для разработки ОО. Это относится, в частности, к языкам программирования, документации, стандартам реализации и некоторым другим частям ОО, например, вспомогательным динамическим библиотекам.

Полностью определенными называют инструментальные средства, которые полно и четко описаны. Например, принято считать полностью определенными языки программирования и системы автоматизации проектирования (САПР), которые основаны на стандартах, изданных органами по стандартизации. Для средств, разработанных самими разработчиками ОО, потребуется проведение дополнительных исследований для установления того, являются ли они полностью определенными.

Зависимости: ADV_IMP.1 Подмножество реализации ФБО.

Элементы действий разработчика

ALC_TAT.1.1D Разработчик должен идентифицировать каждое инструментальное средство, используемое для разработки **(производства)** ОО.

ALC_TAT.1.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки **(производства)**, обусловленные реализацией.

Элементы содержания и представления документированных материалов

ALC_TAT.1.1C Все инструментальные средства разработки **(производства)**, используемые для реализации, должны быть полностью определены.

ALC_TAT.1.2C В документации по инструментальным средствам разработки **(производства)** должны быть однозначно определены значения всех языковых конструкций, используемых в реализации.

ALC_TAT.1.3C В документации по инструментальным средствам разработки **(производства)** должны быть однозначно определены значения всех опций, обусловленных реализацией**, методы, приемы и правила эксплуатации средств разработки (производства) при создании (производстве) ОО**.

ALC_TAT.1.4C Должны иметься и поддерживаться лицензии (права) на все инструментальные средства разработки.

Элементы действий оценщика

ALC_TAT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_TAT.1.1C – ALC_TAT.1.4C.

Работы оценки

1. Оценщик должен выполнить действия в соответствии с пунктом 12.8.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045

«Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

2. Оценщик должен исследовать представленную документацию инструментальных средств разработки, чтобы сделать заключение о том, что для представления реализации представлено четкое и полное описание синтаксиса и детальное описание семантики каждой из языковых конструкций. В документации инструментальных средств разработки (например, в спецификациях языка программирования и в руководствах пользователя) должны быть охвачены все конструкции, используемые в представлении реализации ОО, и для каждой такой конструкции должно быть предоставлено четкое и однозначное определение предназначения и результата выполнения этой конструкции.

3. Оценщик должен исследовать представленную документацию инструментальных средств разработки, чтобы сделать заключение о том, что в ней описаны языковые конструкции, определяющие связи функциональных объектов по управлению. В качестве таких языковых конструкций могут выступать прямые вызовы функций с передачей фактических параметров, а также косвенные вызовы функций по указателю, по значениям полей записей, массивов и т.п.

4. Оценщик должен исследовать представленную документацию инструментальных средств разработки, чтобы сделать заключение о том, имеются ли в определении языка программирования проблемные конструкции, которые могут быть применены к информационным объектам. В качестве таких проблемных конструкций могут выступать, например, преобразование информационного объекта из одного типа данных в другой, использование псевдонимов (альтернативных имен, которые позволяют ссылаться на одну и ту же часть памяти различными способами), указателей (ссылок) на произвольные области памяти, использование стека для передачи

фактических параметров между функциональными объектами, динамическое выделение памяти информационным объектам и т.п.

Оценщик должен исследовать представленную документацию инструментальных средств разработки, с тем чтобы определить проблемные конструкции, которые могут вносить уязвимости в ОО или в среду функционирования ОО.

ALC_TAT_EXT.1 Статический анализ исходного кода

Зависимости: ADV_TDS.3 Базовый модульный проект

Элементы действий разработчика

ALC_TAT_EXT.1.1D Разработчик должен разработать регламент проведения статического анализа исходного кода ПО.

ALC_TAT_EXT.1.2D Разработчик должен определить инструменты статического анализа для каждого используемого в ПО языка программирования. Инструменты статического анализа должны реализовывать следующие методы анализа:

- внутрипроцедурный анализ потоков данных и управления;
- межпроцедурный и межмодульный контекстно-чувствительный анализ потока данных;
- чувствительный к путям выполнения анализ потоков данных и управления;
- межпроцедурный и межмодульный контекстно-чувствительный анализ помеченных данных;
- анализ программы на синтаксическом уровне.

ALC_TAT_EXT.1.3D Разработчик должен определить конфигурацию и параметры настройки инструментов статического анализа.

ALC_TAT_EXT.1.4D Разработчик должен проводить статический анализ с использованием инструментов статического анализа с регистрацией всех предупреждений о потенциальных ошибках, полученных по результатам работы инструментов статического анализа.

ALC_TAT_EXT.1.5D Разработчик должен осуществлять пересмотр конфигурации и параметров настройки инструментов статического анализа при выполнении установленных событий (изменениях в правилах сборки, применяемых статических анализаторах, получении информации об уязвимостях и т.п.).

ALC_TAT_EXT.1.6D Разработчик должен осуществлять повторный статический анализ ПО после устранения ранее выявленных ошибок и уязвимостей; внесения изменений в ходе разработки в исходные тексты ПО; изменения используемых версий компиляторов, сред выполнения (для компилируемого в промежуточное представление или интерпретируемого кода), обновлений используемых инструментов статического анализа.

Элементы содержания и представления документированных материалов

ALC_TAT_EXT.1.1C Регламент проведения статического анализа исходного кода ПО должен содержать следующие сведения:

- обязанности сотрудников и их роли при проведении статического анализа;
- критерии выбора инструментов статического анализа;
- критерии выбора ПО (модулей ПО, компонентов ПО, функциональных подсистем ПО), подлежащих проведению статического анализа;

- правила обработки срабатываний средств статического анализа;
- типы и критичность ошибок (уязвимостей), выявляемых статическим анализатором, подлежащих устранению, и приоритеты устранения ошибок (уязвимостей);
- периодичность проведения статического анализа или события, при наступлении которых необходимо выполнять повторный статический анализ;
- критерии пересмотра конфигурации и параметров настройки инструментов статического анализа.

ALC_TAT_EXT.1.2C Перечень инструментов статического анализа должен включать наименования инструментов статического анализа, их версии и информацию о соответствии используемым языкам программирования.

ALC_TAT_EXT.1.3C Конфигурации и параметры настройки инструментов статического анализа должны обеспечивать выполнение требований регламента проведения статического анализа в части выявления типов и критичности ошибок (уязвимостей), периодичности проведения статического анализа или событий, при наступлении которых необходимо выполнять повторный статический анализ.

ALC_TAT_EXT.1.4C Отчеты по результатам проведения статического анализа должны включать:

- срабатывания инструментов статического анализа;
- результаты анализа (разметки) выявленных ошибок (срабатываний статического анализатора);
- перечень предупреждений о найденных ошибках;
- описание ошибок;

- тип ошибок;
- место в исходном коде программы, где найдены ошибки.

ALC_TAT_EXT.1.5C Конфигурации и параметры настройки инструментов статического анализа должны обеспечивать выполнение требований регламента проведения статического анализа в части выполнения критериев их пересмотра.

Элементы действий оценщика

ALC_TAT_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_TAT_EXT.1.1C - ALC_TAT_EXT.1.5C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 12.8.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ALC_TAT_EXT.2 Динамический анализ кода программы

Зависимости: ADV_TDS.3 Базовый модульный проект, ALC_DVS_EXT.1 Моделирование угроз и разработка описания поверхности атаки.

Элементы действий разработчика

ALC_TAT_EXT.2.1D Разработчик должен разработать регламент проведения динамического анализа кода ПО.

ALC_TAT_EXT.2.2D Разработчик должен определить инструменты динамического анализа и фаззинг-тестирования, порядок их применения.

ALC_TAT_EXT.2.3D Разработчик должен определить перечень модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование.

ALC_TAT_EXT.2.4D Разработчик должен определить сценарии проведения тестирования для каждого исследуемого модуля (компонента) ПО средствами динамического анализа, включая инструменты проведения фаззинг-тестирования.

ALC_TAT_EXT.2.5D Разработчик должен проводить динамический анализ кода программы с использованием инструментов динамического анализа.

ALC_TAT_EXT.2.6D Разработчик должен проводить повторный динамический анализ модулей (компонентов) ПО с целью контроля устранения ошибок.

ALC_TAT_EXT.2.7D Разработчик должен проводить мутационное фаззинг-тестирование с обратной связью..

ALC_TAT_EXT.2.8D При проведении фаззинг-тестирования использовать тестовые коллекции входных данных, подлежащие дальнейшим мутациям, для каждого из подвергаемых фаззинг-тестированию модуля (компонента) ПО (при использовании инструментов выполнения фаззинг-тестирования, использующих коллекции входных данных), вызывающие использование различных функциональных возможностей тестируемого модуля (компонента) ПО.

ALC_TAT_EXT.2.9D Разработчик должен устранять выявленные в процессе динамического анализа, включая фаззинг-тестирование, ошибки в соответствии с принятыми процедурами устранения найденных средствами динамического анализа ошибок

Элементы содержания и представления документированных материалов

ALC_TAT_EXT.2.1C Регламент проведения динамического анализа кода ПО должен содержать следующие сведения:

- обязанности сотрудников и их роли при проведении динамического анализа и фаззинг-тестирования;
- критерии выбора инструментов динамического анализа, включая инструменты проведения фаззинг-тестирования;
- критерии выбора методов и способов динамического анализа;
- критерии выбора модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование;
- правила обработки срабатываний средств динамического анализа, требующих обработки (аварийная остановка, зависание и т.п.);
- процедуры устранения найденных средствами динамического анализа ошибок;
- периодичность проведения динамического анализа или события, при наступлении которых необходимо выполнять повторный динамический анализ (критерии проведения повторного динамического анализа);
- периодичность проведения фаззинг-тестирования и критерии его завершения.

ALC_TAT_EXT.2.2C Перечень инструментов динамического анализа, включая инструменты проведения фаззинг-тестирования, должен включать:

- наименования инструментов динамического анализа, их версии и их соответствие исследуемым модулям (компонентам) ПО;
- параметры эксплуатации инструментов динамического анализа (для платформ, языков программирования и т.п.).

ALC_TAT_EXT.2.3C Перечень модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование, отвечающий требованиям регламента проведения динамического анализа, отвечающий требованиям регламента проведения динамического анализа, должен включать:

- наименование модуля (компонента) ПО;
- идентификатор модуля (компонента) ПО.

ALC_TAT_EXT.2.4C Сценарии проведения тестирования для каждого исследуемого модуля (компонента) ПО средствами динамического анализа, включая инструменты проведения фаззинг-тестирования, обеспечивающие выполнение требований регламента проведения динамического анализа, должен включать:

- идентификатор модуля (компонента) ПО;
- наименование используемого инструмента;
- параметры настройки инструмента;
- критерии запуска и остановки тестирования.

ALC_TAT_EXT.2.5C Отчеты по результатам проведения динамического анализа должны включать:

- срабатывания инструментов динамического анализа;
- результаты анализа (обработки) выявленных ошибок (срабатываний динамического анализатора) для определенных регламентом типов ошибок, требующих обработки (аварийная остановка, зависание и т.п.).

ALC_TAT_EXT.2.6C Отчеты по результатам проведения фаззинг-тестирования должны включать:

- сведения о результатах работы инструментов фаззинг-тестирования (длительность проведения фаззинг-тестирования, количество аварийных завершений работы ПО, количество найденных путей выполнения и др.);
- результаты анализа (обработки) аварийных завершений работы ПО, выявленных при проведении фаззинг-тестирования.

Элементы действий оценщика

ALC_TAT_EXT.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS_EXT.2.1C - ALC_DVS_EXT.2.6C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 12.8.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.4. Оценка задания по безопасности (ASE)

ASE_INT.1 Введение Задания по безопасности

Зависимости: отсутствуют.

Элементы действий разработчика

ASE_INT.1.1D Разработчик ЗБ должен представить «Введение ЗБ».

Элементы содержания и представления документированных материалов

ASE_INT.1.1C «Введение ЗБ» должно содержать «Ссылку ЗБ», «Ссылку ОО», «Аннотацию ОО» и «Описание ОО».

ASE_INT.1.2C «Ссылка ЗБ» должна однозначно идентифицировать ЗБ.

ASE_INT.1.3C «Ссылка ОО» должна однозначно идентифицировать ОО.

ASE_INT.1.4C В «Аннотации ОО» должна быть представлена краткая информация об использовании и основных функциональных возможностях безопасности ОО.

ASE_INT.1.5C В «Аннотации ОО» должен быть идентифицирован тип ОО.

ASE_INT.1.6C В «Аннотации ОО» должны быть идентифицированы любые не входящие в ОО аппаратные, программные, а также программно-аппаратные средства, требуемые ОО.

ASE_INT.1.7C «Описание ОО» должно включать описание физических границ ОО.

ASE_INT.1.8C «Описание ОО» должно включать описание логических границ ОО.

Элементы действий оценщика

ASE_INT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_INT.1.1C – ASE_INT.1.8C.

ASE_INT.1.2E Оценщик должен подтвердить, что «Справка ОО», «Аннотация ОО» и «Описание ОО» не противоречат друг другу.

Работы оценки

Оценщик должен выполнять указанные действия в соответствии с пунктом 9.3.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_CCL.1 Утверждения о соответствии

Зависимости: ASE_INT.1 Введение ЗБ;

ASE_ECD.1 Определение расширенных компонентов;

ASE_REQ.1 Установленные требования безопасности.

Элементы действий разработчика

ASE_CCL.1.1D Разработчик должен представить «Утверждения о соответствии».

ASE_CCL.1.2D Разработчик должен представить «Обоснование утверждений о соответствии».

Элементы содержания и представления документированных материалов

ASE_CCL.1.1C В «Утверждения о соответствии» должно быть включено «Утверждение о соответствии ИСО/МЭК 15408», которое

определяет, для какой редакции ГОСТ Р ИСО/МЭК 15408 утверждается соответствие ЗБ и ОО.

ASE_CCL.1.2C В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ЗБ ГОСТ Р ИСО/МЭК 15408-2; ЗБ описывается либо как соответствующее требованиям ГОСТ Р ИСО/МЭК 15408-2, либо как содержащее расширенные по отношению к ГОСТ Р ИСО/МЭК 15408-2 требования.

ASE_CCL.1.3C В «Утверждении о соответствии ИСО/МЭК 15408» должно приводиться описание соответствия ПЗ ГОСТ Р ИСО/МЭК 15408-3; ЗБ описывается либо как соответствующее требованиям ГОСТ Р ИСО/МЭК 15408-3, либо как содержащее расширенные по отношению к ГОСТ Р ИСО/МЭК 15408-3 требования.

ASE_CCL.1.4C «Утверждение о соответствии ИСО/МЭК 15408» должно согласовываться с «Определением расширенных компонентов».

ASE_CCL.1.5C В «Утверждении о соответствии» должны быть идентифицированы все ПЗ и пакеты требований безопасности, о соответствии которым утверждается в ЗБ.

ASE_CCL.1.6C В «Утверждении о соответствии ЗБ пакету требований» должно приводиться описание любого соответствия ЗБ некоторому пакету требований; ЗБ описывается либо как соответствующее пакету требований, либо как содержащее расширенные по отношению к пакету требования.

ASE_CCL.1.7C В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что тип ОО согласуется с типом ОО в тех ПЗ, о соответствии которым утверждается в ЗБ.

ASE_CCL.1.8C В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Определения проблемы безопасности» согласуется с изложением «Определения проблемы безопасности» в тех ПЗ, о соответствии которым утверждается в ЗБ.

ASE_CCL.1.9C В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Целей безопасности» согласуется с изложением «Целей безопасности» в тех ПЗ, о соответствии которым утверждается в ЗБ.

ASE_CCL.1.10C В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Требований безопасности» согласуется с изложением «Требований безопасности» в тех ПЗ, о соответствии которым утверждается в ЗБ.

Элементы действий оценщика

ASE_CCL.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_CCL.1.1C – ASE_CCL.1.10C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 9.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_SPD.1 Определение проблемы безопасности

Зависимости: отсутствуют.

Элементы действий разработчика

ASE_SPD.1.1D Разработчик должен представить «Определение проблемы безопасности».

Элементы содержания и представления документированных материалов

ASE_SPD.1.1C «Определение проблемы безопасности» должно включать в себя описание угроз.

ASE_SPD.1.2C Описание всех угроз должно проводиться в терминах источника угрозы, активов и негативного действия.

ASE_SPD.1.3C В "Определение проблемы безопасности" должно быть включено описание ПБОр.

ASE_SPD.1.4C «Определение проблемы безопасности» должно содержать описание предположений относительно среды функционирования ОО.

Элементы действий оценщика

ASE_SPD.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_SPD.1.1C – ASE_SPD.1.4C.

Работы оценки

Оценщик должен выполнять указанные действия в соответствии с пунктом 9.5.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_OBJ.2 Цели безопасности

Зависимости: ASE_SPD.1 Определение проблемы безопасности.

Элементы действий разработчика

ASE_OBJ.2.1D Разработчик должен предоставить «Определение целей безопасности».

ASE_OBJ.2.2D Разработчик должен предоставить «Обоснование целей безопасности».

Элементы содержания и представления документированных материалов

ASE_OBJ.2.1C Изложение «Целей безопасности» должно включать в себя описание целей безопасности для ОО и для среды функционирования ОО.

ASE_OBJ.2.2C В «Обосновании целей безопасности» каждая цель безопасности для ОО должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, и к политикам безопасности, на осуществление которых направлена эта цель безопасности.

ASE_OBJ.2.3C В «Обосновании целей безопасности» каждая цель безопасности для ОО должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, к политикам безопасности, на осуществление которых направлена эта цель безопасности, а также к предположениям, поддерживаемым данной целью безопасности.

ASE_OBJ.2.4C В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на противостояние всем идентифицированным угрозам.

ASE_OBJ.2.5C В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на осуществление всех политик безопасности.

ASE_OBJ.2.6C В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности для среды функционирования поддерживают все предположения.

Элементы действий оценщика

ASE_OBJ.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_OBJ.2.1C – ASE_OBJ.2.6C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 9.6.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_ECD.1 Определение расширенных компонентов

Зависимости: отсутствуют.

Элементы действий разработчика

ASE_ECD.1.1D Разработчик должен представить изложение «Требований безопасности».

ASE_ECD.1.2D Разработчик должен представить «Определение расширенных компонентов».

Элементы содержания и представления документированных материалов

ASE_ECD.1.1C В изложении «Требований безопасности» должны быть идентифицированы все расширенные требования безопасности.

ASE_ECD.1.2C В «Определении расширенных компонентов» должен определяться расширенный компонент для каждого расширенного требования безопасности.

ASE_ECD.1.3C В «Определении расширенных компонентов» должно указываться, как каждый расширенный компонент связан с существующими компонентами, семействами и классами ГОСТ Р ИСО/МЭК 15408.

ASE_ECD.1.4C В «Определении расширенных компонентов» должны использоваться в качестве модели представления компоненты, семейства, классы и методология ГОСТ Р ИСО/МЭК 15408.

ASE_ECD.1.5C Расширенные компоненты должны состоять из измеримых объективных элементов, чтобы была возможность продемонстрировать соответствие или несоответствие этим элементам.

Элементы действий оценщика

ASE_ECD.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_ECD.1.1C – ASE_ECD.1.5C.

ASE_ECD.1.2E Оценщик должен подтвердить, что ни один из расширенных компонентов не может быть четко выражен с использованием существующих компонентов.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 9.7.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_REQ.2 Производные требования безопасности

Зависимости: ASE_OBJ.2 Цели безопасности;

ASE_ECD.1 Определение расширенных компонентов.

Элементы действий разработчика

ASE_REQ.2.1D Разработчик должен представить изложение «Требований безопасности».

ASE_REQ.2.2D Разработчик должен представить обоснование «Требований безопасности».

Элементы содержания и представления документированных материалов

ASE_REQ.2.1C Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.

ASE_REQ.2.2C Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, использующиеся в ФТБ и ТБД, должны быть определены.

ASE_REQ.2.3C В изложении «Требований безопасности» должны быть идентифицированы все выполненные над требованиями безопасности операции.

ASE_REQ.2.4C Все операции должны быть выполнены правильно.

ASE_REQ.2.5C Каждая зависимость от «Требований безопасности» должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения зависимости.

ASE_REQ.2.6C В «Обосновании требований безопасности» должно быть представлено прослеживание каждого ФТБ к целям безопасности для ОО.

ASE_REQ.2.7C В «Обосновании требований безопасности» должно быть продемонстрировано, что ФТБ обеспечивают выполнение всех целей безопасности для ОО.

ASE_REQ.2.8C В «Обосновании требований безопасности» должно приводиться пояснение того, почему выбраны определенные ТДБ.

ASE_REQ.2.9C Изложение «Требований безопасности» должно быть внутренне непротиворечивым.

Элементы действий оценщика

ASE_REQ.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_REQ.2.1C – ASE_REQ.2.9C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 9.8.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ASE_TSS.1 Краткая спецификация ОО

Зависимости: ASE_INT.1 Введение ЗБ.

ASE_REQ.1 Установленные требования безопасности

ADV_FSP.1 Базовая функциональная спецификация

Элементы действий разработчика

ASE_TSS.1.1D Разработчик должен представить «Краткую спецификацию ОО».

Элементы содержания и представления документированных материалов

ASE_TSS.1.1C «Краткая спецификация ОО» должна описывать, каким образом ОО выполняет каждое ФТБ.

Элементы действий оценщика

ASE_TSS.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ASE_TSS.1.1C.

ASE_TSS.1.2E Оценщик должен подтвердить, что «Краткая спецификация ОО» не противоречит «Аннотации ОО» и «Описанию ОО».

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 9.9.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий». Дополнительно должно быть проанализировано покрытие ТДБ мерами доверия.

7.2.5. Тестирование (ATE)

ATE_COV.2 Анализ покрытия

Зависимости: ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации;

ATE_FUN.1 Функциональное тестирование.

Элементы действий разработчика

ATE_COV.2.1D Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления документированных материалов

ATE_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.

ATE_COV.2.2C Анализ покрытия тестами должен демонстрировать, что все ИФБО из функциональной спецификации были подвергнуты тестированию.

Элементы действий оценщика

ATE_COV.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ATE_COV.2.1C и ATE_COV.2.2C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 13.3.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ATE_DPT.2 Тестирование: модули обеспечения безопасности

Зависимости: ADV_ARC.1 Описание архитектуры безопасности

ADV_TDS.3 Базовый модульный проект

ATE_FUN.1 Функциональное тестирование

Элементы действий разработчика

ATE_DPT.2.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления документированных материалов

ATE_DPT.2.1C Анализ глубины тестирования должен демонстрировать соответствие между тестами в тестовой документации и подсистемами ФБО, а также осуществляющими выполнение ФТБ модулями из проекта ОО.

Замечания по применению:

Для каждого интерфейса каждой функции обеспечения ИБ должны быть предусмотрены процедуры тестирования, соответствующие этому интерфейсу.

ATE_DPT.2.2C Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО из проекта ОО были подвергнуты тестированию.

ATE_DPT.2.3C Анализ глубины тестирования должен демонстрировать, что осуществляющие выполнение ФТБ модули из проекта ОО были подвергнуты тестированию.

Элементы действий оценщика

ATE_DPT.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ATE_DPT.2.1C – ATE_DPT.2.3C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 13.4.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ATE_FUN.1 Функциональное тестирование

Зависимости: ATE_COV.1 Свидетельство покрытия.

Элементы действий разработчика

ATE_FUN.1.1D Разработчик должен протестировать ФБО и задокументировать результаты.

ATE_FUN.1.2D Разработчик должен представить тестовую документацию.

Элементы содержания и представления документированных материалов

ATE_FUN.1.1C Тестовая документация должна состоять из планов тестирования, а также ожидаемых и фактических результатов тестирования.

ATE_FUN.1.2C В планах тестирования должны быть идентифицированы тесты, которые необходимо выполнить, а также должны содержаться описания сценариев проведения каждого теста. В эти сценарии должны быть включены также любые зависимости последовательности выполнения тестов от результатов других тестов.

Замечания по применению:

В среде разработки и тестирования не рекомендуется использование реальных данных, полученных в результате реализации банковских технологических процессов, технологических процессов финансовой организации.

В случае если для тестирования необходимы данные, максимально приближенные к реальным, рекомендуется формирование тестовых массивов данных путем необратимого обезличивания, маскирования и (или) искажения сведений, полученных в результате реализации банковских технологических процессов, технологических процессов финансовой организации. Запрещается использование в тестировании каких-либо данных, на которые на основании законодательства Российской Федерации, в том числе нормативных актов Банка России, внутренних документов организации БС Российской Федерации и (или) договоров с клиентами и контрагентами, распространяется требование к обеспечению ИБ.

ATE_FUN.1.3C Ожидаемые результаты тестирования должны продемонстрировать прогнозируемые данные на выходе успешного выполнения тестов.

ATE_FUN.1.4C Фактические результаты тестирования должны соответствовать ожидаемым.

Замечания по применению:

Факт выполнения теста должен подтверждаться протоколом тестирования, содержащим дату тестирования, указание на методику тестирования, использованные при выполнении теста исходные данные, полученный результат и решение об успешном или неуспешном выполнении теста.

Элементы действий оценщика

ATE_FUN.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ATE_FUN.1.1C – ATE_FUN.1.4C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 13.5.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ATE_IND.2 Выборочное независимое тестирование

Зависимости: ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации;

AGD_OPE.1 Руководство пользователя по эксплуатации;

AGD_PRE.1 Подготовительные процедуры;

ATE_COV.1 Свидетельство покрытия;

ATE_FUN.1 Функциональное тестирование.

Элементы действий разработчика

ATE_IND.2.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления документированных материалов

ATE_IND.2.1C ОО должен быть пригоден для тестирования.

ATE_IND.2.2C Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.

Элементы действий оценщика

ATE_IND.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ATE_IND.2.1C и ATE_IND.2.2C.

ATE_IND.2.2E Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные заявителем (разработчиком, производителем).

ATE_IND.2.3E Оценщик должен протестировать ФБО так, чтобы подтвердить, что ФБО функционируют в соответствии со спецификациями.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 13.6.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ATE_IND_EXT.1 Нефункциональное тестирование

Зависимости: ADV_FSP.4 Полная функциональная спецификация, ALC_DVS_EXT.1 Моделирование угроз и разработка описания поверхности атаки, AGD_PRE.1 Подготовительные процедуры

Элементы действий разработчика

ATE_IND.EXT.1.1D Разработчик должен проводить нефункциональное тестирование в отношении ПО (модулей ПО, компонентов ПО) в определенных объемах.

Замечание по применению

В настоящем разделе под нефункциональным тестированием понимаются проверки, не относящиеся к тестированию функциональных возможностей ПО. В рамках нефункционального тестирования могут выполняться следующие проверки:

- сетевых взаимодействий ПО;
- локальных интерфейсов взаимодействия ПО;
- производительности функционирования ПО;
- операций, выполняемых с высокими привилегиями;
- работы с конфиденциальными данными;
- корректности выполнения файловых операций;
- реализации защищенности бинарных файлов;
- реализации системы управления секретами;
- реализации безопасности сетевых протоколов;
- работы системы развертывания продукта;
- реализации мер по устранению или снижению критичности угроз, выявленных при моделировании угроз;

- возможности нарушения логики работы программы;
- безопасности реализации механизмов аутентификации и авторизации;
- безопасности обработки данных, полученных от потенциального нарушителя;
- безопасности реализации клиентской и серверной частей ПО.

ATE_IND.EXT.1.2D Разработчик должен разработать регламент нефункционального тестирования.

ATE_IND.EXT.1.3D Разработчик должен проводить нефункциональное тестирование с целью выявления локальных и сетевых интерфейсов взаимодействия с ПО (модулями ПО, компонентами ПО) пользователя и взаимодействий модулей (компонентов) ПО между собой, средой функционирования и внешними объектами.

ATE_IND.EXT.1.4D Разработчик должен осуществлять выполнение нефункциональных тестов, в том числе имитирующих действия потенциального нарушителя.

ATE_IND.EXT.1.5D Разработчик должен осуществлять корректировку описания поверхности атаки, модели угроз и архитектуры ПО по результатам выполнения нефункционального тестирования.

Элементы содержания и представления документированных материалов

ATE_IND.EXT.1.1C Регламент нефункционального тестирования должен содержать следующие сведения:

- критерии выбора версий ПО (модулей ПО, компонентов ПО), подлежащих нефункциональному тестированию, и определения периодичности тестирования;
- перечень используемых для нефункционального тестирования методов и средств;
- обязанности сотрудников и их роли при проведении нефункционального тестирования;
- описание типовых сценариев тестирования;
- описание возможностей и мотивации потенциального нарушителя, в соответствии с результатами моделирования угроз разрабатываемого ПО;
- описание типовых сценариев проведения компьютерных атак для основных сценариев работы ПО (модулей ПО, компонентов ПО).

ATE_IND.EXT.1.2C Отчет по результатам нефункционального тестирования должен содержать следующую информацию:

- краткое описание тестируемого ПО и его инфраструктуры развертывания;
- описание выполненных сценариев тестирования и последовательности их выполнения;
- набор целей (модулей ПО, компонентов ПО) тестирования;
- перечень выполненных действий и ограничений (описание отдельных аспектов, которые не проверялись);
- результаты нефункционального тестирования (снимки экрана (скриншоты), рабочие файлы инструментов нефункционального тестирования и т.п.);

- выводы, включающие следующую информацию: найденные недостатки (уязвимости) программ, средства и методы их выявления, результаты оценки опасности уязвимостей, описание возможных последствий эксплуатации уязвимостей, рекомендации по устранению найденных уязвимостей.

ATE_IND.EXT.1.3C Результаты сравнения архитектуры ПО, модели угроз и описания поверхности атаки с полученными фактическими результатами, перечень необходимых изменений в указанных артефактах реализации требований (при необходимости).

Элементы действий оценщика

ATE_IND.EXT.1.1E Оценщик должен подтвердить, что информация, представленная в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в ATE_IND.EXT.1.1C – ATE_IND.EXT.1.3C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 13.6.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.6. Оценка уязвимостей (AVA)

AVA_VAN.5 Усиленный методический анализ

Зависимости: ADV_ARC.1 Описание архитектуры безопасности;

ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации;

ADV_TDS.3 Базовый модульный проект;

ADV_IMP.2 Полное отображение представления реализации ФБО;

AGD_OPE.1 Руководство пользователя по эксплуатации;

AGD_PRE.1 Подготовительные процедуры.

Элементы действий разработчика

AVA_VAN.5.1D Разработчик должен представить ОО для тестирования.

AVA_VAN.5.2D Разработчик должен выполнить анализ уязвимостей.

Замечания по применению:

Разработчик проводит анализ уязвимостей с целью выявления типовых ошибок программирования и иных дефектов, приводящих к возникновению уязвимостей. Проведение анализа уязвимостей Разработчиком включает выполнение следующих работ.

1. Разработчик должен выполнить выявление известных и типовых уязвимостей в ОО. Разработчик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО. Выявление уязвимостей включает в себя:

- выявление известных уязвимостей в сетевых службах;

- выявление типовых уязвимостей в веб-приложениях;
- выявление известных уязвимостей в программном обеспечении;
- выявление учетных записей с паролями, содержащимися в словарях, используемых при проведении исследования.

Известные уязвимости могут быть выявлены следующими способами:

- идентификацией наименований и версий программного обеспечения ОО, сред его разработки и функционирования с последующим поиском в базах данных известных для них уязвимостей;
- запуском тест-программ (эксплойтов), воспроизводящих в полном объеме или частично выполнение компьютерных атак с использованием известных уязвимостей.

Сообщения об уязвимостях программного обеспечения рекомендуется получать из различных источников, таких как:

- база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru);
- уведомления Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (ФинЦЕРТ Банка России);
- уведомления, публикуемые центрами реагирования на компьютерные инциденты, платежными системами), производителями технических и программных средств;

- уведомления, публикуемые в общедоступных базах данных уязвимостей, а также распространяемые по подписке (например, www.cve.mitre.org);
- сообщения об уязвимостях в ППО, направляемые сторонними специалистами в адрес организации БС Российской Федерации или публикуемые ими в общедоступных источниках, для чего рекомендуется предусматривать способы оперативной связи с соответствующими специалистами организации БС Российской Федерации.

Для веб-приложений должен быть выполнен поиск следующих типов известных уязвимостей:

- инъекции, в особенности SQL-инъекции, команды операционной системы, LDAP, SSI и XPath-инъекции;
- подбор аутентификационных данных;
- небезопасная передача данных, в том числе в процессе аутентификации;
- ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, невозможность ограничения доступа по URL и обход директорий);
- межсайтовый скриптинг (XSS);
- подделка межсайтовых запросов (CSRF);
- расщепление запроса HTTP, сокрытие ответа HTTP;
- открытое перенаправление;
- раскрытие информации о директориях/сценариях;
- предсказуемое расположение ресурсов;

- идентификация приложений;
- чтение произвольных файлов;
- раскрытие защищаемой информации;
- обратный путь в директориях;
- переполнение буфера;
- небезопасная конфигурация сервера;
- внедрение внешних сущностей (XML, IMAP/SMTP);
- загрузка и выполнение произвольного кода;
- подмена контента;
- недостатки защиты от атак типа Clickjacking;
- недостатки защиты от атак на функции форматирования строк;
- уязвимости клиентских плагинов;
- уязвимости авторизации и аутентификации API-интерфейсов;
- уязвимость неограниченного доступа API-интерфейсов к конфиденциальным процессам;
- небезопасные данные, полученные от сторонних API-интерфейсов;
- недостаточная безопасность цепочки поставок.

Исследование производится путем анализа данных веб-форм, отправки веб-серверу тестовых запросов с варьируемыми значениями параметров запроса и анализа ответов.

Идентификация известных уязвимостей программного обеспечения включает в себя:

- инвентаризацию программного обеспечения, установленного на исследуемом техническом средстве, с идентификацией наименований и версий программ, а также установленных обновлений безопасности;
- выборку из базы данных уязвимостей, относящихся к идентифицированным версиям программ;
- исключение из полученной выборки уязвимостей, устранение которых обеспечено установленными обновлениями безопасности.

2. Разработчик должен выполнить динамический анализ кода ОО с целью выявления уязвимостей.

Динамический анализ кода программы осуществляется путем выполнения или эмуляции выполнения программы на определенной совокупности наборов тестовых исходных данных. Перед выполнением или в процессе выполнения программа иногда инструментируется путем дополнения ее функциями трассировки выполнения для задания и контроля инвариантов, предусловий, постусловий и др. Динамический контроль проводится с использованием специализированных автоматизированных средств и может включать в себя, в частности:

а) исследование особенностей исполнения потенциально опасных функций при задании заведомо некорректных аргументов;

б) построение динамических путей исполнения программы и идентификацию точек принятия решений, существенных для выполнения функций обеспечения ИБ;

в) поиск защищаемой информации в оперативной памяти и в аргументах функций;

г) исследование особенностей исполнения программы при типовых атаках (переполнение буфера, внедрение операторов SQL в данные, используемые для формирования запросов к СУБД).

Вне зависимости от применяемых способов и методов анализа кода при его осуществлении рекомендуется использование классификаторов типовых ошибок программирования, например, Общего перечня недостатков (Common Weakness Enumeration, CWE), а также способов выявления различных типов ошибок.

Выявленным в рамках контроля кода уязвимостям в коде разрабатываемых компонентов ОО целесообразно присваивать оценку степени их критичности (например, высокая, средняя, низкая). Для каждой выявленной уязвимости с учетом ее критичности принимается решение о доработке программного компонента ОО (и о приоритетности доработки) или о принятии рисков, связанных с наличием уязвимости.

AVA_VAN.5.3D Разработчик должен выполнить тестирование на проникновение.

Замечания по применению:

При тестировании на проникновение исследователь выполняет поиск уязвимостей ОО, воспроизводя действия злоумышленника. Перед началом работ для исследователя создаются условия, эквивалентные тем, в которых действует потенциальный злоумышленник.

Перед проведением тестирования на проникновение рекомендуется определить начальные условия его проведения. Рекомендуется учитывать, что максимальная полнота оценки достигается при внутреннем тестировании на проникновение с использованием предоставленного доступа к среде функционирования ОО.

Тестирование на проникновение подразделяется на исследования с предоставлением доступа к ОО и без предоставления такого доступа. При исследовании с предоставлением доступа Оценщику предоставляются учетные записи для доступа к ОО. При исследовании без предоставления доступа к ОО задача самостоятельного получения учетных записей пользователей ОО является составной частью тестирования на проникновение. При необходимости тестирование проводится с разными правами доступа в ОО.

При тестировании на проникновение могут использоваться две стратегии предоставления исследователю информации об ОО. При стратегии «черного ящика» исследователь оперирует только теми сведениями об ОО, которые получены им самостоятельно в ходе тестирования на проникновение. При стратегии «белого ящика» исследователю заблаговременно предоставляется вся доступная информация об ОО, включая (при наличии) проектную и эксплуатационную документацию, исходные коды программных компонентов ОО и возможность просмотра параметров настройки компонентов ОО.

По расположению разработчика относительно сетевого периметра ОО тестирование на проникновение разделяется на внешнее и внутреннее.

Тестирование на проникновение, в зависимости от типа ОО, может включать в себя следующие направления исследований, применимые к ОО и среде его функционирования:

а) оценка защищенности веб-приложений;

б) оценка защищенности специализированных банковских приложений (специализированного ПО) финансовых организаций;

в) оценка защищенности мобильных устройств.

При проведении оценки защищенности веб-приложений рекомендуются следующие мероприятия:

а) выявление уязвимостей, связанных с раскрытием защищаемой информации о приложении, в том числе путем отправки некорректных сообщений, анализа стандартных системных сообщений об ошибках, поиска защищаемой информации в коде и комментариях веб-страниц;

б) получение сведений о структуре файловой системы перебором путей и имен файлов (полный перебор, перебор по словарю, проверка наличия стандартных файлов используемых платформ и средств разработки, поиск резервных копий файлов);

в) проверка корректности обработки специальных символов в параметрах запроса (символы форматирования вывода, перевода строки и возврата каретки, перехода в вышестоящий каталог, двойное URL-кодирование);

г) проверка корректности обработки параметров различной длины;

д) проверка корректности обработки числовых параметров, в том числе не предусмотренных технологией обработки больших величин, отрицательных и нулевых значений;

е) проверка корректности приведения и преобразования типов параметров;

ж) проверка корректности обработки различного представления пользовательских данных, в том числе дублирование заголовков запроса, дублирование параметров сценария;

з) проверка корректности обработки параметров универсального идентификатора ресурса (URI – uniform resource identifier), в том числе возможности подключения произвольного внешнего источника данных или перенаправления на внешний или внутренний веб-сайт, возможности обращения к сетевым протоколам, возможности замены полного пути к ресурсу на относительный;

и) проверка наличия ошибок, связанных с обработкой загружаемых файлов, в том числе с обработкой имен файлов без расширения, несоответствием расширения типу файла, альтернативными расширениями для файлов одного типа, специальными символами (включая нулевой символ) в имени файла;

к) проверка корректности исполнения сценариев при манипулировании входными параметрами, в том числе атрибутами безопасности, используемыми при управлении доступом;

л) проверка возможности подбора аутентификационных данных (паролей, включая словарные, идентификаторов сессий, атрибутов, используемых для восстановления паролей);

м) проверка корректности обработки идентификаторов сессий пользователей, в том числе обработки событий завершения сессии, интервалов неактивности, сопоставление идентификатора сессии с дополнительными атрибутами, прямо или косвенно идентифицирующими пользователя или его рабочее место, предотвращение повторного и множественного использования идентификаторов сессий;

н) проверка корректности реализации механизмов авторизации;

о) проверка корректности противодействия атакам на клиентские приложения, в том числе с использованием межсайтового выполнения сценариев и подделки межсайтовых запросов;

п) проверка корректности обработки входных параметров сценариев при внедрении в них команд операционных систем, синтаксических конструкций языков программирования и разметки;

р) проверка невозможности обхода средств межсетевого экранирования прикладного уровня путем фрагментации данных, смешивания параметров, замены алгоритма кодирования и формата представления данных, замены специальных символов их альтернативными представлениями.

При проведении оценки защищенности специализированных банковских приложений (специализированного ПО) финансовых организаций рекомендуются следующие мероприятия:

а) прослушивание сетевого трафика и поиск в нем защищаемой информации, включая пароли и хеш-значения паролей пользователей, идентификаторы сессий, авторизационные маркеры, криптографические ключи;

б) запуск программ с различными параметрами, в том числе нестандартными, в том числе с использованием значений различной длины, дублирование отдельных параметров с присвоением им разных значений, включение в значения параметров специальных символов, команд операционной системы, операторов интерпретируемых языков программирования;

в) мониторинг характера взаимодействия приложения с операционной системой в процессе функционирования, включая идентификацию файлов данных, содержащих защищаемую информацию, трассировку системных вызовов;

г) проверка прав доступа к файлам данных, содержащим защищаемую информацию, а также контроль целостности исполняемых файлов приложения.

При проведении оценки защищенности мобильных устройств рекомендуются следующие мероприятия:

а) проверка наличия защищаемой информации в файлах данных, журналах регистрации событий, в оперативной памяти устройства, а также передачи защищаемой информации в незашифрованном виде;

б) проверка возможности чтения ключей шифрования и электронной подписи, а также записи и замены сертификатов ключей;

в) идентификация протоколов взаимодействия и проверка возможности принудительного навязывания устройству использования незащищенных версий протоколов (HTTP вместо HTTPS, TELNET вместо SSH, SSH1 вместо SSH2);

г) проверка корректности обработки мобильным приложением входящих параметров, в том числе с использованием значений различной длины, дублирование отдельных параметров с присвоением им разных значений, включение в значения параметров специальных символов, команд операционной системы, операторов интерпретируемых языков программирования;

д) проверка наличия в мобильном приложении средств защиты от исследования и возможность неавторизованного доступа к интерфейсу программирования приложений.

Элементы содержания и представления документированных материалов

AVA_VAN.5.1C ОО должен быть пригоден для тестирования.

AVA_VAN.5.2C Документация анализа уязвимостей Разработчиком должна содержать:

а) перечень исследованных компонентов ОО и среды его функционирования с указанием наименований и версий программ, а также установленных обновлений безопасности;

б) перечень баз данных уязвимостей, по которым проводился поиск;

в) результаты анализа, выполненного для поиска способов, которыми потенциально может быть нарушена реализация ФТБ;

г) идентификацию проанализированных предполагаемых уязвимостей;

д) перечень выявленных уязвимостей, оценку степени их критичности. Оценку критичности уязвимостей рекомендуется определять в соответствии с методикой Common Vulnerability Scoring System (CVSS);

е) рекомендации по устранению выявленных уязвимостей;

ж) сведения об устранении обнаруженных уязвимостей;

з) демонстрацию для всех выявленных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования ОО.

AVA_VAN.5.3C Результаты анализа уязвимостей Разработчиком должны оформляться протоколами анализа уязвимостей, подписываемыми Разработчиками — непосредственными исполнителями разработки ОО и лицами, участвовавшими в его проверке, с отражением в протоколе сведений о дате мероприятия, проверенной части ОО, выявленных уязвимостях и иных дефектах (при наличии), повторном контроле ОО с подтверждением устранения выявленных уязвимостей, дефектов.

AVA_VAN.5.4C 1. Отчет о тестировании на проникновение должен содержать:

а) описание начальных условий исследования и постановку задачи;

б) описание последовательности действий, которые приводили к выявлению уязвимостей или изменению возможностей исследователя, а также решения об отказе от выполнения запрашиваемых действий;

в) описание выявленных уязвимостей, оценку степени их критичности;

г) рекомендации по устранению выявленных уязвимостей;

д) сведения об устранении уязвимостей.

Элементы действий оценщика

AVA_VAN.5.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AVA_VAN.5.1C.

AVA_VAN.5.2E Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

Замечания по применению:

Поиск и проверка устранения в ОО и средах его функционирования известных (подтвержденных) уязвимостей (в том числе уязвимостей «нулевого дня») проводится по результатам анализа общедоступных источников информации об уязвимостях.

Сообщения об уязвимостях программного обеспечения рекомендуется получать из различных источников, таких как:

а) база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru);

б) уведомления Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (ФинЦЕРТ Банка России);

в) уведомления, публикуемые центрами реагирования на компьютерные инциденты, платежными системами, производителями технических и программных средств;

г) уведомления, публикуемые в общедоступных базах данных уязвимостей, а также распространяемые по подписке;

д) сообщения об уязвимостях в ППО, направляемые сторонними специалистами в адрес организации БС Российской Федерации или публикуемые ими в общедоступных источниках, для чего рекомендуется предусматривать способы оперативной связи с соответствующими специалистами организации БС Российской Федерации;

е) информация об инцидентах защиты информации направляется посредством технической инфраструктуры Банка России – автоматизированной системы обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (АСОИ ФинЦЕРТ).

ж) информация НКЦКИ о средствах и способах проведения компьютерных атак и о методах предупреждения и обнаружения. (www.cert.gov.ru).

В качестве потенциальных должны быть также рассмотрены известные (подтвержденные) уязвимости, выявленные в отличных от сертифицируемых версиях ОО, а также однотипных ОО.

Поиск информации о потенциальных уязвимостях необходимо сосредоточить на источниках, в которых содержится информация об однотипном с ОО прикладном программном обеспечении, а также на источниках, содержащих информацию о типовых уязвимостях, ошибках, недостатках языков программирования, используемых при разработке ОО. Результатом такого поиска является выявление всех возможных способов, которыми может быть нарушена реализация функциональных возможностей безопасности ОО.

В качестве источников информации о потенциальных уязвимостях наряду с документацией заявителя должны рассматриваться базы данных уязвимостей и угроз безопасности информации, включая Общий перечень недостатков (CWE), Общий перечень шаблонов атак (CAPEC), рассылки и форумы по безопасности, «хакерские» форумы в сети Интернет, в которых сообщается об уязвимостях в конкретных технологиях и атаках на эти технологии.

Оценщику не следует ограничиваться рассмотрением общедоступной информации вышеупомянутых источников, ему следует рассмотреть любую другую доступную

информацию, имеющую отношение к уязвимостям ОО или среды функционирования ОО при их использовании в представлении реализации ОО. Процесс идентификации проблемных конструкций может быть итерационным (повторяющимся), т.е. идентификация одной проблемной конструкции может привести к идентификации другой проблемной конструкции, которая требует дальнейшего исследования.

В случае обнаружения в ОО пригодных для использования известных уязвимостей сертификационные испытания могут быть продолжены только после их устранения разработчиком.

AVA_VAN.5.3E Оценщик должен провести независимый методический анализ уязвимостей ОО с использованием документации руководств, функциональной спецификации, проекта ОО, описания архитектуры безопасности и представления реализации, чтобы идентифицировать потенциальные уязвимости в ОО.

Замечания по применению:

Независимый методический анализ уязвимостей должен включать выявление типовых ошибок программирования и иных дефектов, приводящих к возникновению уязвимостей. При этом выявлению подлежат уязвимости кода и уязвимости конфигурации ОО.

Идентификация потенциальных уязвимостей предусматривает формирование перечня предполагаемых, но не подтвержденных уязвимостей в ОО по результатам исследований доступных документированных материалов и источников информации об уязвимостях. Предположения

основываются на допустимых сценариях реализации угроз безопасности информации в заданных средах функционирования ОО.

Оценщик должен выполнить контроль информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п.).

С этой целью оценщик должен исследовать представленную документацию инструментальных средств разработки, чтобы сделать заключение о том, имеются ли в определении языка программирования проблемные конструкции, которые могут быть применены к информационным объектам. В качестве источников информации о проблемных конструкциях языка программирования, которые могут быть применены к информационным объектам, наряду с документацией заявителя должны также рассматриваться базы данных уязвимостей и угроз безопасности информации, включая Общий перечень недостатков (CWE), Общий перечень шаблонов атак (CAPEC), рассылки и форумы по безопасности, «хакерские» форумы в сети Интернет, в которых сообщается об уязвимостях в конкретных технологиях и атаках на эти технологии. В качестве таких проблемных конструкций, которые могут быть применены к информационным объектам, могут выступать, например, преобразование информационного объекта из одного типа данных в другой, использование псевдонимов (альтернативных имен, которые позволяют ссылаться на одну и ту же часть памяти различными способами), указателей (ссылок) на

произвольные области памяти, использование стека для передачи фактических параметров между функциональными объектами, динамическое выделение памяти информационным объектам и т.п.

Оценщик должен исследовать представление реализации, с тем чтобы сделать заключение о том, что любое использование проблемных конструкций языка программирования применительно к информационным объектам не вносит уязвимостей. Оценщику следует также удостовериться, что конструкции, не предусмотренные соответствующим стандартом языка программирования, не используются в представлении реализации.

Оценщик должен также сделать заключение о том, что ввод данных пользователем обрабатывается ФБО таким способом, при котором ФБО защищены от внесения в них искажений вводимыми данными. Следует отметить, что части ОО, которые не относятся к ФБО, могут не исследоваться, если оценщиком проведено обоснование отсутствия их влияния на ФБО.

Результатом идентификации потенциальных уязвимостей должен быть перечень потенциальных уязвимостей, которые являются предметом тестирования проникновения и применимы к ОО. Из рассмотрения могут быть исключены потенциальные уязвимости, для которых обосновано, что используемые в среде функционирования меры защиты информации исключают возможность эксплуатации (использования) этих уязвимостей.

AVA_VAN.5.4E Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы

сделать заключение о том, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим высоким потенциалом нападения.

Замечания по применению:

Тестирование проникновения должно проводиться относительно всех идентифицированных потенциальных уязвимостей в ОО из составленного перечня.

Для тестирования проникновения разрабатываются тесты, которые должны охватывать все возможные допустимые сценарии реализации угроз безопасности информации в заданных средах функционирования ОО (шаблоны атак). Тесты проникновения должны позволять оценить все возможности нарушителя по эксплуатации (использованию) идентифицированных потенциальных уязвимостей в ОО.

Наиболее тщательно должны быть подготовлены и проведены тесты проникновения, связанные с тестированием уязвимостей, которые потенциально могут быть использованы нарушителем для обхода, отключения или преодоления функций безопасности, реализующих основные функциональные возможности ОО, определяемые видом и типом ОО.

Для каждой идентифицированной потенциальной уязвимости из составленного списка должны быть разработаны способы тестирования, учитывающие интерфейсы ОО, используемые для выполнения функций безопасности, определены исходные данные и условия, которые необходимы для тестирования, средства тестирования, необходимые для инициирования

интерфейсов, а также возможность использования при анализе уязвимостей тестов, которые выполнялись ранее.

Результаты тестирования проникновения должны подтверждать стойкость ОО к действиям нарушителя с высоким потенциалом нападения. Если результаты показывают, что ОО, находящийся в заданных средах функционирования, имеет уязвимости, пригодные для использования нарушителем, по компоненту доверия в целом не может быть вынесена положительная оценка.

Результаты анализа уязвимостей отражаются в отдельном протоколе, в котором, как минимум, указываются:

а) перечень проанализированных источников информации;

б) перечень идентифицированных потенциальных уязвимостей (с указанием источника информации, описанием, указанием последствий от использования нарушителем, минимального уровня компетентности нарушителя для подготовки и реализации уязвимости, времени, возможности по доступу, оборудования, требуемого ему для использования уязвимости);

в) описание тестов и методик тестирования проникновения;

г) результаты тестирования.

Работы оценки

1. Проверяющая организация должна выполнить действия в соответствии с пунктом 14.2.5 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» для нарушителя с высоким потенциалом нападения.

2. Результаты анализа уязвимостей отражаются в отдельном протоколе, в котором, как минимум, указываются:

а) перечень проанализированных источников информации;

б) перечень идентифицированных потенциальных уязвимостей (с указанием источника информации, описанием, указанием последствий от использования нарушителем, минимального уровня компетентности нарушителя для подготовки и реализации уязвимости, времени, возможности по доступу, оборудования, требуемого ему для использования уязвимости);

в) описание тестов и методик тестирования проникновения;

г) результаты тестирования.

AVA_VAN_EXT.1 Реагирование на информацию об уязвимостях

Зависимости: AVA_VAN.5 Усиленный методический анализ.

Элементы действий разработчика

AVA_VAN_EXT.1.1D Разработчик должен разработать регламент реагирования на информацию об уязвимостях.

AVA_VAN_EXT.1.2D Разработчик должен осуществлять обработку поступающих запросов от пользователей (через службу технической поддержки, по иным каналам взаимодействия) с последующим анализом ошибок функционирования на предмет наличия уязвимостей (в случае получения таких запросов).

AVA_VAN_EXT.1.3D Разработчик должен, при обработке поступающих запросов и при последующем анализе, использовать средства автоматизации (например, систему управления изменениями, систему отслеживания ошибок, систему управления задачами и т.п.).

AVA_VAN_EXT.1.4D Разработчик должен осуществлять анализ информации о найденных уязвимостях в ПО на предмет подтверждения наличия/отсутствия уязвимостей и принимать решение о необходимости их устранения по результатам оценки.

AVA_VAN_EXT.1.5D Разработчик должен осуществлять оценку актуальности и критичности уязвимости с точки зрения безопасности ПО (в случае получения информации об уязвимости ПО из внешнего источника) и принимать решение о необходимости ее устранения по результатам оценки.

Элементы содержания и представления документированных материалов

AVA_VAN_EXT.1.1C Регламент реагирования на информацию об уязвимостях должен содержать:

- обязанности сотрудников и их роли при реагировании на информацию об уязвимостях ПО;
- правила реагирования на информацию об уязвимостях;
- правила оценки актуальности и критичности уязвимости с точки зрения безопасности ПО;
- периодичность проведения поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО.

AVA_VAN_EXT.1.2C Артефакты реализации требований, подтверждающие получение и обработку запросов от пользователей, должны содержать следующие сведения:

- информацию о запросах пользователей об ошибках (уязвимостях) ПО (дата, время запроса, идентификатор пользователя, статус запроса);
- результат анализа ошибок функционирования на предмет наличия уязвимостей.

AVA_VAN_EXT.1.3C Артефакты реализации требований, подтверждающие выполнение анализа информации о найденных уязвимостях в ПО, должны содержать следующие сведения:

- информацию о результатах тестирования ПО на предмет применимости информации об уязвимости ПО;
- проект (шаблон) ответа пользователям на запросы пользователей об ошибках (уязвимостях) ПО (о применимости информации о найденных уязвимостях);
- решение по результатам анализа информации о найденных уязвимостях в ПО.

AVA_VAN_EXT.1.4C Артефакты реализации требований, подтверждающие выполнение оценки актуальности и критичности уязвимости с точки зрения безопасности, должны содержать следующие сведения:

- информацию об оценке актуальности уязвимости;
- информацию об оценке уровня критичности уязвимости ПО;
- решение по результатам анализа актуальности и критичности уязвимости.

Элементы действий оценщика

AVA_VAN_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в AVA_VAN_EXT.1.1C - AVA_VAN_EXT.1.4C.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 14.2.4 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

AVA_CCA_EXT.1 Анализ скрытых каналов

Зависимости: AVA_VAN.4 Методический анализ уязвимостей;

ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации;

ADV_IMP.2 Полное отображение представления реализации функций безопасности ОО;

AGD_OPE.1 Руководство пользователя по эксплуатации;

AGD_PRE.1 Подготовительные процедуры;

[FDP_ACC.1 Ограниченное управление доступом

или

FDP_IFC.1 Ограниченное управление информационными потоками].

Элементы действий разработчика

AVA_CCA_EXT.1.1D Разработчик должен провести поиск скрытых каналов для реализуемых ОО **[выбор:**

политики управления информационными потоками;

политики управления доступом;

[назначение: иные политики]

].

AVA_CCA_EXT.1.2D Разработчик должен представить документацию по анализу скрытых каналов.

Элементы содержания и представления документированных материалов

AVA_CCA_EXT.1.1C В документации по анализу скрытых каналов должны быть идентифицированы скрытые каналы и должна содержаться оценка их пропускной способности.

AVA_CCA_EXT.1.2C Документация по анализу скрытых каналов должна содержать описание процедур, использованных для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

AVA_CCA_EXT.1.3C Документация по анализу скрытых каналов должна содержать описание всех предположений (быстродействие процессора, системная конфигурация, объем памяти и (или) иных), сделанных при анализе скрытых каналов.

AVA_CCA_EXT.1.4C Документация по анализу скрытых каналов должна содержать описание метода, использованного для оценки пропускной способности канала для наиболее опасного сценария.

AVA_CCA_EXT.1.5C Документация по анализу скрытых каналов должна содержать описание наиболее опасного сценария использования каждого идентифицированного скрытого канала.

Элементы действий оценщика

AVA_CCA_EXT.1.1E Оценщик должен подтвердить, что информация, представленная разработчиком в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в AVA_CCA_EXT.1.1C - AVA_CCA_EXT.1.5C.

AVA_CCA_EXT.1.2E Оценщик должен подтвердить, что результаты анализа скрытых каналов, выполненного разработчиком, свидетельствуют об удовлетворении ОО соответствующих функциональных требований (по управлению информационными потоками, управлению доступом и (или) иных).

AVA_CCA_EXT.1.3E Оценщик должен подтвердить правильность результатов анализа скрытых каналов, выполненного заявителем (разработчиком, производителем).

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 14.2.4 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.7 Композиция (ACO)

ACO_DEV.1 Функциональное описание

Зависимости: ACO_REL.1 Базовая информация о зависимостях.

Элементы действий разработчика

ACO_DEV.1.1D Разработчик должен предоставить информацию по разработке базового компонента.

Элементы содержания и представления свидетельств

ACO_DEV.1.1C Информация по разработке должна описывать назначение каждого интерфейса базового компонента, используемого в составном ОО.

ACO_DEV.1.2C Информация по разработке должна показывать соответствие между интерфейсами базового и зависимого компонентов, используемыми в составном ОО для поддержки ФБО зависимого компонента.

Элементы действий оценщика

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

ACO_DEV.1.2E Оценщик должен установить, что предоставленное описание интерфейсов согласуется с информацией о зависимостях, предоставленной для зависимого компонента.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 15.4.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ACO_REL.1 Базовая информация о зависимостях

Зависимости: отсутствуют.

Элементы действий разработчика

ACO_REL.1.1D Разработчик должен предоставить информацию о зависимостях для зависимого компонента.

Элементы содержания и представления свидетельств

ACO_REL.1.1C В информации о зависимостях должны быть описаны функции аппаратного, программного и программно-аппаратного обеспечения базового компонента, на которые полагаются ФБО зависимого компонента.

ACO_REL.1.2C В информации о зависимостях должны быть описаны все взаимодействия, через которые ФБО зависимого компонента запрашивают сервисы базового компонента.

ACO_REL.1.3C В информации о зависимостях должно быть описание того, каким образом ФБО зависимого компонента обеспечивают собственную защиту от вмешательства со стороны базового компонента.

Элементы действий оценщика

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

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 15.5.1 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

ACO_VUL.2 Анализ уязвимостей композиции

Зависимости: отсутствуют.

Элементы действий разработчика

ACO_VUL.2.1D Разработчик должен представить для тестирования составной ОО.

Элементы содержания и представления свидетельств

ACO_VUL.2.1C Составной ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ACO_VUL.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ACO_VUL.2.2E Оценщик должен выполнить анализ, чтобы сделать заключение, что любые остаточные уязвимости, идентифицированные для базового и зависимых компонентов, не могут быть использованы по отношению к составному ОО в его среде функционирования.

ACO_VUL.2.3E Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать возможные уязвимости, возникающие при использовании базового и зависимых компонентов в среде функционирования составного ОО.

ACO_VUL.2.4E Оценщик должен выполнить независимый анализ уязвимостей составного ОО, используя документацию руководств, информацию о зависимостях и обоснование композиции для идентификации потенциальных уязвимостей составного ОО.

ACO_VUL.2.5E Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы продемонстрировать, что составной ОО противостоит атакам нарушителя с Базовым потенциалом нападения.

Работы оценки

Оценщик должен выполнить действия в соответствии с пунктом 15.7.2 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».

7.2.7. Обновление ОО (AMA)

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность ОО

Зависимости: отсутствуют.

Элементы действий разработчика

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

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность ОО должны содержать краткое описание влияния обновлений на ЗБ, реализацию ОО функциональных возможностей или логическое обоснование отсутствия такого влияния, подтверждение устранения уязвимости (уязвимостей), на устранение которой (которых) направлен выпуск данных обновлений, и невнесения иных уязвимостей в ОО.

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

Элементы действий оценщика

AMA_SIA_EXT.3.1E Оценщик должен подтвердить, что информация, представленная в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в AMA_SIA_EXT.3.1C, AMA_SIA_EXT.3.2C.

AMA_SIA_EXT.3.2E Оценщик должен подтвердить влияние (отсутствие влияния) обновлений на безопасность ОО.

7.3. Обоснование требований безопасности

7.3.1. Обоснование требований безопасности для ОО

7.3.1.1. Обоснование функциональных требований безопасности ОО

Таблица 7.3.1.1 – Отображение функциональных требований безопасности на цели безопасности

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6
FAU_GEN.1					X	
FAU_GEN.2					X	
FAU_GEN_EXT.1			X		X	
FAU_SAR.1					X	
FAU_SAR.2					X	
FAU_STG.1					X	
FAU_STG.3					X	
FAU_STG.4					X	
FDP_ACC.1	X					
FDP_ACF.1	X					
FDP_DAR_EXT.1			X			
FDP_ETC.1				X		
FDP_IFC.1		X		X		
FDP_IFF.1					X	
FDP_ITC.2					X	
FDP_RIP.2			X			
FDP_ROL.1	X					
FIA_AFL.1						X
FIA_ATD.1						X
FIA_IWS_EXT.1	X					
FIA_SOS.1						X
FIA_SOS.2				X		

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6
FIA_UAU.2						X
FIA_UAU.4						X
FIA_UAU.5						X
FIA_UAU.6						X
FIA_UAU.7						X
FIA_UID.1						X
FMT_CFG_EXT.1		X				
FMT_MEC_EXT.1		X		X		
FMT_MSA.1	X					
FMT_MSA.3	X					
FMT_MTD.1	X					
FMT_SMF.1	X					
FMT_SMR.1	X					
FPR_ANO_EXT.1			X			X
FPT_AEX_EXT.1	X	X				
FPT_API_EXT.1	X					
FPT_LIB_EXT.1	X					
FPT_STM.1					X	
FPT_TDC.1		X				
FPT_TST.1	X					
FPT_TUD_EXT.1	X					
FTA_MCS.1	X					
FTP_DIT_EXT.1			X	X		

FAU_GEN.1 Генерация данных аудита

Выполнение требований данного компонента обеспечивает возможность регистрации возникновения всех событий, связанных с выполнением функций безопасности ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FAU_GEN.2 Ассоциация идентификатора пользователя

Выполнение требований данного компонента обеспечивает возможность регистрации возникновения всех событий, связанных с идентификатором пользователя, который был инициатором этого события. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FAU_GEN_EXT.1 Ассоциация защищаемой информации

Выполнение требований данного компонента обеспечивает возможность не регистрировать в записях аудита защищаемую информацию, если иное не предусмотрено целями функционирования и техническими особенностями, а также ограничениями реализации АСБиФО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления администратору ППО всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает возможность ограничения доступа пользователям к чтению записей аудита, за исключением пользователей, которым явно предоставлен доступ на чтение. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает возможность защиты хранимых записей аудита от несанкционированного удаления и предотвращения модификации записей аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FAU_STG.3 Действия в случае возможной потери данных аудита

Выполнение требований данного компонента обеспечивает возможность защиты журнала аудита от переполнения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает возможность выполнения действий, направленных на предотвращение потери данных аудита при переполнении журнала аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FDP_ACC.1 Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает возможность задания политики управления доступом для определенного подмножества (списка, числа) операций, выполняемых субъектами доступа по отношению к объектам доступа. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

Выполнение требований данного компонента обеспечивает возможность осуществления управления доступом к объектам доступа ОО на основе списков управления доступом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FDP_DAR_EXT.1 Шифрование защищаемой информации приложения

Выполнение требований данного компонента обеспечивает защиту защищаемой информации при хранении и обработке. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FDP_ETC.1 Экспорт данных пользователя без атрибутов безопасности

Выполнение требований данного компонента обеспечивает чтобы ФБО осуществляли соответствующие ПФБ, используя функцию, которая точно и однозначно ассоциирует атрибуты безопасности с экспортируемыми данными пользователя. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FDP_IFC.1 Ограниченное управление информационными потоками

Выполнение требований данного компонента обеспечивает чтобы каждая идентифицированная ПФБ управления информационными потоками охватывала все операции для субъектов доступа и информацию под управлением этой ПФБ. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2**, **Цель безопасности-4** и способствует их достижению.

FDP_IFF.1 Простые атрибуты безопасности

Выполнение требований данного компонента обеспечивает наличия атрибутов безопасности информации и субъектов доступа, которые выступают как инициаторы отправления или как получатели этой информации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FDP_ITC.2 Импорт данных пользователя с атрибутами безопасности

Выполнение требований данного компонента обеспечивает, чтобы атрибуты безопасности правильно представляли данные пользователя, а также точно и однозначно ассоциировались с данными пользователя, импортируемыми из-за пределов ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FDP_RIP.2 Полная защита остаточной информации

Выполнение требований данного компонента обеспечивает недоступность содержания всей остаточной информации любых ресурсов, контролируемых ОО, при распределении или освобождении ресурса. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FDP_ROL.1 Базовый откат

Выполнение требований данного компонента обеспечивает возможность восстановления ресурсов в случае сбоев и ошибок, возникающих при функционировании ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает ограничение попыток пройти процедуру аутентификации для лиц, не являющихся уполномоченными пользователями. При достижении определенного числа неуспешных попыток аутентификации некоторого лица ОО предпринимаются действия, направленные на дальнейшее предотвращение попыток доступа со стороны данного лица, ограниченные временным интервалом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя (или других уполномоченных идентифицированных ролей) список атрибутов безопасности. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_IWS_EXT.1 Идентификация сессий веб-приложений

Выполнение требований данного компонента обеспечивает безопасность в процессе идентификации сессий веб-приложений, предъявляя требования безопасности к идентификаторам сессий. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает предоставление механизма для верификации соответствия паролей определенным требованиям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_SOS.1 Генерация секретов ФБО

Выполнение требований данного компонента обеспечивает предоставление механизма для генерации паролей, отвечающих определенным требованиям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает аутентификацию субъекта доступа до выполнения любых действий по доступу в информационную систему или привилегированного субъекта доступа до выполнения действий по управлению ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_UAU.4 Механизмы одноразовой аутентификации

Выполнение требований данного компонента предотвращает повторное применение аутентификационных данных. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_UAU.5 Сочетание механизмов аутентификации

Выполнение требований данного компонента обеспечивает возможность выполнения аутентификации с использованием сочетания различных механизмов аутентификации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_UAU.6 Повторная аутентификация

Выполнение требований данного компонента обеспечивает определение событий, при которых необходима повторная аутентификация пользователя. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_UAU.7 Аутентификация с защищенной обратной связью

Выполнение требований данного компонента обеспечивает исключение отображения действительного значения аутентификационной информации при ее вводе пользователем в диалоговом интерфейсе. Рассматриваемый

компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FIA_UID.1 Выбор момента идентификации

Выполнение требований данного компонента обеспечивает выполнение определенных действий до идентификации пользователя. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FMT_CFG_EXT.1 Конфигурация безопасности по умолчанию

Выполнение требований данного компонента обеспечивает предоставление уполномоченным пользователям только ограниченной функциональности ОО при его конфигурировании по умолчанию. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FMT _MEC_EXT.1 Поддерживаемый механизм конфигурации

Выполнение требований данного компонента обеспечивает защиту конфигурационных данных, находящихся под управлением ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики управления доступом только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает возможность определения правил политики управления доступом, которую должен наследовать атрибут безопасности. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность запроса и добавления данных компонентов ОО и данных аудита, запроса и модификации всех прочих данных ОО, а также внесения новых правил контроля только администратору. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_SMF.1 Спецификация функций управления

Выполнение требований данного компонента обеспечивает наличие у ОО, как минимум, функций управления режимом выполнения функций безопасности и функций управления данными ФБО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_SMR.1 Роли безопасности

Выполнение требований данного компонента обеспечивает поддержание ролей безопасности и их ассоциации. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FPR_ANO_EXT.1 Согласие пользователей на обработку персональных данных (идентификационной информации)

Выполнение требований данного компонента обязывает ОО запрашивать согласие пользователя на использование его персональной идентификационной информации. Рассматриваемый компонент сопоставлен с

целями **Цель безопасности-3, Цель безопасности-6** и способствуют их достижению.

FPT_AEX_EXT.1 Противодействие использованию уязвимостей безопасности

Выполнение требований данного компонента обеспечивает возможность контролировать использование уязвимых программных ресурсов. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1**, **Цель безопасности-2** и способствуют их достижению.

FPT_API_EXT.1 Использование поддерживаемых сервисов и прикладных программных интерфейсов

Выполнение требований данного компонента обеспечивает возможность контролировать использование в программном продукте только легитимных программных ресурсов. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FPT_LIB_EXT.1 Использование сторонних библиотек

Выполнение требований данного компонента обеспечивает возможность контроля использования сторонних библиотек. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Выполнение требований данного компонента обеспечивает возможность по предоставлению надежных меток времени в пределах ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FPT_TDC.1 Базовая согласованность данных ФБО между ФБО

Выполнение требований данного компонента необходимо, чтобы ФБО предоставили возможность обеспечить согласованность атрибутов между

ФБО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FPT_TST.1 Тестирование ФБО

Выполнение требований данного компонента обеспечивает возможность тестирования (самотестирования) функций безопасности ОО, проверки целостности программного обеспечения ОО и целостности данных ОО. **Рассматриваемый комп**онент сопоставлен с целью Цель **безопасности-1** и способствует ее достижению.

FPT_TUD_EXT.1 Целостность при установке и обновлении

Выполнение требований данного компонента обеспечивает возможность контроля целостности устанавливаемых обновлений ПО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FTA_MCS.1 Базовое ограничение на параллельные сеансы

Выполнение требований данного компонента ограничивает максимальное число параллельных сеансов, предоставляемых одному и тому же пользователю. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FTP_DIT_EXT.1 Защита данных при передаче

Выполнение требований данного компонента обеспечивает контроль за передачей данных между ОО и другими доверенными продуктами ППО. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-3**, **Цель безопасности-4** и способствуют их достижению.

FTP_ITC.1 Доверенный канал передачи между ФБО

Выполнение требований данного компонента обеспечивает, чтобы ФБО предоставили доверенный канал связи между ними самими и другим

доверенным продуктом ИТ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствуют ее достижению.

7.3.1.2. Обоснование удовлетворения зависимостей функциональных требований безопасности

В таблице 7.3.1.2 представлены результаты удовлетворения зависимостей функциональных требований безопасности. Все зависимости компонентов требований удовлетворены в настоящем ПЗ либо включением компонентов, определенных в национальном стандарте Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в национальном стандарте Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» под рубрикой «Зависимости».

Столбец 1 таблицы 7.3.1.2 является справочным и содержит компоненты, определенные в национальном стандарте Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности», в описании компонентов требований, приведенных в столбце 2 таблицы 7.3.1.2 под рубрикой «Зависимости».

Столбец 3 таблицы 7.3.1.2 показывает, какие компоненты требований были включены в настоящий ПЗ для удовлетворения зависимостей компонентов, приведенных в столбце 2 таблицы 7.3.1.2. Компоненты требований в столбце 3 таблицы 7.3.1.2 либо совпадают с компонентами в столбце 2 таблицы 7.3.1.2, либо иерархичны по отношению к ним.

Таблица 7.3.1.2 – Зависимости функциональных требований безопасности

Функциональные компоненты	**Зависимости в соответствии с ГОСТ Р ИСО/МЭК 15408 и подразделом 7.1 настоящего ПЗ**	**Удовлетворение зависимостей**
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_ETC.1	[FDP_ACC.1 или FDP_IFC.1]	FDP_ACC.1
FDP_IFC_1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1	FDP_IFC.1
FDP_ROL.1	[FDP_ACC.1 или FDP_IFC.1]	FDP_ACC.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UAU.2	FIA_UID.1	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FMT_CFG_EXT.1	FMT_SMF.1	FMT_SMF.1
FMT_MEC_EXT.1	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 или	FDP_ACC.1

Функциональные компоненты	**Зависимости в соответствии с ГОСТ Р ИСО/МЭК 15408 и подразделом 7.1 настоящего ПЗ**	**Удовлетворение зависимостей**
	FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTA_MCS.1	FIA_UID.1	FIA_UID.1

7.3.1.3. Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ПЗ соответствуют ОУД4, усиленному компонентами

ADV_IMP.2 «Полное отображение представления реализации ФБО»,

ALC_FLR.2 «Процедуры сообщений о недостатках»,

AVA_VAN.5 «Усиленный методический анализ»,

ACO_DEV.1 «Функциональное описание»,

ACO_REL.1 «Базовая информация о зависимостях»,

ACO_VUL.2 «Анализ уязвимостей композиции»,

расширенный компонентами

ADV_IMP_EXT.3 «Реализация ОО»,

ADV_TDS_EXT.3 «Разработка, уточнение и анализ архитектуры программного обеспечения ОО»,

ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения ОО»,

ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки»,

AVA_CCA_EXT.1 «Анализ скрытых каналов»,

AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность»,

AGD_OPE_EXT.1 «Правила кодирования»,

ALC_DEL_EXT.1 «Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок»,

ALC_DVS_EXT.1 «Моделирование угроз и разработка описания поверхности атаки»,

ALC_DVS_EXT.2 «Обеспечение безопасности сборочной среды программного обеспечения»,

ALC_DVS_EXT.3 «Управление доступом и контроль целостности кода при разработке программного обеспечения»,

ALC_TAT_EXT.1 «Статический анализ исходного кода»,

ALC_TAT_EXT.2 «Динамический анализ кода программы»,

ATE_IND.EXT.1 «Нефункциональное тестирование»,

AVA_VAN_EXT.1 «Реагирование на информацию об уязвимостях».

Включение указанных требований доверия к безопасности ОО в ПЗ определяется положениями Рекомендаций в области стандартизации Банка России РС БР ИББС-2.6-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на этапах жизненного цикла автоматизированных банковских систем», с учетом положений национального стандарта Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

7.4. Безопасный жизненный цикл ОО. Требования к гибкой безопасной разработке и тестированию ОО

7.4.1. Общие положения

Целью применения методологий безопасного жизненного цикла к ОО является обеспечение высокой конкурентоспособной скорости разработки и внедрения безопасных программных продуктов при сохранении гарантированного и достаточного уровня защищенности ОО в условиях изменяющихся требований, при высокой вовлеченности и ответственности компетентных подразделений (от разработчиков, специалистов по информационной безопасности до служб эксплуатации и поддержки), одновременно привлекаемых на самых ранних этапах жизненного цикла ОО, включая обновления ОО, и сопровождающих жизненный цикл ОО вплоть до вывода ОО из эксплуатации.

Объектом применения требований настоящего раздела являются процессы жизненного цикла ОО и, обеспечивающие их функционирование, инфраструктура и ресурсы. Возможно частичное распространение требований на смежные и обеспечивающие процессы и объекты.

В связи с этим, требования настоящего раздела могут использоваться в целях реализации ТДБ ОО (п. 7.2. настоящего ПЗ) в случаях, когда финансовая организация либо разработчик ОО (далее при совместном упоминании – Разработчик) реализует документированный безопасный жизненный цикл ОО, основанный на современных гибких практиках разработки, тестирования и внедрения ОО, в основе которых лежат различные методологии безопасного жизненного цикла программных продуктов.

Требования настоящего раздела сформированы таким образом, что их выполнение должно обеспечить покрытие необходимых и достаточных ТДБ ОО, сформированных в разделе 7.2 настоящего ПЗ, а также положений национального стандарта Российской Федерации ГОСТ Р 56939-2024 «Защита

информации. Разработка безопасного программного обеспечения. Общие требования».

При этом переход от ТДБ, связанных с оценочным уровнем доверия, к настоящей методологии безопасного жизненного цикла возможен только при условии соответствия отдельных процессов Разработчика критериям и условиям, указанным в п. 7.4.2 настоящего раздела.

Оценка соответствия требованиям безопасности процесса разработки ОО, установленным настоящим разделом, проводится Разработчиком самостоятельно либо с участием организации, независимой от организаций, осуществлявших или осуществляющих оказание услуг Разработчику в области информатизации и защиты информации (в части внедрения и/или сопровождения систем, средств, процессов информатизации и защиты информации). По результатам проведения оценки должен быть подготовлен отчет, содержащий:

- Перечень процессов РБПО, реализованных Разработчиком;
- Результаты определения достаточности и соответствия процессов РБПО, реализованных Разработчиком, положениям настоящего Профиля защиты и иным стандартам, содержащим требования к РБПО, используемым инструментам и технологиям, включая:

- результаты сравнительного анализа этапов спринта[1] безопасной разработки, реализуемого Разработчиком, с этапами спринта в ориентировочном процессе безопасной разработки, изложенном в Приложении В настоящего ПЗ;

- результаты сравнительного анализа ролей сотрудников Разработчика, участвующих в процессе безопасной разработки, с ролями, приведенными в разделе 7.4.3.2.3 настоящего ПЗ;

- результаты контрольных мероприятий по ИБ;

---

[1] Спринт – элемент гибкой методологии разработки, который обеспечивает эффективное и последовательное выполнение задач в рамках коротких отрезков времени.

- результаты проведенных контролей безопасности (security controls);

•Результаты работ по анализу уязвимостей и тестированию защищенности ОО при подтвержденном общем соответствии документированному процессу безопасной разработки;

•Ключевые артефакты (документация) процесса безопасной разработки;

•План развития процессов РБПО и План реализации процессов РБПО.

7.4.2. Критерии и условия для реализации безопасного жизненного цикла ОО

Для возможности перехода от оценки соответствия ТБД ОО к оценке соответствия требованиям безопасности процесса разработки ОО процессы Разработчика, связанные или влияющие на жизненный цикл разработки, должны удовлетворять определенным условиям и соответствовать определенным критериям, приведенным в п. 7.4.2.1 и п. 7.4.2.2 настоящего раздела, что должно быть задокументировано в организационно-распорядительной документации Разработчика. При оценке соответствия критериям допустимо применять риск-ориентированный подход и соответствующую оценку выполнения критериев.

7.4.2.1. Условия для реализации безопасного жизненного цикла ОО

Условия для перехода к оценке соответствия требованиям безопасности процесса разработки ОО:

•ОО не должен использоваться в составе объектов критической информационной инфраструктуры (КИИ)[2], которым присвоена категория значимости;

[2] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

- Разработчик должен иметь документированный процесс разработки, тестирования и эксплуатации[3], включая описания реализуемых мер, контролей безопасности (security controls) и проверок по обеспечению информационной безопасности, а также документированные процедуры планирования процессов безопасной разработки;

- Разработчик должен иметь документированный процесс управления версиями и изменениями программного обеспечения;

- Инфраструктура Разработчика, на которой выполняются процессы разработки, тестирования и развертывания, а также среды постоянной эксплуатации финансовой организации, должна соответствовать требованиям ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» с учетом определенного уровня защиты информации для финансовой организации[4] и иметь соответствующее подтверждение оценки соответствия по ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия». При этом инфраструктурные системы (платформы) и решения по обеспечению информационной безопасности и соответствующие требования к ним должны быть документированы в достаточном виде для подтверждения и формирования автотестов и контрольных процедур (например, в рамках интеграционного тестирования с компонентами СОИБ, СМИБ).

7.4.2.2. Критерии для реализации безопасного жизненного цикла ОО

Критерии, при выполнении которых возможен переход к оценке соответствия требованиям безопасности процесса разработки ОО:

---

[3] В случае если в качестве Разработчика выступает финансовая организация.

[4] В случае если в качестве Разработчика выступает финансовая организация.

- состав команды, участвующей в реализации безопасного жизненного цикла ОО, должен иметь необходимые компетенции, в том числе предусматривать наличие специализированных ролей, соответствующих ролевой модели в пункте 7.4.3.2.3 настоящего раздела, включая роли аналитика ИБ (специалиста по безопасности прикладного программного обеспечения и приложений, также встречаются наименования «Application Security», «AppSec») и Security Champion[5] – члена команды с высокой осведомленностью в вопросах обеспечения информационной безопасности, имеющего определенные компетенции в области безопасности прикладного программного обеспечения и принципов безопасной разработки;

- должно быть обеспечено наличие специального программного обеспечения для реализации процессов жизненного цикла безопасной разработки, включая программные средства автоматической проверки правил кодирования, инструменты статического, динамического и композиционного анализа кода программы, обеспечения условий непрерывности процесса разработки и тестирования, автоматизации процессов тестирования, управления недостатками и запросами на изменение разрабатываемого ПО, а также переноса и взаимодействия между средами, использования общих ресурсов в условиях обеспечения информационной безопасности;

- функциональные требования и описание реализации ОО должны быть документированы в степени, позволяющей определить основные функции (в частности функции безопасности), роли, применяемые архитектурные, технологические и технические решения, в том числе по обеспечению информационной безопасности программного обеспечения.

---

[5] Security Champion – активный член команды, как правило, не являющийся сотрудником подразделения информационной безопасности, который вводит и поддерживает в рамках командных практик лучшие практики по обеспечению информационной безопасности, идентификации рисков ИБ и т.д. Такой член команды может сочетать роль Security Champion с ролью разработчика, тестировщика и др.

7.4.2.3.Определение условий для проведения мероприятий по оценке соответствия

Условиями для проведения мероприятий по оценке соответствия процесса разработки ОО требованиям безопасности являются:

- успешное прохождение этапов (задач) жизненного цикла ОО;
- получение формального заключения (результатов прохождения контрольных мероприятий по безопасности) о соответствии требованиям информационной безопасности от ответственных лиц на каждом этапе (задаче);
- получение документального подтверждения успешного переноса ОО в среду промышленной эксплуатации.

Разработчик самостоятельно определяет частоту проведения оценки соответствия ОО требованиям настоящего раздела, но не реже срока, установленного нормативными правовыми актами. При этом Разработчик оценивает риски самостоятельно, и основанием для проведения оценки могут, например, служить:

- изменения в составе средств обеспечения безопасной разработки кода, включая средства обеспечения информационной безопасности (например, замена либо добавление нового анализатора исходного кода);
- изменения ролевой модели процесса разработки;
- изменения в подсистемах обеспечения ИБ, компонентах ИБ ОО;
- изменения функционала ОО;
- изменения ролевой модели ОО;
- выявления/устранения недостатка и (или) запроса на изменение ОО;
- необходимость формирования дополнительных событий аудита информационной безопасности ОО;
- разработка ОО, обрабатывающего ранее не предусмотренный тип информации ограниченного доступа, подлежащей защите в соответствии с требованиями нормативных документов;

- изменение схем взаимодействия ОО со смежными системами;
- расширение или изменение структуры базы данных ОО;
- мажорный релиз ОО.

Указанный перечень не является исчерпывающим и при необходимости может быть расширен. В целях принятия обоснованного решения о проведении оценки необходимо включать вышеуказанные сведения в функциональные требования, что в том числе позволит более качественно подготовить техническое задание на разработку (или иной аналогичный документ: частное техническое задание, задание на разработку и т.д.).

При этом заключением по итогам проведенной оценки будут являться результаты контрольных мероприятий по ИБ с учетом соответствия ОО функциональным требованиям безопасности (ФТБ), результаты проведенных контролей безопасности (security controls), работ по анализу уязвимостей и тестированию защищенности ОО при подтвержденном общем соответствии документированному процессу безопасной разработки.

7.4.3. Процесс безопасного жизненного цикла ОО

7.4.3.1. Описание процесса безопасного жизненного цикла ОО. Определение методологии процесса безопасного жизненного цикла ОО

Под методологией безопасного жизненного цикла ОО в настоящем документе понимается соблюдение совокупности принципов, правил, мер, требований, а также последовательности выполнения мероприятий жизненного цикла для целей предотвращения появления и устранения уязвимостей в ОО, поддержания доверия к ОО на всем протяжении жизненного цикла ОО и обеспечения необходимого и достаточного уровня безопасности ОО.

В зависимости от выбора методологии функционирования конкретных установленных Разработчиком процессов работы команды безопасного жизненного цикла ОО возможно параллельное и одновременное выполнение

ряда мероприятий, включая контрольные, и этапов жизненного цикла ОО, в связи с чем по тексту настоящего раздела вместо термина «этап» жизненного цикла будет использован термин «задача».

В состав задач безопасного жизненного цикла ОО входят:

- Задача «Организационная подготовка» – в данной задаче определяются требования по подготовке, организации, поддержанию актуальности и развитию реализации процесса безопасного жизненного цикла ОО, в том числе требования по периодическому анализу текущего статуса реализации процессов РБПО, по периодическому анализу потребностей в ресурсах, необходимых для реализации процессов РБПО, к организационной модели команды, ролевому составу, ответственности, компетенциям участников команды и планам по развитию их профессиональных навыков, знаний и компетенций;
- Задача «Формирование требований к ОО» – в данной задаче формулируются функциональные и нефункциональные требования к разрабатываемому ОО, включая требования к обеспечению информационной безопасности ОО и используемых секретов;
- Задача «Архитектура и проектирование ОО» – в данной задаче разрабатываются архитектурное решение и проектное описание ОО с учетом результатов моделирования угроз и разработки описания поверхности атаки;
- Задача «Реализация (разработка) ОО» – в данной задаче осуществляются непосредственное кодирование и процесс реализации ОО;
- Задача «Тестирование ОО» – в данной задаче проводятся: проверка реализации ОО и качества его исполнения на соответствие функциональным и нефункциональным требованиям, в том числе требованиям к обеспечению информационной безопасности ОО, экспертиза исходного кода, статический анализ исходного кода и динамический анализ кода программы, функциональное и нефункциональное тестирование.

Взаимосвязь задач безопасного жизненного цикла ОО с шагами ориентировочного процесса безопасного жизненного цикла ОО приведена в таблице 7.4.3.1.

Таблица 7.4.3.1. Связь задач безопасного жизненного цикла в соответствии с ГОСТ Р 56939-2024[6] и шагов процесса безопасного жизненного цикла ОО раздела 7.4 ПЗ

Задача безопасного жизненного цикла	**Процесс безопасного жизненного цикла в соответствии с ГОСТ Р 56939-2024**	**Шаг процесса (Приложение В)**
Задача «Организационная подготовка»	- Планирование и определение области применения процессов РБПО (в том числе, анализ текущего статуса реализации процессов РБПО, анализ потребностей в ресурсах для реализации РБПО, планирование развития процессов РПБО); - Обучение сотрудников Разработчика в соответствии с планом обучения по актуальной программе обучения; - Повышение осведомленности сотрудников Разработчика в части обеспечения информационной безопасности при реализации процессов РБПО; - Подготовка руководств по РБПО и документирование	- Планирование процессов РБПО; Определение потребностей, в т.ч. в ресурсах; - Определение ролевого состава команды; - Организация обучения и повышения осведомленности сотрудников Разработчика; - Повышение квалификации и осведомленности членов команды Разработчика; - Разработка руководств по процессам РБПО; - Формирование и поддержание в актуальном состоянии правил кодирования; - Обеспечение безопасности

[6] ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования. (утв. и введен в действие Приказом Росстандарта от 24.10.2024 N 1504-ст)

	процессов безопасного жизненного цикла ОО; - Организация процесса управления конфигурациями программного обеспечения (как для ОО, так и в рамках ПО, которое реализует процессы РБПО); - Организация процесса управления недостатками и запросами на изменение; - Организация формирования и поддержания в актуальном состоянии правил кодирования; - Разработка схемы безопасной сборочной среды, описания ожидаемых результатов сборки ПО, ролевой модели доступа к среде сборки ПО; - Организация процесса управления уязвимостями; - Организация процесса управления секретами; - Осуществление контроля взаимоотношений с внешними поставщиками продуктов и услуг; - Организация работы службы технической поддержки.	инфраструктур разработки и тестирования; - Организация управления конфигурациями ПО, в том числе ОО; - Организация процессов управления секретами (в том числе, формирование парольной политики); - Организация процесса управления уязвимостями; - Организация процесса управления недостатками и запросами на изменение. ***<u>Не отражено в приложении В, так как выходит за пределы стандартного спринта разработки</u>***
Задача «Формирование требований к ОО»	- Разработка, актуализация, учет, предъявление и пересмотр общих	- Анализ рисков нарушения ИБ, формирование перечня мер для

	требований и требований безопасности к ОО;	минимизации рисков нарушения ИБ; - Разработка требований ИБ к ОО; - Согласование общих требований к ОО;
Задача «Архитектура и проектирование ОО»	- Контроль реализации изменений ОО, элементов ОО и документации на ОО; - Разработка проектной документации с учетом аспектов ИБ; - Разработка и уточнение модели угроз ОО; - Описание и уточнение описания поверхности атаки; - Формирование и уточнение перечня целей (функциональных подсистем, модулей (компонентов ПО и их интерфейсов) для проведения проверок безопасности ОО; - Определение инструментов статического, динамического и композиционного анализа, их конфигураций и сценариев проведения тестирований; - Осуществление анализа и контроля использования кода ОО, полученного через цепочки поставок.	- Разработка модели угроз ОО, описания поверхности атаки; - Разработка архитектурных и проектных решений по ИБ в соответствии с требованиями к ОО; - Контроль выполнения требований ИБ в архитектурной и проектной реализациях ОО; - Актуализация и доработка требований по ИБ; - Формирование перечня целей для проведения проверок безопасности ОО; - Проверка соответствия стороннего программного обеспечения требованиям ИБ ОО; - Определение инструментов статического, динамического и композиционного анализа и их

		конфигураций, их настройка и контроль конфигураций.
Задача «Реализация (разработка) ОО»	- Определение перечня элементов конфигурации для контроля реализации изменений ОО; - Осуществление контроля изменений и контроля запросов на изменение ОО, используя средства автоматизации; - Разработка эксплуатационной документации с учетом аспектов ИБ, учет сведений об эксплуатационной документации на ОО.	- Актуализация и уточнение разработанных артефактов по обеспечению ИБ ОО; - Анализ стороннего программного обеспечения на наличие уязвимостей; - Композиционный анализ заимствованных компонентов ОО; - Управление секретами - Управление целостностью ОО и его компонент; - Управление доступом к ОО; - Управление изменениями ОО и контроль запросов на изменение в части ИБ; - Статический анализ кода ОО на уязвимости ИБ; - Разработка автоматизированных тестов по безопасности; - Разработка эксплуатационной документации на ОО в части ИБ, согласование эксплуатационной

		документации на ОО; - Проверки выполнения требований ИБ и контролей ИБ; - Экспертиза исходного кода ОО на выполнение требований к ОО, включая требования ИБ;
Задача «Тестирование ОО»	- Экспертиза исходного кода программы; - Статический анализ исходного кода ОО; - Динамический анализ и фаззинг-тестирование исходного кода ОО; - Композиционный анализ заимствованных компонентов ОО; - Функциональное тестирование ОО; - Нефункциональное тестирование ОО; - Устранение выявленных при тестировании ОО ошибок и уязвимостей.	- Актуализация и уточнение разработанных артефактов по обеспечению ИБ ОО; - Определение требований к проведению тестов ИБ и подготовка плана и сценариев тестирования; - Автоматизированное тестирование безопасности ОО; - Функциональное тестирование ОО; - Проведение нефункционального тестирования ОО; - Статический анализ исходного кода ОО; - Динамический анализ и фаззинг-тестирование; исходного кода ОО - Интеграционное тестирование с сервисами СОИБ; - Устранение выявленных при тестировании и анализе кода ОО

		ошибок и уязвимостей; - Приемо-сдаточные испытания.
Задача «Подготовка и перенос ОО в промышленную эксплуатацию»	- Осуществление анализа и фиксация степени влияния на безопасность ОО неустраненных ошибок; - Обеспечение возможности проверки пользователями целостности ОО; - Обеспечение хранения и поставки ОО пользователям вместе с эксплуатационной документацией с фиксацией версий ОО и документации.	- Управление версиями ОО; - Контроль целостности ОО; - Тестирование на проникновение; - Проверка выполнения требований ИБ ОО; - Управление резервированием; - Управление конфигурациями ОО.
Задача «Эксплуатация и сопровождение ОО»	- Контроль изменений и отслеживание состояния перечня элементов конфигурации в рамках управления конфигурациями ОО; - Анализ рисков нарушения ИБ, пересмотр и актуализация Модели угроз и нарушителя, описания поверхности атаки, корректировка и актуализация требований по ИБ, инициирование соответствующих запросов на изменение ОО; - Обработка запросов пользователей с последующим анализом ошибок функционирования,	- Управление конфигурациями ОО; - Управление и реагирование на уязвимости ИБ ОО; - Управление изменениями ОО; - Мониторинг и тестирование безопасности ОО; - Проведение периодических контролей безопасности ОО; - Управление уязвимостями при эксплуатации ОО; - Анализ рисков нарушения ИБ; - Актуализация артефактов ОО в части ИБ. ***<u>Не отражено в</u>***

	используя средства автоматизации; - Анализ, оценка актуальности и критичности выявленных при обработке запросов пользователей уязвимостей в ОО; - Реализация процесса управления и реагирования на уязвимости (включая информирование пользователей ОО о выявленных уязвимостях и способах их нейтрализации до разработки обновлений безопасности); - Поиск ошибок и уязвимостей на всем протяжении эксплуатации и технической поддержки; оценка выявленных ошибок на предмет наличия уязвимостей.	***приложении В, так как выходит за пределы стандартного спринта разработки***
Задача «Вывод из эксплуатации ОО»	- Информирование пользователя о прекращении технической поддержки ОО (версии ОО); - Архивирование информации, содержащейся в ОО; - Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение	- Контроль соблюдения правил и процедур обеспечения ИБ при выводе из эксплуатации ОО; - Архивирование информации, содержащейся в ОО; - Уничтожение (стирание) данных и остаточной информации с машинных носителей

	машинных носителей информации.	информации и (или) уничтожение машинных носителей информации. ***Не отражено в приложении В, так как выходит за пределы стандартного спринта разработки***

- Задача «Подготовка и перенос ОО в промышленную эксплуатацию» – в данной задаче требуется проверить выполнение требований ИБ и готовность ОО к переносу в промышленную эксплуатацию, корректно перенести версию ОО в среду эксплуатации;
- Задача «Эксплуатация и сопровождение ОО» – в данной задаче реализуются мониторинг, обновление, сопровождение и сопутствующая эксплуатация ОО;
- Задача «Вывод из эксплуатации ОО» – в данной задаче производится снятие с эксплуатации ОО.

Ориентировочный процесс безопасного жизненного цикла ОО (типовой спринт разработки, перед началом которого реализованы мероприятия организации и планирования процессов разработки безопасного ОО, обучения сотрудников, первичного проектирования архитектуры ОО и первичного моделирования угроз для ОО) приведен на схемах в Приложении В к настоящему ПЗ.

7.4.3.2. Организационная подготовка

7.4.3.2.1. Определение требований к организации процессов безопасного жизненного цикла ОО

Ответственность за организацию процесса безопасного жизненного цикла ОО должна быть возложена на руководство Разработчика. Разработчик должен документировать процесс безопасного жизненного цикла ОО. В том

числе, на этапе организации процесса безопасного жизненного цикла ОО необходимо обеспечить документирование и регламентацию следующих подпроцессов:

- планирования процесса безопасного жизненного цикла ОО;
- организации обучения и повышения осведомленности работников финансовой организации (Разработчика);
- управления конфигурациями ОО, а также программного обеспечения, которое реализует процессы безопасного жизненного цикла;
- управления недостатками и запросами на изменение ОО;
- обеспечения безопасности сборочной среды ОО;
- обеспечения безопасности используемых секретов, используемых в процессе безопасного жизненного цикла;
- формирования и предъявления требований безопасности к ОО;
- безопасная поставка ОО;
- обеспечение поддержки ОО при эксплуатации пользователями;
- реагирование на информацию об уязвимостях;
- поиск уязвимостей в ОО при эксплуатации;
- обеспечение безопасности при выводе ОО из эксплуатации;

В рамках планирования процессов безопасного жизненного цикла ОО должны быть проведены/зафиксированы:

1) Периодический (не менее 1 раза в год) анализ текущего статуса реализации процессов РБПО.

Необходимо определить общий свод применимых требований ИБ для разработки, определить приоритеты требований и поддерживать требования в актуальном состоянии. Такими требованиями могут являться:

- требования ИБ для программного обеспечения, а также методы безопасного кодирования, которым должны следовать разработчики;

•требования к архитектуре программного обеспечения (например, создание модульного кода для упрощения повторного использования кода, изоляция функций безопасности от других функций во время выполнения кода);

•требования ИБ для защиты инфраструктуры разработки (требования обеспечения безопасности сборочной среды, автоматизированные рабочие места разработчиков, репозиториев кода, инструментов сред разработки и переноса между средами).

•требования ИБ при взаимоотношениях со сторонними поставщиками ПО и услуг.

Разработчик должен проводить внутренние проверки выполнения мер по обеспечению безопасности жизненного цикла ОО, позволяющие установить, что реализуемые меры соответствуют требованиям настоящего ПЗ.

2) Периодический (не менее 1 раза в квартал) анализ потребностей в ресурсах, необходимых для реализации процессов РБПО.

Разработчик должен предусмотреть выделение ресурсов, необходимых для реализации мер по поддержанию безопасного жизненного цикла ОО, и обеспечить организацию развития профессиональных навыков, знаний и компетенций участников команды, повышение осведомленности в отношении информационной безопасности в рамках процессов РБПО.

3) План развития процессов и план реализации РБПО.

Разработчик должен на постоянной основе осуществлять совершенствование процессов, связанных с обеспечением безопасного жизненного цикла ОО, на основе:

•несоответствий, выявленных в ходе внутренних проверок;

•изменения рисков нарушения информационной безопасности как во внутренней модели угроз и нарушителя самого Разработчика (при наличии), так и в моделях угроз и нарушителя для ОО;

•изменения целей применения и объектов применения процессов РБПО.

4) Область применения процессов РБПО.

Разработчик должен определять область применения процессов РПБО. Описание области применения процессов РБПО должно содержать состав ПО (версии, модули, компоненты, функциональные подсистемы и т.п.), в отношении которого должны быть реализованы процессы РБПО, с обоснованием выбора указанного состава ПО.

В рамках организации обучения и повышения осведомленности работников ФО Разработчик должен:

- проводить анализ (не менее 1 раза в квартал) существующих (доступных для анализа) практик, документов, обучающих курсов и тренингов по РБПО;
- проводить обучение (не менее 1 раза в пять лет) сотрудников типовым практикам РБПО с учетом актуальных потребностей;
- осуществлять определение критериев пересмотра программ обучения (курсов, тренингов и т.п.);
- повышать осведомленность на регулярной основе (не менее 1 раза в год) сотрудников о возможных типовых угрозах, ошибках и уязвимостях в разрабатываемом ОО, механизмах их недопущения или минимизации вероятности их возникновения, порядке сопровождения ОО и управления жизненным циклом.

В рамках управления конфигурациями ОО, а также программного обеспечения, которое реализует процессы безопасного жизненного цикла Разработчик должен:

- определить перечень элементов конфигурации, подлежащих отслеживанию в рамках управления конфигурацией ОО.
- осуществлять контроль реализации изменений ОО, документации на ОО, других элементов, подлежащих отслеживанию в рамках управления конфигурацией ОО (элементов конфигурации).
- проводить анализ и согласование результатов тестирования

безопасности системы управления конфигурациями.

В рамках управления недостатками и запросами на изменение ОО Разработчик должен:

- осуществлять контроль реализации изменений, связанных с недостатками ОО.
- осуществлять контроль реализации запросов на изменение в рамках жизненного цикла ОО.
- использовать средства автоматизации для управления недостатками и запросами на изменение разрабатываемого ОО.

В рамках управления обеспечением безопасности сборочной среды ОО Разработчик должен:

- осуществлять фиксацию описания ожидаемых результатов сборки ОО, прав доступа к среде сборки ОО и хранилищу результатов сборки ОО и ролей пользователей, участвующих в процессе сборки ОО.
- разработать схему сборочной среды.
- обеспечивать регистрацию всех выполняемых действий при сборке ОО в журналах аудита; журналы аудита должны храниться способом, обеспечивающим их целостность; сроки хранения журналов аудита должны быть зафиксированы в регламенте обеспечения безопасности сборочной среды.
- обеспечивать хранение результатов сборки ОО в выделенном хранилище – хранилище результатов сборки ОО.
- если применимо, обеспечивать повторяемость сборки ОО (идемпотентность).

В рамках обеспечения безопасности используемых секретов, используемых в процессе безопасного жизненного цикла Разработчик должен:

- использовать секреты.
- проверять код и конфигурационные файлы ОО в целях исключения хранения секретов, в том числе для вносимых изменений в ОО.
- для хранения, управления и предоставления секретов использовать систему управления секретами.

В рамках обеспечения формирования и предъявления требований безопасности к ОО Разработчик должен:

- предъявлять к ОО требования безопасности.
- вести учет предъявленных требований безопасности и контроль однозначности трактования и непротиворечивости набора требований безопасности ОО.
- осуществлять пересмотр набора требований безопасности при внесении изменений в ОО.

В рамках безопасной поставки программного обеспечения пользователям, Разработчиком должны быть проведены:

- фиксация версий поставляемого пользователям ОО и соответствующей поставляемой документации.
- организация хранения копий версий поставляемого пользователям ОО и соответствующей поставляемой документации.
- поставка ОО вместе с эксплуатационной документацией, содержащей, как минимум, описание штатного функционирования ОО, параметров настроек (конфигураций) ОО и среды функционирования, действий по установке и настройке средства, как с точки зрения штатного функционирования, так и с точки зрения обеспечения безопасности.
- контроль корректности поставляемых версий и целостности ОО.

В рамках обеспечения поддержки программного обеспечения при эксплуатации пользователями Разработчиком должны быть проведены:

- организация работы службы технической поддержки.
- разработка процедуры оповещения пользователей о выпуске обновлений (включая обновления безопасности) и необходимости их установки.
- обучение специалистов службы технической поддержки работе с поставляемым ОО, особенностям его установки и функционирования, ограничениям и указаниям по эксплуатации.
- разработка процедуры информирования пользователей ОО о выявленных уязвимостях и способах реализации мер по их нейтрализации до разработки обновлений безопасности, устраняющих уязвимость, по установленным каналам взаимодействия.

В рамках реагирования на информацию об уязвимостях Разработчиком должны быть проведены:

- обработка поступающих запросов от пользователей (через службу технической поддержки, по иным каналам взаимодействия) с последующим анализом ошибок функционирования на предмет наличия уязвимостей (в случае получения таких запросов).
- организация использования средств автоматизации при обработке поступающих запросов и при последующем анализе (например, система управления изменениями, система отслеживания ошибок, система управления задачами и т.п.).
- осуществление анализа информации о найденных уязвимостях в ОО на предмет подтверждения наличия/отсутствия уязвимостей и принятие решения о необходимости их устранения по результатам оценки.
- осуществление оценки актуальности и критичности уязвимости с точки зрения безопасности ОО (в случае получения информации об уязвимости ОО из внешнего источника) и принятие решения о необходимости ее устранения по результатам оценки.
- документирование процесса реагирования на выявленные уязвимости и

их устранение.

В рамках формирования и поддержания в актуальном состоянии правил кодирования Разработчик должен:

- обеспечивать эффективную и единообразную организацию оформления и использования исходного кода в соответствии с предъявляемыми к ОО требованиями.
- при разработке ОО использовать программные средства автоматической проверки правил кодирования.
- предъявлять требования к качеству кода и осуществлять контроль их выполнения, в том числе с применением программных средств автоматической проверки правил кодирования.

7.4.3.2.2 Особенности обеспечения безопасности инфраструктур разработки и тестирования

Разработчик должен обеспечить защиту компонентов сред разработки ОО от рисков нарушения ИБ. Важно реализовать защиту компонентов инфраструктуры ОО от НСД, нарушений целостности и доступности, обеспечив при этом:

- разделение сред на изолированные сегменты (например, среда разработки, среда тестирования, среда интеграционного тестирования, среда промышленной эксплуатации);
- разграничение доступа к результатам исследований и тестирования, обеспечение защищенного хранения соответствующей информации и антивирусную защиту;
- разграничение доступа к исходному коду;
- регистрацию в журналах аудита событий информационной безопасности.

Процессы РБПО должны быть интегрированы с применяемыми в сегментах разработки ОО (среда разработки, тестирования и т.п.) системами и средствами обеспечения информационной безопасности.

Разработчик должен обеспечить контроль целостности всего программного кода и размещение доступных механизмов для контроля в соответствующих средах:

- обеспечить контроль целостности хранимых в репозиториях файлов;
- обеспечить доступность инструментов контроля целостности программного кода;
- обеспечить защиту от несанкционированного доступа и нарушения целостности ресурса хранения контрольных сумм релизов.

Разработчик должен обеспечить архивирование копий каждого выпуска и всех его компонентов (код, файлы пакетов, сторонние библиотеки, документация и информация о проверке целостности выпуска):

- обеспечить хранение всех файлов релизов в репозитории;
- обеспечить реализацию требований ИБ по защите репозитория от НСД, нарушений целостности и доступности;
- внедрить процесс управления версиями и обеспечить наличие соответствующих инструментов автоматизации процесса;
- обеспечить резервное копирование хранилищ, репозиториев, баз знаний проекта/платформы.

7.4.3.2.3 Определение ролевого состава команды и ролей, ответственных за обеспечение информационной безопасности в процессах безопасного жизненного цикла ОО

При формировании команды проекта необходимо определить роли и обязанности участников процессов жизненного цикла ОО, а также определить организационную модель команды, ролевой состав, ответственность,

компетенции участников команды и планы развития их профессиональных навыков, знаний и компетенций.

Базовое определение ролей, связанных с обеспечением информационной безопасности:

- роль Аналитик ИБ (может являться специалистом по ИБ прикладного программного обеспечения и приложений, также может именоваться «Application Security», «AppSec» – обычно роль выполняет сотрудник подразделения информационной безопасности и защиты информации);
- роль Security Champion, сформированная внутри команды для специалиста с высокой осведомленностью в вопросах обеспечения информационной безопасности, имеющего также определенные компетенции в области безопасности прикладного программного обеспечения и принципов безопасной разработки, который может занимать в команде любую роль, кроме Аналитика ИБ.

С целью предупреждения возникновения рисков нарушения ИБ не допускается совмещение исполняющих и контролирующих функций в рамках одной роли при выполнении контрольного мероприятия процесса РПБО.

В качестве необходимых компетенций для ролей Аналитика ИБ и Security Champion рекомендуется учитывать, в том числе, следующие навыки:

- владение риск-ориентированным подходом при анализе рисков нарушения информационной безопасности;
- знание актуальных рисков, уязвимостей, атак, принципов, методов и средств обеспечения ИБ, требований и лучших практик обеспечения ИБ;
- понимание безопасного жизненного цикла ОО и лучших практик гибких подходов к разработке, внедрению и тестированию;
- знание принципов, методов и средств обеспечения ИБ, уязвимостей ПО, методов проведения атак;
- умение работать с инструментальными средствами безопасности;
- умение собирать и анализировать информацию о событиях безопасности, поступающую из различных источников, участие в разработке

правил выявления инцидентов информационной безопасности.

Ориентировочное распределение контрольных мероприятий процессов РБПО, по ролям, связанным с обеспечением информационной безопасности, приведено в таблице 7.4.3.2.3

Таблица 7.4.3.2.3. Ориентировочное распределение контрольных мероприятий по ролям.

Этап	Контрольные мероприятия и контроли по ИБ	
	Аналитик ИБ	Security Champion (SecChamp)
Задача "Формирование требований к ОО"	Участие (согласование) в разработке общих требований к ОО	Участие (согласование) в разработке общих требований к ОО
	Разработка, предъявление требований ИБ к ОО	Согласование и учет требований ИБ к ОО
	Анализ рисков нарушения ИБ, формирование перечня мер для минимизации рисков нарушения ИБ	
Задача "Архитектура и проектирование ОО"	Разработка и уточнение модели угроз ОО, описания поверхности атаки	
	Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ОО	
	Анализ архитектурных и проектных решений на соответствие требованиям ИБ к ОО	Участие в анализе архитектурных и проектных решений на соответствие требованиям ИБ к ОО
	Контроль выполнения требований ИБ в предложенных архитектурной и проектной реализациях ОО	Мониторинг выполнения требований ИБ в предложенных архитектурной и проектной реализациях ОО
	Актуализация и доработка требований по ИБ, предъявляемых к ОО после уточнения архитектурных и проектных решений	
	Анализ проектной документации ОО на соответствие требованиям ИБ ОО	
	Формирование и уточнение перечня целей (функциональных подсистем, модулей (компонентов ПО и их интерфейсов) для	Формирование и уточнение перечня целей (функциональных подсистем, модулей (компонентов ПО и их интерфейсов) для проведения проверок безопасности ОО

	проведения проверок безопасности ОО	
	Проверка соответствия стороннего программного обеспечения требованиям ИБ ОО	Проверка соответствия стороннего программного обеспечения требованиям ИБ ОО
	Подготовка предложений/согласование инструментов статического, динамического и композиционного анализа, их конфигураций	Определение инструментов статического, динамического и композиционного анализа, их конфигураций
	Участие в настройке и контроль конфигураций инструментов согласно определенным конфигурациям	Участие в настройке и мониторинг конфигураций инструментов согласно определенным конфигурациям
Задача "Реализация (разработка) ОО"	Уточнение модели угроз ОО, описания поверхности атаки	
	Актуализация требований, проектных и архитектурных решений по ИБ для ОО	Инициация изменения требований, проектных и архитектурных решений по ИБ для ОО
	Актуализация проектной документации в части требований ИБ к ОО	Актуализация проектной документации в части требований ИБ к ОО
	Анализ стороннего программного обеспечения на наличие уязвимостей	Анализ стороннего программного обеспечения на наличие уязвимостей
	Обработка результатов композиционного анализа заимствованных компонентов ОО (при необходимости)	Композиционный анализ заимствованных компонентов ОО
	Контроль безопасного использования секретов	Обеспечение безопасного использования секретов
	Контроль и мониторинг доступа к исходному коду ОО	Обеспечение контроля доступа к исходному коду ОО и размещение доступных механизмов для контроля доступа в соответствующих средах
	Контроль и мониторинг целостности программного кода ОО	Обеспечение контроля целостности программного кода ОО и размещение доступных механизмов для контроля в соответствующих средах
	Контроль изменений ОО и запросов на изменение ОО в части ИБ (кроме информирования)	Формирование перечня и настройка элементов конфигурации для контроля изменений ОО

		Осуществление контроля изменений и запросов на изменение ОО в части ИБ и информирование Аналитика ИБ
	Статический анализ кода ОО на уязвимости ИБ и/или обработка результатов статического анализа кода ОО на уязвимости ИБ. Участие в устранении выявленных при статическом анализе кода ОО ошибок и уязвимостей	Статический анализ кода ОО на уязвимости ИБ. Участие в устранении выявленных при статическом анализе кода ОО ошибок и уязвимостей
	Разработка автоматизированных тестов по безопасности	
	Разработка эксплуатационной документации на ОО в части ИБ. Согласование эксплуатационной документации на ОО	Разработка эксплуатационной документации на ОО в части ИБ
	Проверки выполнения требований ИБ и контролей ИБ до размещения исходных кодов и компонентов ОО в базы знаний и репозитории разработки	Экспертиза исходного кода ОО на выполнение требований к ОО, включая требования ИБ
Задача "Тестирование ОО"	Актуализация эксплуатационной документации на ОО в части ИБ	Инициация изменения эксплуатационной документации на ОО в части ИБ
	Определение требований к проведению тестов ИБ и подготовка плана и сценариев тестирования	
	Обработка результатов автоматизированного тестирования безопасности ОО	Проведение автоматизированного тестирования безопасности ОО
	Участие в функциональном тестировании ОО	Проведение функционального тестирования ОО
	Участие в нефункциональном тестировании ОО	Проведение нефункционального тестирования ОО
	Обработка результатов динамического анализа и фаззинг-тестирования исходного кода ОО	Динамический анализ и фаззинг-тестирование исходного кода ОО
	Обработка результатов статического анализа исходного кода ОО.	Статический анализ исходного кода ОО

	Обработка результатов интеграционного тестирования с сервисами СОИБ	Проведение интеграционного тестирования с сервисами СОИБ
	Участие в устранении выявленных при тестировании и анализе кода ОО ошибок и уязвимостей	Устранение выявленных при тестировании и анализе кода ОО ошибок и уязвимостей
	Участие в приемо-сдаточных испытаниях. Оценка выполнения требования ИБ и контролей ИБ ОО для перевода ОО в эксплуатацию	Участие в приемо-сдаточных испытаниях
Задача "Подготовка и перенос ОО в промышленную эксплуатацию"		Контроль корректности поставляемых версий и целостности ОО
	Анализ и согласование результатов тестирования на проникновение	Тестирование на проникновение
		Резервное копирование каждого выпуска ОО и всех его компонентов
	Проверка ОО на соответствия выполнения требований ИБ ОО, проектной и эксплуатационной документации	Проверка ОО на соответствия выполнения требований ИБ ОО, проектной и эксплуатационной документации
Задача "Эксплуатация и сопровождение ОО"	Мониторинг ОО на наличие уязвимостей ИБ	Мониторинг ОО на наличие уязвимостей
		Периодический анализ и тестирование кода ОО для выявления ранее не обнаруженных уязвимостей и ошибок
	Реализация процесса управления и реагирования на уязвимости ИБ (включая информирование пользователей ОО о выявленных уязвимостях ИБ и способах их нейтрализации до разработки обновлений безопасности)	Реализация процесса управления и реагирования на уязвимости ИБ (включая информирование пользователей ОО о выявленных уязвимостях ИБ и способах их нейтрализации до разработки обновлений безопасности)
	Анализ рисков нарушения ИБ, пересмотр и актуализация Модели угроз и нарушителя, описания поверхности атаки, корректировка и актуализация требований по ИБ, инициирование соответствующих запросов на изменение ОО	

	Анализ, оценка актуальности и критичности выявленных при обработке запросов пользователей уязвимостей ИБ в ОО	Анализ, оценка актуальности и критичности выявленных при обработке запросов пользователей уязвимостей и ошибок в ОО
Задача "Вывод из эксплуатации ОО"	Контроль соблюдения правил и процедур обеспечения ИБ при выводе из эксплуатации ОО	Контроль соблюдения правил и процедур обеспечения ИБ при выводе из эксплуатации ОО
		Архивирование информации, содержащейся в ОО
	Уничтожение данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации	Уничтожение данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации

При необходимости могут быть созданы иные роли и изменены обязанности для существующих ролей в рамках безопасного жизненного цикла разработки ОО. Отдельные мероприятия в процессах РБПО, по усмотрению Разработчика, могут проводиться коллегиально. Разработчику необходимо осуществлять периодический (не менее 1 раза в год) пересмотр состава ролей и их обязанностей.

7.4.3.5. Задача "Формирование требований к ОО"

Задачи ИБ, которые должны быть выполнены командой DevSecOps: определение требований ИБ, определение основных векторов атак, планирование первичного конфигурирования и настройки решений по обеспечению ИБ. На основе результатов вышеперечисленного формируется окончательный свод требований по информационной безопасности и проводится оценка соответствия на этапе проверки технического решения.

Состав контрольных мероприятий безопасности, выполняемых в рамках задачи "Формирование требований к ОО", приведен в таблице 7.4.3.5.

Таблица 7.4.3.5. - Контрольные мероприятия безопасности, выполняемые в рамках задачи "Формирование требований к ОО"

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
Участие (согласование) в разработке общих требований к ОО	Участие (согласование) в разработке общих требований к ОО на соответствие требованиям безопасности ОО	Согласование всеми заинтересованным и сторонами, как внешними, так и внутренними, соответствия набора требований и их достаточности	Перечень требований ИБ и мер защиты ОО. Актуальные требования к ОО, включая требования по ИБ.	Согласованные требования к ОО, включая требования по ИБ	Инструменты командной работы	
Разработка, предъявление требований ИБ к ОО	Разработка требований безопасности к ОО	Определение актуальных требований ИБ и мер защиты по	Регламент управления требованиями безопасности ПО. Перечень векторов	Перечень требований ИБ и мер защиты ОО. Обновление базы	Инструментальные средства для проектирования	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
		набору мер из базы знаний по ИБ и по определенному ранее набору слабостей ОО (CWE), наборов актуальных атак CAPEC, уязвимых конфигураций CPE для ОО	атак для ОО (описание поверхности атак) Набор слабостей ОО (CWE), перечень связанных уязвимостей (CVE) и конфигураций, имеющих уязвимости (CPE). Перечень требований по ИБ	знаний ИБ и актуализация состава мер и требований в ней. Требования к ОО, включая требования по ИБ		
	Предъявление требований безопасности к ОО	Предъявление требований безопасности ОО, предоставление требований безопасности исполнителям, отслеживание процесса предоставления, получения и выполнения требований безопасности ОО.	Регламент управления требованиями безопасности ПО. Требования к ОО, включая требования по ИБ	Перечень предъявленных требований безопасности ОО, сведения о принятии требований и их изменении, статус реализации требований и его изменения	Инструментальные средства для проектирования. Система управления изменениями/задачами	Набор требований безопасности ОО должен содержать следующую информацию: - идентификатор требования безопасности ОО; - формулировку требования безопасности ОО; - дату предъявления требований безопасности ОО; - приоритет/важность требования безопасности ОО; - предполагаемые сроки реализации;

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
						- сведения о сотрудниках (подразделениях), предъявивших требования; - сведения о сотрудниках (подразделениях), принявших требования к реализации. Требования должны трактоваться однозначно и не противоречить друг другу
	Актуализация требований безопасности к ОО	Осуществление пересмотра набора требований безопасности при изменениях ОО	Регламент управления требованиями безопасности ПО. Требования к ОО, включая требования по ИБ Перечень требований ИБ и мер защиты ОО	Актуальный набор требований к ОО, включая требования по ИБ	Инструментальные средства для проектирования	Критерии пересмотра требований безопасности ПО определяются Регламентом управления требованиями безопасности ПО.
Согласование и учет требований ИБ к ОО	Согласование требований ИБ к ОО	Согласование соответствия набора требований ИБ к ОО и их	Перечень требований ИБ и мер защиты ОО. Актуальные требования к ОО,	Согласованные требования к ОО, включая	Инструменты командной работы	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
		достаточности	включая требования по ИБ	требования по ИБ		
	Учет требований ИБ к ОО	Осуществление автоматизированного учета предъявленных требований безопасности ОО, включающего сведения о принятии требований и их изменении, статус реализации требований и его изменение	Перечень предъявленных требований безопасности ОО, сведения о принятии требований и их изменении, статус реализации требований и его изменения	Перечень требований безопасности ОО	Инструментальные средства для проектирования. Система управления изменениями/задачами	Требования безопасности ОО необходимо формировать однозначно трактуемыми и непротиворечивыми. Критерии однозначности трактования и непротиворечивости набора требований безопасности ПО определяются экспертным методом
Анализ рисков нарушения ИБ, формирование перечня мер для минимизации рисков нарушения ИБ	Анализ рисков ИБ, моделирование угроз	Анализ рисков нарушения ИБ ОО и определение мер минимизации выявленных рисков. Определение основных векторов атак для ОО с учетом специфики разрабатываемого ОО и инфраструктуры	Перечень требований ИБ к ОО. Перечень актуальных атак и векторов атак для ОО. Отчеты о выявленных уязвимостях предыдущих релизов (при наличии)	Перечень векторов атак для ОО (входит в состав описания поверхности атаки) Набор слабостей ОО (CWE), перечень связанных уязвимостей (CVE) и конфигураций, имеющих уязвимости (CPE)	Инструментальные средства для проектирования	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
		размещения. Подготовка информации для формирования модели угроз и нарушителя				

7.4.3.6. Задача "Архитектура и проектирование ОО"

Задачи ИБ, которые должны быть выполнены командой DevSecOps: разработка и выбор решений по информационной безопасности в соответствии с требованиями по обеспечению ИБ, анализ решений на соответствие требованиям ИБ, определение осуществимости выполнения требований ИБ, определение достаточности требований по ИБ для архитектуры ОО, разработка модели угроз и описания поверхности атаки ОО, проверка соответствия стороннего ПО требованиям безопасности, формирование и уточнение перечня целей для проведения проверок безопасности ОО.

Состав контрольных мероприятий безопасности, выполняемых в рамках задачи "Архитектура и проектирование ОО", приведен в таблице 7.4.3.6.

Архитектура должна определять подход к безопасности на стадии проектирования ОО и на уровне кода ОО. На этапе проектирования архитектуры необходимо осуществлять моделирование угроз, включающее в себя анализ актуальных рисков и атак:

- архитектура ОО должна быть гибкой, должна допускать относительно простое, без коренных структурных

изменений, развитие инфраструктуры и изменение конфигурации используемых средств, наращивание функций и ресурсов ОО в соответствии с расширением сфер и задач его применения;

- должны быть обеспечены операционная надежность, безопасность функционирования системы при различных видах угроз и надежная защита данных от ошибок проектирования, разрушения или потери информации, а также авторизация пользователей, управление рабочей загрузкой, резервированием данных и вычислительных ресурсов, максимально быстрым восстановлением функционирования ОО;
- ОО должна сопровождать актуальная документация, обеспечивающая квалифицированную эксплуатацию и возможность развития ОО.

Наиболее важными являются следующие принципы построения архитектуры ОО:

- проектирование ОО на принципах открытых систем, следование признанным стандартам, использование апробированных решений, иерархическая организация ОО способствуют прозрачности и хорошей управляемости ОО;
- непрерывность защиты, невозможность преодолеть защитные средства, исключение спонтанного или вызванного перехода в небезопасное состояние, обеспечение того, что защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ в систему или ее часть;
- эшелонирование обороны, разнообразие защитных средств, простота и управляемость ОО и системой его безопасности.

Таблица 7.4.3.6. - Контрольные мероприятия безопасности, выполняемые в рамках задачи "Архитектура и

проектирование ОО"

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
Разработка модели угроз ОО, описание поверхности атаки	Разработка модели угроз ОО, описание поверхности атаки	Разработка модели угроз ОО, описание поверхности атаки для снижения количества недостатков, связанных с особенностями реализации архитектуры ОО и логики его функционирования, выработка мер по нейтрализации угроз безопасности, связанных с особенностями реализации архитектуры ОО	Архитектурное решение ОО (описание проектируемого решения). Описание технической инфраструктуры размещения ОО (текущая документация на инфраструктуру платформы с описанием применяемых технологий: ОС, СУБД, сетевые компоненты, компоненты виртуализации, карта информационного взаимодействия и т.д.). Перечень векторов атак для ОО (входит в состав описания поверхности атаки). Набор слабостей ОО (CWE), перечень связанных	Модель угроз безопасности информации ОО, включающая совокупность угроз безопасности, актуальных для разрабатываемого ОО. Описание поверхности атаки, включающее совокупность потенциальных областей воздействия на информационную (автоматизированную) систему с использованием разрабатываемого ОО	Инструментальные средства для проектирования. Инструмент для определения поверхности атаки	При составлении перечня угроз безопасности и их описания рекомендуется учитывать положения ГОСТ Р 58412-2019, а также угрозы безопасности информации Банка данных угроз безопасности информации ФСТЭК России, других источников (например, методологии STRIDE, Open Web Application Security Project (OWASP), DREAD и пр.)

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
			уязвимостей (CVE) и конфигураций, имеющих уязвимости (CPE)			
Разработка и выбор архитектурных и проектных решений по ИБ в соответствии с требованиями к ОО	Подготовка архитектурных и проектных решений	Разработка и выбор архитектурных и проектных решений по ИБ. Описание проектных решений по ИБ для ОО	Требования к ОО, включая требования безопасности к ОО. Модель угроз безопасности информации ОО	Требования по ИБ уточнены для архитектуры ОО (в том числе, требования к архитектуре сред разработки, инструментам и пр.) Разработаны и документированы архитектурные и проектные решения по ИБ для ОО. Могут быть уточнены требования к ОО, включая требования безопасности к ОО	Инструментальные средства для проектирования	
Анализ архитектурных и проектных решений на соответствие	Уточнение архитектурного/проектного решения	Анализ проектной и архитектурной реализаций ОО на соответствие требованиям ИБ к	Требования к ОО, включая требования безопасности к ОО. Архитектурные и проектные решения	Требования по ИБ определены (доработаны) для архитектуры ОО. Уточнены и	Инструментальные средства для проектирования	Необходимо учитывать особенности программирования (используемые языки и технологии

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
требованиям ИБ к ОО		ОО и доработка соответствующих решений или требований по ИБ, предъявляемых к ОО	ОО, включая решения по ИБ ОО	документированы архитектурные и проектные решения для ОО в соответствии с требованиями ИБ к ОО		программирования, используемые библиотеки, фреймворки, готовые решения)
Контроль выполнения требований ИБ в предложенных архитектурной и проектной реализациях ОО	Контроль выполнения требований ИБ	Контроль реализации требований проекта архитектуры ОО и доработка соответствующих требований к ОО или архитектурных и проектных решений, в том числе по ИБ, предъявляемых к ОО	Требования к ОО, включая требования по ИБ (в части архитектуры ОО). Архитектурные и проектные решения для ОО в соответствии с требованиями ИБ к ОО.	Требования по ИБ выполняются для архитектуры ОО	Инструментальные средства для проектирования	
Актуализация и доработка требований по ИБ, предъявляемых к ОО после уточнения архитектурных	Уточнение архитектурного/проектного решения	Доработка соответствующих требований по ИБ, предъявляемых к ОО	Модель угроз безопасности информации ОО. Скорректированные архитектурные и проектные решения для ОО, в соответствии с	Актуальные требования по ИБ к ОО. Актуальные архитектурные и проектные решения для ОО, в соответствии с требованиями ИБ к	Инструментальные средства для проектирования	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
и проектных решений			требованиями ИБ к ОО.	ОО		
Анализ проектной документации ОО на соответствие требованиям ИБ ОО	Разработка проектной документации	Разработка проектной документации с учетом актуальных требований ИБ к ОО, архитектурных и проектных решений, учитывающих требования ИБ	Актуальные требования к ОО, включая требования по ИБ. Актуальные архитектурные и проектные решения для ОО, в соответствии с требованиями ИБ к ОО	Проектная документация ОО	Инструментальные средства для проектирования	
Проверка соответствия стороннего программного обеспечения требованиям ИБ ОО	Проверка соответствия стороннего программного обеспечения требованиям ИБ ОО	Определение набора требований безопасности и включение их в документы о приобретении, контракты на программное обеспечение и другие соглашения с третьими сторонами. Снижение риска, связанного с использованием приобретенных	Набор требований безопасности и описывающие документы о приобретении, контракты на программное обеспечение и другие соглашения с третьими сторонами. Связанные с безопасностью критерии выбора стороннего программного обеспечения.	Перечень критериев выбора стороннего ПО дополнен требованиями ИБ. Включение требований ИБ в типовые соглашения и договоры. Включение в SLA обязательства по устранению выявленных уязвимостей	Инструментальные средства для проектирования	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
		программных модулей и сервисов, которые являются потенциальными источниками дополнительных уязвимостей	Доказательства полученных у поставщиков коммерческих программных модулей того, что их программное обеспечение соответствует требованиям безопасности			
Формирование и уточнение перечня целей (функциональных подсистем, модулей (компонентов) ПО и их интерфейсов) для проведения проверок безопасности ОО	Формирование перечня целей для проведения проверок безопасности ОО	Сформировать перечень целей (функциональных подсистем, модулей (компонентов) ПО и их интерфейсов) для проведения проверок безопасности ОО с учетом архитектуры ПО, результатов моделирования угроз и выполнения анализа поверхности атаки	Архитектурные и проектные решения для ОО, проектная документация, описание среды функционирования ОО, модель угроз безопасности информации ОО, описание поверхности атаки	Актуальный перечень целей для проведения проверок безопасности ОО	Инструменты командной работы	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
Определение инструментов статического, динамического и композиционного анализа и их конфигураций, их настройка и контроль конфигураций	Определение инструментов статического, динамического и композиционного анализа и их конфигураций, их настройка и контроль конфигураций	Определение инструментов статического, динамического и композиционного анализа и их конфигураций, их настройка и контроль конфигураций	Описание архитектуры ОО, регламенты проведения статического, динамического и композиционного анализов, модель угроз безопасности информации ОО, описание поверхности атаки, актуальный перечень целей для проведения проверок безопасности ОО, перечень зависимостей ОО, информация об инфраструктуре функционирования (средах эксплуатации, разработки и тестирования), языках программирования, конфигурациях, влияющих на совместимость инструментов	Перечень инструментов статического, динамического и композиционного анализов. Конфигурации и параметры настройки инструментов	Инструментальные средства для проектирования	

7.4.3.7. Задача "Реализация (разработка) ОО"

Задачи ИБ, которые должны быть выполнены командой DevSecOps: оценка соответствия ОО требованиям и решениям по ИБ, создание тестовых сценариев, первичное конфигурирование и настройка решений по обеспечению ИБ, управление версиями и изменениями, принятие решения о допустимости выпуска ОО в тестовую среду в отношении защищенности ОО.

Состав контрольных мероприятий безопасности, выполняемых в рамках задачи "Реализация (разработка) ОО", приведен в таблице 7.4.3.7.

На текущей задаче происходит разработка исходных текстов программы, автоматизированных тестов, проведение статического анализа кода программы.

Для обеспечения управления версиями и контроля за изменениями ОО, а также в целях:

- маркировки создаваемых промежуточных версий ОО,
- идентификации исходных текстов программ, используемых для реализации ОО,

рекомендуется создать процесс управления версиями и изменениями ОО, включая промежуточные версии, версии исходных кодов и т.д.

Таблица 7.4.3.7. - Контрольные мероприятия безопасности, выполняемые в рамках задачи "Реализация (разработка) ОО"

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
Уточнение модели угроз ОО, описания	Уточнение модели угроз,	Уточнение модели угроз ОО для	Отчет по анализу риска нарушения	Актуальная модель угроз безопасности	Системы планирования	Необходимость уточнения модели

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
поверхности атаки	описания поверхности атаки	изменяемого в ходе разработки ОО кода. Уточнение описания поверхности атаки для изменяемого в ходе разработки кода ОО	ИБ. Отчет о результатах статического анализа исходных текстов. Отчет о проверке сторонних компонентов	информации ОО и актуальное описание поверхности атаки	работ и управления задачами	угроз и описания поверхности атаки устанавливается на основе проведенного анализа риска нарушения ИБ
Актуализация требований, проектных и архитектурных решений по ИБ для ОО	Актуализация требований, проектных и архитектурных решений по ИБ	Осуществление пересмотра набора требований безопасности, проектных и архитектурных решений по ИБ	Набор требований ИБ к ОО. Перечень актуальных атак и векторов атак для ОО. Проектная документация на ОО. Архитектурное решение по ИБ для ОО	Актуализированная проектная документация на ОО. Актуализированное архитектурное решение по ИБ для ОО	Системы планирования работ и управления задачами	
Актуализация проектной документации в части требований ИБ к ОО	Актуализация проектной документации	Проведение пересмотра и актуализации проектной документации в части требований ИБ к ОО	Проектная документация на ОО. Актуальные требования, проектные и архитектурные решения по ИБ для ОО	Актуализированная проектная документация в части требований ИБ к ОО.	Системы планирования работ и управления задачами	
Анализ стороннего программного обеспечения	Контроль сторонних компонентов ОО	Выявление уязвимостей в сторонних компонентах программного обеспечения, в том	Перечень процессов, компонентов инфраструктуры, частей разрабатываемого	Отчет о результатах сканирования, решение о применимости сторонних	Инструмент проверки сторонних компонентов. Инструмент	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
		числе сторонних библиотек до размещения их в базы знаний и репозитории разработки	ОО, зависящих от сторонних поставщиков, перечень компонентов стороннего программного обеспечения	компонентов	антивирусной защиты информации	
Композиционный анализ заимствованных компонентов ОО	Контроль сторонних компонентов ОО	Создание условий для снижения рисков наследования уязвимостей и недекларированных возможностей при использовании заимствованного кода в коде ОО	Регламент композиционного анализа	Перечень зависимостей ОО. Отчет о результатах анализа заимствованных компонентов.	Инструменты композиционного анализа	В результате проведения композиционного анализа необходимо проводить корректирующие воздействия по устранению уязвимостей в зависимостях ОО
Контроль безопасного использования секретов	Безопасное использование секретов	Проверка кода ОО и конфигурационных файлов ОО на предмет включения секретов. Осуществление хранения, управления и предоставление секретов	Регламент использования секретов. Описание архитектуры ОО.	Обеспечение безопасности используемых секретов	Статические анализаторы. Инструменты сканирования для поиска секретов	
Контроль и мониторинг доступа к исходному коду ОО	Контроль доступа к исходному коду ОО	Обеспечение контроля доступа к хранимым в репозиториях файлам. Обеспечение доступности инструментов контроля	Регламент доступа к исходному коду ПО и обеспечения его целостности.	Отчеты и предупреждения безопасности	Инструменты контроля и управления доступом	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
		доступа к программному коду. Обеспечение защиты от несанкционированного доступа к исходному коду ОО				
Контроль и мониторинг целостности программного кода ОО	Обеспечение целостности программного кода ОО	Обеспечение контроля целостности хранимых в репозиториях файлов. Обеспечение доступности инструментов контроля целостности программного кода. Обеспечение защиты от несанкционированного доступа и нарушения целостности ресурса хранения контрольных сумм релизов	Регламент доступа к исходному коду ПО и обеспечения его целостности. Контрольные суммы релизов	Отчеты и предупреждения безопасности	Модули безопасности репозитория системы управления версиями и изменениями	
Контроль изменений ОО и запросов на изменение ОО в части ИБ (кроме информирования)	Контроль управления изменениями	Контроль реализации изменений ОО. Контроль реализации запросов на изменение в процессе разработки	Регламент управления запросами на изменение ПО	Отчеты, подтверждающие реализации управления запросами на изменение ПО	Системы управления изменениями, системы управления задачами	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
Статический анализ кода ОО на уязвимости ИБ или обработка результатов статического анализа кода ОО на уязвимости ИБ. Участие в устранении выявленных при статическом анализе кода ОО ошибок и уязвимостей	Статический анализ исходного кода	Анализ исходного текста программ на потенциальные уязвимости, анализ результатов, которые влияют на решение об изменении статуса кода. Устранение выявленных при статическом анализе кода ОО ошибок и уязвимостей	Регламент проведения статического анализа исходного кода ПО. Исходный текст программы, известные уязвимости и недостатки	Отчет о результатах статического анализа исходных текстов, фиксация результатов сканирования в базу знаний ИБ, рекомендуемые меры по снижению рисков, решение о переходе к следующему этапу жизненного цикла	Инструменты статического анализа исходных текстов программ	Необходимо проводить статический анализ с использованием инструментов статического анализа с регистрацией всех предупреждений о потенциальных ошибках, полученных по результатам работы инструментов статического анализа
Разработка автоматизированных тестов по безопасности	Разработка наборов автоматизированных тестов	Разработка подробных процедур тестирования, подготовка тестовых данных, тестовых сценариев, конфигураций тестовых сценариев для функций обеспечения информационной безопасности и решений информационной безопасности	План тестирования ОО. Набор требований ИБ к ОО.	Исполняемые файлы автоматизированных тестов (исполняемый код тестовых сценариев ИБ – «авто-тесты»). Документ о процедуре тестирования, тестовые сценарии ИБ	Инструментальные средства для тестирования. Инструменты командной работы	
Разработка эксплуатационной	Разработка эксплуатацио	Подготовка эксплуатационной	Регламент безопасной поставки	Эксплуатационная документация,	Системы планирования	Сведения о поставляемой

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
документации на ОО в части ИБ. Согласование эксплуатационной документации на ОО	нной документации на ОО	документации для ОО, содержащей, как минимум, описание штатного функционирования ОО, параметров настроек (конфигураций) ОО и среды функционирования, действий по установке и настройке средства с точки зрения обеспечения безопасности. Фиксация сведений об эксплуатационной документации в поставляемой документации к ОО	ПО пользователям	содержащая требования ИБ	работ и управления задачами. Инструменты командной работы	эксплуатационной документации на ОО должны быть зафиксированы в электронном виде или на физическом носителе в поставляемой документации к ОО
Проверки выполнения требований ИБ и контролей ИБ до размещения исходных кодов и компонентов ОО в базы знаний и репозитории разработки	Проверка перед размещением ОО и компонентов ОО в базы знаний и репозитории разработки	Анализ результатов статического сканирования и отчетов о проверке сторонних компонентов	Результаты сборки, отчет статического сканирования, отчет о проверке сторонних компонентов, план проекта	Заключение по контролям для принятия решений об изменении статуса кода/переносе в другую среду	Инструменты проведения контроля ИБ	
Экспертиза исходного кода ОО на выполнение требований к ОО, включая требования	Экспертиза исходного кода ОО	Обеспечение соответствия исходного кода ОО предъявляемым к нему требованиям.	Регламент проведения экспертизы исходного кода ПО. Исходный текст	Результаты проведения экспертизы исходного кода ОО	Инструменты проведения контроля ИБ	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
ИБ.		Проведение экспертизы определенных областей кода ОО (в первую очередь для модулей (компонентов) ОО, составляющих поверхность атаки)	программы ОО. Набор требований ИБ к ОО			

7.4.3.8. Задача "Тестирование ОО"

Задачи ИБ, которые должны быть выполнены командой DevSecOps: оценка соответствия ОО требованиям ИБ, автоматизированное тестирование безопасности ОО, устранение выявленных при тестировании и анализе кода ОО ошибок и уязвимостей, приемочные испытания, оценка остаточных рисков ИБ, принятие решения о допустимости выпуска ОО в промышленную эксплуатацию в отношении защищенности ОО и допустимости остаточных рисков ИБ.

Состав контрольных мероприятий безопасности, выполняемых в рамках задачи "Тестирование ОО", приведен в таблице 7.4.3.8.

Под тестированием в общем виде, если не предусмотрено уточнение вида, понимаются следующие варианты: модульное тестирование, функциональное тестирование, интеграционное тестирование, системное тестирование, регрессионное тестирование, приемочное тестирование, тестирование производительности, изоляционное/компонентное тестирование и различные тесты безопасности. В случае если в рамках определенного вида тестирования, не являющегося контрольной проверкой информационной безопасности, предусматривается включение в объем тестирования функционала СОИБ или функций безопасности, а также влияющих на них смежных компонент ОО, подразделение безопасности определяет свой уровень вовлеченности и участия.

В процессе тестирования могут применяться как ранее разработанные, так и подготовленные в рамках тестирования тесты, в которых прописываются подробные процедуры тестирования, сценарии тестирования, тестовые скрипты и тестовые данные. Автоматизированный тест можно выполнить, запустив набор тестовых скриптов или набор тестовых сценариев на конкретном инструменте тестирования без участия человека. Если полная автоматизация невозможна, рекомендуется обеспечить наивысший процент автоматизации.

В среде тестирования не рекомендуется использование реальных данных. В случае если для тестирования необходимы данные, максимально приближенные к реальным, рекомендуется формирование тестовых массивов данных путем необратимого обезличивания, маскирования и (или) искажения сведений.

Таблица 7.3.4.8. - Контрольные мероприятия безопасности, выполняемые в рамках задачи "Тестирование ОО"

Контрольные мероприятия безопасности	**Подзадача жизненного цикла**	**Описание**	**Входные данные**	**Результат**	**Необходимые инструменты**	**Комментарий**
Актуализация эксплуатационной документации на ОО в части ИБ	Актуализация эксплуатационной документации	Актуализация эксплуатационной документации, в том числе в части требований ИБ к ОО, проектным решениям по ИБ к ОО, параметров и конфигурации механизмов безопасности, описания обновления ОО	Эксплуатационная документация на ОО Актуализированная проектная документация на ОО (архитектурные решения, проектные решения, конфигурации компонентов ОО)	Актуальная эксплуатационная документация	Инструментальные средства для проектирования	
Определение требований к проведению тестов ИБ и подготовка плана и сценариев тестирования	Определение требований к проведению тестирования	Согласование объемов и стратегии тестирования ОО, приоритезации задач по тестированию	Автоматизированные тесты по безопасности. Критерии ИБ к проведению тестирования по безопасности. Функциональные требования по безопасности	План и сценарии тестирования ОО в части ИБ	Инструменты командной работы	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
Автоматизированное тестирование безопасности ОО	Автоматизированное тестирование	Проведение автоматизированного тестирования с помощью специализированных автоматизированных средств, анализ результатов, которые влияют на решение об изменении статуса ОО	План и сценарии тестирования ОО Исходные модули программы, исполняемый код ОО, тестовые наборы входных данных, тестовые сценарии ИБ, автоматизированные тесты по безопасности (исполняемый код тестовых сценариев ИБ)	Отчет о тестировании (выявленные недостатки, уязвимости ИБ), рекомендуемые меры по снижению рисков	Инструментальные средства тестирования. Системы управления недостатками (ошибками, уязвимостями)	
Функциональное тестирование ОО	Функциональное тестирование	Проведение функционального тестирования	План и сценарии тестирования ОО, Регламент функционального тестирования исполняемый код ОО, тестовые наборы входных данных	Отчет о тестировании, рекомендуемые меры по снижению рисков, журналы функционального тестирования	Инструментальные средства тестирования. Системы управления недостатками (ошибками, уязвимостями)	При проведении функционального тестирования выполнять тестирование на уровне модулей (компонентов), подсистем, всего ОО в целом
Нефункциональное тестирование ОО	Нефункциональное тестирование ОО	Проведение проверки особенностей ОО, не связанных с функциональным тестированием. Обнаружение недостатков программы ОО путем выполнения нефункциональных	План и сценарии тестирования ОО. Регламент нефункционального тестирования, исполняемый код ОО, тестовые наборы входных данных	Протокол тестирования, отчеты по результатам нефункционального тестирования	Инструментальные средства тестирования. Системы управления недостатками (ошибками, уязвимостями)	В рамках нефункционального тестирования могут выполняться проверки: - сетевых взаимодействий ОО; - локальных интерфейсов взаимодействия ОО; - производительности функционирования ОО;

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
		тестов, в том числе имитирующих действия потенциального нарушителя.				- операций, выполняемых с высокими привилегиями; - работы с конфиденциальными данными; - корректности выполнения файловых операций; - реализации защищенности бинарных файлов; - реализации системы управления секретами; - реализации безопасности сетевых протоколов; - работы системы развертывания продукта; - реализации мер по устранению или снижению критичности угроз, выявленных при моделировании угроз; - возможности нарушения логики работы программы; - безопасности реализации механизмов аутентификации и авторизации; - безопасности обработки данных, полученных от потенциального нарушителя;

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
						- безопасности реализации клиентской и серверной частей ОО
Динамический анализ и фаззинг-тестирование исходного кода ОО	Динамический анализ исходного кода ОО	Выполнение динамического анализа безопасности ОО, анализ результатов, которые влияют на решение об изменении статуса кода ОО	План и сценарии тестирования ОО Регламент проведения динамического анализа кода ПО, исполняемый код ОО, тестовые наборы входных данных	Отчет о тестировании, рекомендуемые меры по снижению рисков	Инструментальные средства тестирования. Системы управления недостатками (ошибками, уязвимостями)	
	Фаззинг-тестирование исходных текстов ОО	Исследование ОО, направленное на оценку его свойств и основанное на передаче случайных или специально сформированных входных данных, отличных от данных, предусмотренных алгоритмом работы ОО	План и сценарии тестирования ОО, исполняемый код ОО, тестовые наборы входных данных			
Статический анализ исходного кода ОО	Статический анализ исходного кода ОО	Автоматическое сканирование и анализ кода для выявления недостатков и	План и сценарии тестирования ОО, Регламент проведения статического анализа исходного кода ПО,	Отчеты по результатам проведения статического анализа	Инструментальные средства тестирования. Системы управления	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
		уязвимостей ИБ	исполняемый код ОО, сценарии проведения тестирования		недостатками (ошибками, уязвимостями)	
Проведение и обработка результатов интеграционного тестирования с сервисами СОИБ	Интеграционное тестирование с компонентами СОИБ	Проведение интеграционного тестирования для проверки взаимодействия ОО, в том числе конфигураций ОО, конфигураций модулей взаимодействия СОИБ, тестирование интеграции ОО в СОИБ	План и сценарии тестирования ОО, исполняемый код ОО, тестируемые программные блоки	Отчет о тестировании, рекомендуемые меры по снижению рисков	Инструментальные средства тестирования. Системы управления недостатками (ошибками, уязвимостями)	Отчет должен показать сравнение результатов теста в соответствии с архитектурным и проектным решением по ИБ
Устранение выявленных при тестировании и анализе кода ОО ошибок и уязвимостей	Устранение ошибок и уязвимостей	Устранение выявленных в процессе тестирования ошибок	Отчеты о тестировании, протоколы тестирований, журналы тестирований ОО	Отчет о повторном тестировании	Инструментальные средства тестирования. Системы управления недостатками (ошибками, уязвимостями)	
Участие в приемо-сдаточных испытаниях. Оценка	Приемочное тестирование	Проведение тестирования безопасности в рамках комплексного приемочного	План и сценарии тестирования ОО, исполняемый код ОО, тестовые наборы входных данных	Протокол приемо-сдаточных испытаний	Инструментальные средства тестирования. Системы управления	Данные тесты проводятся на окончательной конфигурации. При проведении тестирования на

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
выполнения требования ИБ и контролей ИБ ОО для перевода ОО в эксплуатацию.		тестирования для определения уровня готовности ОО к последующей эксплуатации			недостатками (ошибками, уязвимостями)	проникновение могут использоваться не только реестры известных угроз информационной безопасности и уязвимостей ОО, но и базы со сценариями эксплуатации самих уязвимостей
	Проверка соответствия ОО перед переносом в среду промышленной эксплуатации	Анализ результатов тестирования и отчетов о проверке	Отчеты о тестировании, отчет о проверке функционального тестирования ОО, протоколы тестирований	Заключение по контролям для принятия решений об изменении статуса кода ОО/переносе в другую среду	Инструментальные средства тестирования. Системы управления недостатками (ошибками, уязвимостями)	

7.4.3.9. Задача "Подготовка и перенос ОО в промышленную эксплуатацию"

Задачи ИБ, которые должны быть выполнены командой DevSecOps: контроль корректности версий и целостности ОО при передаче в среду промышленной эксплуатации, контроль выполнения требований ИБ ОО в проектной и эксплуатационной документации.

Состав контрольных мероприятий безопасности, выполняемых в рамках задачи "Подготовка и перенос ОО в промышленную эксплуатацию", приведен в таблице 7.4.3.9.

На этапе подготовки и переноса в промышленную эксплуатацию компоненты ОО проверяются на целостность и источник происхождения компонентов ОО. При успешном прохождении проверки ОО компоненты с положительным результатом контроля ИБ передаются на хранение в репозиторий. Состав передаваемых на хранение компонентов ОО содержит в том числе: образы контейнеров, образы виртуальных машин, бинарные исполняемые файлы, результаты тестов, результаты сканирования безопасности, сценарии развертывания, сценарии управления конфигурациями, документацию на ОО.

Также в данной задаче осуществляются развертывание выпусков ОО, включая различные компоненты ОО, в промышленную эксплуатацию и контроль всех операций.

Таблица 7.4.3.9. - Контрольные мероприятия безопасности, выполняемые в рамках задачи "Подготовка и перенос ОО в промышленную эксплуатацию"

Контрольные мероприятия безопасности	**Подзадача жизненного цикла**	**Описание**	**Входные данные**	**Результат**	**Необходимые инструменты**	**Комментарий**
Контроль корректности поставляемых версий и целостности ОО	Доставка собранных компонентов ОО, получаемых в процессе разработки	Отправка собранных компонентов ОО в хранилище компонентов с обеспечением контроля корректности версий и целостности	Выпуск ОО	Новый выпуск в хранилище собранных компонентов	Система хранения собранных компонентов	Обеспечить защиту от несанкционированного доступа и нарушения целостности ресурса хранения контрольных сумм выпусков
Тестирование на	Оценка защищенности	Тестирования на проникновение	Развернутый ОО	Отчет о тестировании,	Инструментальные средства	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
проникновение	ОО	охватывает все аспекты функционирования подсистем ОО в среде эксплуатации		перечень недостатков и уязвимостей для проведения анализа и обработки в рамках процесса управления уязвимостями		
Резервное копирование каждого выпуска ОО и всех его компонентов	Резервное копирование	Контроль корректности резервного копирования хранилищ, репозиториев, баз знаний проекта/платформы	Правила резервного копирования исходного кода ПО. Доступ к системе резервных копий, компоненты ОО.	Актуальные резервные копии компонентов ОО	Система управления резервным копированием	
Проверка ОО на соответствия выполнения требований ИБ ОО, проектной и эксплуатационной документации	Принятие решения о выпуске ОО	Итоговые сверки результатов проведенных контролей безопасности и контрольных мероприятий по безопасности для принятия решения о выпуске ОО в промышленную эксплуатацию	Требования к ОО, включая требования ИБ. Проектная документация, Отчетные артефакты: отчеты о тестировании, отчеты о проверке безопасности, компоненты ОО, заключение по контролям для принятия решений об	Решение о выпуске в промышленную эксплуатацию	Система оркестрации, непрерывной интеграции/непрерывной доставки	Компоненты ОО помечаются маркером финального выпуска, если принято положительное решение

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
			изменении статуса кода/переносе в другую среду			

7.4.3.10. Задача "Эксплуатация и сопровождение ОО"

Задачи ИБ, которые должны быть выполнены командой DevSecOps: контроль состава, мест размещения и параметров настроек технических защитных мер, контроль выполнения правил эксплуатации технических защитных мер, включая правила обновления и управления, периодическая оценка защищенности ОО.

Состав контрольных мероприятий безопасности, выполняемых в рамках задачи "Эксплуатация и сопровождение ОО", приведен в таблице 7.4.3.10.

Таблица 7.4.3.10. - Контрольные мероприятия безопасности, выполняемые в рамках задачи "Эксплуатация и сопровождение ОО"

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
Контроль изменений и отслеживание состояния перечня элементов	Оценка защищенности ОО	Контроль изменений ПО, документации на ПО, других элементов, подлежащих отслеживанию в	Регламент управления изменениями. Перечень элементов конфигурации, подлежащих отслеживанию в рамках	Актуальный перечень элементов конфигурации, подлежащих отслеживанию	Системы управления изменениями	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
конфигурации в рамках управления конфигурациями ОО		рамках управления конфигурацией ПО (элементов конфигурации).	управления конфигурацией ПО			
Мониторинг ОО на наличие уязвимостей	Сопровождение ОО	Поиск ошибок и уязвимостей на всем протяжении эксплуатации и технической поддержки. Оценка выявленных ошибок на предмет наличия уязвимостей.	Общеизвестные базы данных уязвимостей, списки рассылки безопасности, отчеты об уязвимостях	Отчет осуществления мониторинга	Инструментальные средства мониторинга	
Реализация процесса управления и реагирования на уязвимости ИБ (включая информирование пользователей ОО о выявленных уязвимостях ИБ и способах их нейтрализации	Сопровождение ОО	Обеспечение выявления и устранения уязвимостей при эксплуатации ОО. Осуществление обработки поступающих запросов от пользователей ОО (через службу технической поддержки, по иным каналам взаимодействия) с	Регламент управления и реагирования на уязвимости ИБ	Отчеты о реализации требований, подтверждающие реализацию процесса управления и реагирования на уязвимости ИБ	Системы планирования работ и управления задачами. Системы управления изменениями. Системы управления уязвимостями и недостатками	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
до разработки обновлений безопасности)		последующим анализом ошибок функционирования на предмет наличия уязвимостей				
Анализ, оценка актуальности и критичности выявленных при обработке запросов пользователей уязвимостей и ошибок в ОО.	Оценка защищенности ОО	Осуществление оценки актуальности и критичности уязвимости с точки зрения безопасности ОО и принятие решения о необходимости ее устранения по результатам оценки	Регламент управления и реагирования на уязвимости ИБ. Перечень уязвимостей и ошибок, выявленных при обработке запросов пользователей	Отчеты о реализации требований, подтверждающие выполнение анализа информации о найденных уязвимостях в ПО	Системы планирования работ и управления задачами. Системы управления изменениями. Системы управления уязвимостями и недостатками	
Периодический анализ и тестирование кода ОО для выявления ранее не обнаруженных уязвимостей и ошибок	Оценка защищенности ОО	Проведение анализа и осуществление тестирования кода ОО	Перечень контрольных мероприятий безопасности. Требования к ОО, включая требования по ИБ, Проектная и эксплуатационная документация Развернутый ОО, исполняемый код, тестовые наборы входных данных,	Отчеты о выявленных уязвимостях. Скорректированная оценка векторов и актуальных атак на ОО, описания поверхности атаки ОО	Инструментальные средства оценки защищенности	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
			тестовые сценарии			
Анализ рисков нарушения ИБ, пересмотр и актуализация модели угроз и нарушителя, описания поверхности атаки, корректировка и актуализация требований по ИБ, инициирование соответствующих запросов на изменение ОО	Оценка защищенности ОО	Уточнение модели угроз ОО в процессе эксплуатации ОО. Уточнение описания поверхности атаки в процессе эксплуатации ОО. Инициирование запросов на изменение ОО при необходимости внесения корректировок в ОО	Модель угроз безопасности информации ОО. Описание поверхности атаки ОО. Требования ИБ к ОО	Отчет по анализу риска нарушения ИБ. Актуальная модель угроз и нарушителя ОО. Актуальное описание поверхности атаки ОО	Системы планирования работ и управления задачами. Системы управления изменениями.	

7.4.3.11. Задача "Вывод из эксплуатации ОО"

Задачи ИБ, которые должны быть выполнены командой DevSecOps: контроль соблюдения правил и процедур

обеспечения ИБ при снятии с эксплуатации ОО, архивирование информации, содержащейся в ОО, гарантированное уничтожение (стирание) данных с носителей информации.

Состав контрольных мероприятий безопасности, выполняемых в рамках задачи "Вывод из эксплуатации ОО", приведен в таблице 7.4.3.11.

Мероприятия, указанные в таблице, проводятся владельцами ОО совместно с ИТ-специалистами под обязательным и непосредственным контролем офицера безопасности. Офицер безопасности должен быть указан в документированном решении о выводе ОО из промышленной эксплуатации в обязательном порядке в качестве лица, осуществляющего контроль мероприятий.

Таблица 7.4.3.11. - Контрольные мероприятия безопасности, выполняемые в рамках задачи "Вывод из эксплуатации ОО"

Контрольные мероприятия безопасности	**Подзадача жизненного цикла**	**Описание**	**Входные данные**	**Результат**	**Необходимые инструменты**	**Комментарий**
Контроль соблюдения правил и процедур обеспечения ИБ при выводе из эксплуатации ОО	Проведение работ по выводу ОО из эксплуатации	Документирование решения о выводе ОО из промышленной эксплуатации	Регламент вывода ПО из эксплуатации. Решение о выводе ОО из промышленной эксплуатации	Документированное решение о выводе ОО из промышленной эксплуатации. Недопущение реализации угроз безопасности, связанных с эксплуатацией неподдерживаемой версии ОО	Инструменты командной работы	

Контрольные мероприятия безопасности	Подзадача жизненного цикла	Описание	Входные данные	Результат	Необходимые инструменты	Комментарий
Архивирование информации, содержащейся в ОО	Проведение работ по выводу ОО из эксплуатации	Архивирование информации, содержащейся в ОО, должно осуществляться в случае принятия решения о ее возможном дальнейшем использовании	Файлы и компоненты ОО	Заархивированные файлы и компоненты ОО	Система управления архивированием и резервным копированием	
Уничтожение данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации	Проведение работ по выводу ОО из эксплуатации	В случае принятия решения осуществляется уничтожение данных и остаточной информации с машинных носителей информации	Документированное решение о выводе ОО из промышленной эксплуатации	Уничтоженные файлы и компоненты ОО	Инструментальные средства, работающие с данными	Данная операция подлежит документированию в соответствии с действующей внутренней организационно-распорядительной документацией финансовой организации

Приложение А

Расширенные компоненты функциональных требований безопасности ОО

Для ОО определены следующие компоненты функциональных требований безопасности, сформулированные в явном виде в стиле компонентов из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» (расширенные (специальные) компоненты).

А.1. Класс FAU «Аудит безопасности»

А.1.1. Генерация данных аудита безопасности (FAU_GEN)

Характеристика семейства

Семейство FAU_GEN определяет требования по регистрации возникновения событий, относящихся к безопасности, которые подконтрольны ФБО. Это семейство идентифицирует уровень аудита, перечисляет типы событий, которые потенциально должны подвергаться аудиту с использованием ФБО, и определяет минимальный объем связанной с аудитом информации, которую следует представлять в записях аудита различного типа.

Ранжирование компонентов

FAU_GEN_EXT.1 "Ассоциация защищаемой информации" ФБО не должны регистрировать в записях аудита защищаемую информацию, если иное не предусмотрено целями функционирования и техническими особенностями, а также ограничениями реализации АСБиФО.

Управление: FAU_GEN_EXT.1

Действия по управлению не определены.

Аудит: FAU_GEN_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FAU_GEN_EXT.1 "Ассоциация защищаемой информации"

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FAU_GEN_EXT.1.1 ФБО не должны регистрировать в записях аудита защищаемую информацию, если иное не предусмотрено целями функционирования и техническими особенностями, а также ограничениями реализации АСБиФО: [выбор:

пароли пользователей;

полные номера платежных карт и критичные авторизационные данные;

закрытые криптографические ключи;

[**назначение**: *другая защищаемая информация*]

].

А.2. Класс FDP «Защита данных пользователя»

А.1.2. Шифрование защищаемой информации приложения (FDP_DAR_EXT)

Характеристика семейства

Семейство FDP_DAR_EXT «Шифрование защищаемой информации приложения» определяет компоненты требований, направленные на обеспечение защиты защищаемой информации, которые хранятся и обрабатываются ОО.

Ранжирование компонентов

FDP_DAR_EXT.1 «Шифрование защищаемой информации приложения» предназначен для задания требований, связанных с тем, чтобы ОО выполнял конкретные процедуры для защиты защищаемой информации, находящиеся под контролем ОО.

Управление: FDP_DAR_EXT.1

Действия по управлению не определены.

Аудит: FDP_DAR_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FDP_DAR_EXT.1 Шифрование защищаемой информации приложения

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FDP_DAR_EXT.1.1 ФБО должны [**выбор**:

не хранить любую защищаемую информацию;

усилить предоставленную платформой функциональность для шифрования защищаемой информации;

реализовать функциональность для шифрования защищаемой информации;

определить необходимость шифрования защищаемой информации в высокопроизводительных системах с высокой критичностью по времени передачи данных;

использовать альтернативные методы зашиты защищаемой информации;

] в энергонезависимой памяти.

А.3. Класс FIA «Идентификация и аутентификация»

А.3.1. Идентификация сессий веб-приложений (FIA_IWS_EXT)

Характеристика семейства

Семейство FIA_IWS_EXT «Идентификация сессий веб-приложений» определяет компоненты требований, направленные на предотвращение некорректного использования и раскрытия идентификаторов сессий веб-приложений.

Ранжирование компонентов

FIA_IWS_EXT.1 «Идентификация сессий веб-приложений» предназначен для задания требований, связанных с предотвращением некорректного использования и раскрытия идентификаторов сессий веб-приложений.

Управление: FIA_IWS_EXT.1

Действия по управлению не определены.

Аудит: FIA_IWS_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FIA_IWS_EXT.1 Идентификация сессий веб-приложений

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FIA_IWS_EXT.1.1 ФБО должны [**уточнение**:

определить минимальную длину идентификатора в размере 8 символов]

[**выбор**:

нет идентификации сессий веб-приложений;

исключать использование предсказуемых идентификаторов сессий;

исключать возможность повторного использования идентификатора сессии (в том числе использование одинаковых идентификаторов в нескольких сессиях одного пользователя, неизменность идентификатора сессии после повторной аутентификации пользователя);

исключать возможность использования идентификатора сессии после ее завершения;

исключать возможность раскрытия идентификаторов сессий, в том числе передачу идентификаторов в незашифрованном виде, а также включение идентификаторов в запись журналов регистрации событий, в сообщения об ошибках

].

А.4. Класс FMT «Управление безопасностью»

А.4.1. Конфигурация безопасности по умолчанию (FMT_CFG_EXT)

Характеристика семейства

Семейство FMT_CFG_EXT «Конфигурация безопасности по умолчанию» определяет компоненты требований, направленные на ограничение предоставления уполномоченным пользователям функциональности ОО при его конфигурировании по умолчанию.

Ранжирование компонентов

FMT_CFG_EXT.1 «Конфигурация безопасности по умолчанию» предназначен для задания требований, связанных с предоставлением уполномоченным пользователям только ограниченной функциональности ОО при его конфигурировании по умолчанию.

Управление: FMT_CFG_EXT.1

Действия по управлению не определены.

Аудит: FMT_CFG_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FMT_CFG_EXT.1 Конфигурация безопасности по умолчанию

Иерархический для: нет подчиненных компонентов.

Зависимости: FMT_SMF.1 Спецификация функций управления.

FMT_CFG_EXT.1.1 ФБО должны при установке новых учетных данных, когда конфигурируются с учетными данными по умолчанию или без учетных данных, предоставить [**назначение**: *уполномоченные пользователи*] только ограниченную функциональность.

FMT_CFG_EXT.1.2 ФБО должны запрещать создание технологических учетных записей со стандартными паролями и иными механизмами аутентификации, использующими стандартный секрет для аутентификации, задаваемыми автоматически при установке программного обеспечения.

А.4.2. Поддерживаемый механизм конфигурации (FMT_MEC_EXT)

Характеристика семейства

Семейство FMT_MEC_EXT «Поддерживаемый механизм конфигурации» определяет компоненты требований, направленные на защиту конфигурационной информации ОО.

Ранжирование компонентов

FMT_MEC_EXT.1 «Поддерживаемый механизм конфигурации» предназначен для задания требований, связанных с тем, чтобы ОО обеспечивал соответствующими механизмами защиту параметров конфигурации (настроек) от несанкционированной модификации и использование для их хранения и установки механизмов, рекомендованных производителем платформы.

Управление: FMT_MEC_EXT.1

Действия по управлению не определены.

Аудит: FMT_MEC_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FMT_MEC_EXT.1 Поддерживаемый механизм конфигурации

Иерархический для: нет подчиненных компонентов.

Зависимости: FMT_SMF.1 Спецификация функций управления.

FMT_MEC_EXT.1.1 ФБО должны защищать хранилища параметров конфигурации (настроек) ОО от несанкционированного доступа.

FMT_MEC_EXT.1.2 ФБО должны обеспечить возможность экспорта параметров конфигурации ОО в формат, пригодный для анализа пользователем.

FMT_MEC_EXT.1.3 ФБО должны использовать для хранения и установки параметров конфигурации ОО механизмы, предусмотренные платформой.

А.5. Класс FPR «Приватность»

А.5.1. Согласие пользователей на обработку персональных данных (идентификационной информации) (FPR_ANO_EXT)

Характеристика семейства

Семейство FPR_ANO_EXT «Согласие пользователей на обработку персональных данных (идентификационной информации)» определяет компоненты требований, направленные на защиту и предотвращение злоупотребления персональными данными пользователей.

Ранжирование компонентов

FPR_ANO_EXT.1 «Согласие пользователей на обработку персональных данных (идентификационной информации)» предназначен для задания требований, связанных с тем, чтобы обработка персональных данных пользователя осуществлялась только после получения его согласия на их использование.

Управление: FPR_ANO_EXT.1

Действия по управлению не определены.

Аудит: FPR_ANO_EXT.1:

Действия или события, подвергаемые аудиту, не определены.

FPR_ANO_EXT.1 Согласие пользователей на обработку персональных данных (идентификационной информации)

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPR_ANO_EXT.1.1 ФБО должны: [**выбор**:

не обрабатывать персональную идентификационную информацию;

запрашивать согласие пользователя на обработку его персональной идентификационной информации

], защита которой требуется в соответствии с законодательством.

А.6. Класс FPT «Защита ФБО»

А.6.1. Противодействие использованию уязвимостей безопасности (FPT_AEX_EXT)

Характеристика семейства

Семейство FPT_AEX_EXT «Противодействие использованию уязвимостей безопасности» определяет компоненты требований, направленные на обеспечение противодействия возможности использования нарушителем потенциальных уязвимостей ОО.

Ранжирование компонентов

FPT_AEX_EXT.1 «Противодействие использованию уязвимостей безопасности» предназначен для задания требований, связанных с применением средств и процедур, с помощью которых ОО может противостоять действиям нарушителя по использованию потенциальных уязвимостей.

Управление: FPT_AEX_EXT.1

Действия по управлению не определены.

Аудит: FPT_AEX_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FPT_AEX_EXT.1 Противодействие использованию уязвимостей безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPT_AEX_EXT.1.1 ФБО не должны требовать отображения памяти с явными адресами, за исключением [**назначение**: *список явных исключений*].

FPT_AEX_EXT.1.2 ФБО должны [**выбор**:

не выделять никакую область памяти с разрешениями писать и выполнять;

выделять области памяти с разрешениями писать и выполнять только для [назначение: список функций, выполняющих компиляцию just-in-time]

].

FPT_AEX_EXT.1.3 ФБО должны [**выбор**:

запрещать запись пользовательской информации в системные директории;

разрешать запись пользовательской информации [назначение: список системных директорий]

].

FPT_AEX_EXT.1.4 В ФБО не должны использоваться элементы управления в графическом интерфейсе пользователя ППО, предназначенные для выполнения операций, права на выполнение которых у пользователя отсутствуют. Проверка прав на выполнение любых операций пользователя должна осуществляться таким образом, чтобы пользователь не мог повлиять на результаты такой проверки.

FPT_AEX_EXT.1.5 ФБО должны быть совместимы со средствами защиты, предоставляемыми поставщиком платформы.

FPT_AEX_EXT.1.6 ФБО не должны записывать модифицируемые пользователем файлы в директории, которые содержат исполняемые файлы, [**выбор**:

если делать так явно не предписано разработчиком;

если модифицирование проходит не пользователем

].

FPT_AEX_EXT.1.7 ФБО должны позволять смену пароля пользователем или иного используемого параметра аутентификации только после предварительной аутентификации.

FPT_AEX_EXT.1.8 ФБО должны обеспечивать предварительную инициализацию переменных и структур данных при выделении оперативной памяти.

FPT_AEX_EXT.1.9 ФБО должны исключать возможность просмотра содержимого каталогов веб-сайта в случаях, когда такой просмотр не является необходимым. Если такой просмотр и изменение необходимы, ФБО должны исключать возможность просмотра и изменения произвольного каталога веб-сайта и возможность изменения каталога веб-сайта, в котором может быть расположен исполняемый код.

FPT_AEX_EXT.1.10 ФБО [**выбор**:

не должны использовать при обработке данных в формате XML внешние сущности (External Entity), внешние параметры сущностей (External Parameter Entity) и внешние описания типа документа (External Doctype);

контролировать невозможность включения пользователем таких внешних сущностей, параметров и описаний типа документа, которые могут вызвать атаку типа XXE;

].

FPT_AEX_EXT.1.11 ОО не должен требовать для своего выполнения прав администратора операционной системы, за исключением случаев, когда такие права технически необходимы для корректного функционирования ОО.

FPT_AEX_EXT.1.12 ФБО должны предусматривать меры защиты от обратной разработки и меры по противодействию отладке ППО.

FPT_AEX_EXT.1.13 ФБО должны выполнять все значимые проверки первичных электронных документов таким образом, чтобы пользователь ППО не мог повлиять на результат проверки (например, проводить проверки реквизитов отправителя на стороне банка).

FPT_AEX_EXT.1.14 ФБО не должна использовать полученную от пользователя информацию для определения типа сущности ФБО, которая будет создана на основе полученной информации, без дополнительной проверки на допустимость создания такой сущности (противодействие атакам небезопасной десериализации).

FPT_AEX_EXT.1.15 В случае использования многопоточности ФБО должна корректно обрабатывать конкурентный доступ к информации для предотвращения модификации информации в обход проверок доступа (противодействие уязвимостям типа «состояние гонки»).

A.6.2. Использование поддерживаемых сервисов и прикладных программных интерфейсов (FPT_API_EXT)

Характеристика семейства

Семейство FPT_API_EXT «Использование поддерживаемых сервисов и прикладных программных интерфейсов» определяет компоненты требований, направленные на обеспечение применения сервисов и прикладных программных интерфейсов, разрешенных производителем платформы.

Ранжирование компонентов

FPT_API_EXT.1 «Использование поддерживаемых сервисов и прикладных программных интерфейсов» предназначен для задания требований, связанных с обеспечением применения в ОО только задокументированных разработчиком платформы сервисов и прикладных программных интерфейсов.

Управление: FPT_API_EXT.1

Действия по управлению не определены.

Аудит: FPT_API_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FPT_API_EXT.1 Использование поддерживаемых сервисов и прикладных программных интерфейсов

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPT_API_EXT.1.1 ФБО должны использовать в программном продукте только задокументированные производителем сервисы и прикладные программные интерфейсы платформы. Выбор: [назначение: использовать в

программном продукте задокументированные производителем сервисы.] [назначение: использовать доверенные самописные (сторонние) библиотеки функций противодействия использованию уязвимостей.]

FPT_API_EXT.1.2 ФБО должны использовать механизмы, предоставляемые архитектурой процессора, операционной системой и средствами компиляции кода (например, защиты от переполнения буфера, защиты от нарушения обработки исключений, защиты от исполнения кода в сегментах стека и данных, случайного размещения сегментов в адресном пространстве);

FPT_API_EXT.1.3 ФБО не должны использовать функции стандартных библиотек, уязвимых к атакам переполнения буфера, при наличии аналогичных функций со встроенной защитой.

А.6.3. Использование сторонних библиотек (FPT_LIB_EXT)

Характеристика семейства

Семейство FPT_LIB_EXT «Использование сторонних библиотек» определяет компоненты требований, направленные на ограничение использования в ОО сторонних библиотек только разрешенными к применению.

Ранжирование компонентов

FPT_LIB_EXT.1 «Использование сторонних библиотек» предназначен для задания требований, связанных с обеспечением возможности применения в ОО только разрешенных сторонних библиотек.

Управление: FPT_LIB_EXT.1

Действия по управлению не определены.

Аудит: FPT_LIB_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FPT_LIB_EXT.1 Использование сторонних библиотек

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPT_LIB_EXT.1.1 ФБО должны использовать только [**назначение**: *список разрешенных сторонних библиотек*].

А.6.4. Целостность при установке и обновлении (FPT_TUD_EXT)

Характеристика семейства

Семейство FPT_TUD_EXT «Целостность при установке и обновлении» определяет компоненты требований, направленные на обеспечение целостности компонентов ОО при его установке и обновлении.

Ранжирование компонентов

FPT_TUD_EXT.1 «Целостность при установке и обновлении» предназначен для задания требований, связанных с обеспечением наличия в ОО механизмов, обеспечивающих поддержание доверия к безопасности ОО при его установке и обновлении.

Управление: FPT_TUD_EXT.1

Действия по управлению не определены.

Аудит: FPT_TUD_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FPT_TUD_EXT.1 Целостность при установке и обновлении

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FPT_TUD_EXT.1.1 ФБО должны [**выбор**:

предоставлять возможность;

эффективно использовать платформу

], чтобы проверить обновление и установку патчей для ОО.

FPT_TUD_EXT.1.2 Программное обеспечение ОО должно распространяться с использованием формата, поддерживаемого платформой диспетчера пакетов. [выбор:

использовать средства по установке/удалению/обновлению программного обеспечения собственного производства;

использовать средства по установке/удалению/обновлению программного обеспечения стороннего производства.]

FPT_TUD_EXT.1.3 Программное обеспечение ОО должно быть упаковано таким образом, чтобы его удаление приводило к удалению всех его следов, за исключением параметров конфигурации, выходных файлов и контрольных/ регистрационных событий. [выбор:

использовать средства по установке/удалению/обновлению программного обеспечения собственного производства;

использовать средства по установке/удалению/обновлению программного обеспечения стороннего производства.]

FPT_TUD_EXT.1.4 Программное обеспечение ОО не должно загружать, изменять, заменять или обновлять [**выбор**:

при отсутствии автообновления

]

его собственный двоичный код.

FPT_TUD_EXT.1.5 Программное обеспечение ОО должно [**выбор**:

предоставлять возможность,

эффективно использовать платформу

], чтобы выяснить текущую версию прикладного программного обеспечения.

А.7. Класс FTP «Доверенный маршрут/канал»

А.7.1. Защита данных при передаче (FTP_DIT_EXT) Характеристика семейства

Семейство FTP_DIT_EXT «Защита данных при передаче» определяет компоненты требований, направленные на обеспечение защиты данных, в виде реализации функциональности для шифрования защищаемой информации, передаваемой между ОО и другими доверенными продуктами ИТ.

Ранжирование компонентов

FTP_DIT_EXT.1 «Защита данных при передаче» предназначен для задания требований, связанных с применением средств и процедур, с помощью которых ОО может шифровать защищаемую информацию при передаче.

Управление: FTP_DIT_EXT.1

Действия по управлению не определены.

Аудит: FTP_DIT_EXT.1

Действия или события, подвергаемые аудиту, не определены.

FTP_DIT_EXT.1 Защита данных при передаче.

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

FTP_DIT_EXT.1.1 ФБО должны [**выбор**:

не передавать любые данные;

не передавать любую защищаемую информацию;

шифровать всю передаваемую защищаемую информацию;

реализовать функциональность для шифрования защищаемой информации

] между ОО и другими доверенными продуктами

Приложение Б

Расширенные компоненты требований доверия к безопасности ОО

Для ОО определены следующие расширенные (специальные) компоненты требований доверия к безопасности: ADV_IMP_EXT.3 «Реализация ОО», ADV_TDS_EXT.3 «Разработка, уточнение и анализ архитектуры программного обеспечения ОО», AGD_OPE_EXT.1 «Правила кодирования», ALC_DEL_EXT.1 «Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок», ALC_DVS_EXT.1 «Моделирование угроз и разработка описания поверхности атаки», ALC_DVS_EXT.2 «Обеспечение безопасности сборочной среды программного обеспечения», ALC_DVS_EXT.3 «Управление доступом и контроль целостности кода при разработке программного обеспечения», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения», ALC_LCD_EXT.3 «Определенные разработчиком сроки поддержки», ALC_TAT_EXT.1 «Статический анализ исходного кода», ALC_TAT_EXT.2 «Динамический анализ кода программы», ATE_IND_EXT.1 «Нефункциональное тестирование», AVA_VAN_EXT.1 «Реагирование на информацию об уязвимостях», AVA_CCA_EXT.1 «Анализ скрытых каналов» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность», сформулированные в явном виде в стиле компонентов из национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

Б.1. Класс ADV «Разработка»

Б.1.1. Представление реализации (ADV_IMP)

ADV_IMP_EXT.3 Реализация ОО

Цели

Цель проверки выполнения требования ADV_IMP_EXT.3 заключается в обеспечении прослеживания реализации ОО к представлению реализации ФБО.

Иерархический для: нет подчиненных компонентов.

Зависимости: ADV_IMP.2 Полное отображение представления реализации ФБО.

Элементы действий разработчика

ADV_IMP_EXT.3.1D Разработчик должен предоставить реализацию ОО.

ADV_IMP_EXT.3.2D Разработчик должен обеспечить прослеживание реализации ОО к представлению реализации ФБО.

Элементы содержания и представления документированных материалов

ADV_IMP_EXT.3.1C В документации должны быть указаны состав и значения контрольных сумм элементов реализации ПО [выбор: *загрузочные модули ПО*, [назначение: *иные типы элементов реализации ПО*]].

ADV_IMP_EXT.3.2C В прослеживании между реализацией ОО и представлением реализации должно быть продемонстрировано [выбор:

а) для аппаратной платформы – соответствие между реализацией аппаратной платформы и ее представлением реализации [выбор: *схемы аппаратных средств, представления (кода) на языке описания аппаратных средств* [назначение: *иные формы представления реализации*]];

б) для ПО – соответствие между реализацией ПО [выбор: *загрузочные модули ПО*, [назначение: *иные типы элементов реализации ПО*]] *и их представлением реализации* [выбор: *исходные тексты ПО,* [назначение: *иные формы представления реализации*]]].

Элементы действий оценщика

ADV_IMP_EXT.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_IMP_EXT.3.1C и ADV_IMP_EXT.3.2C.

Б.1.2. Проект ОО (ADV_TDS)

ADV_TDS_EXT.3 Разработка, уточнение и анализ архитектуры программного обеспечения ОО

Цели

Создание условий для снижения количества возможных недостатков при разработке архитектуры ПО. Уточнение архитектуры ПО в процессе разработки кода.

Иерархический для: нет подчиненных компонентов.

Зависимости: ADV_TDS.3 Базовый модульный проект

Элементы действий разработчика

ADV_TDS_EXT.3.1D Разработчик должен определить требования безопасности к принципам проектирования архитектуры ПО, направленным на снижение количества возможных недостатков в разрабатываемом ПО.

ADV_TDS_EXT.3.2D Разработчик должен выполнить первичное проектирование архитектуры ПО.

ADV_TDS_EXT.3.3D Разработчик должен установить критерии необходимости уточнения архитектуры ПО.

ADV_TDS_EXT.3.4D Разработчик должен выполнять уточнение архитектуры ПО в процессе разработки кода и его изменений с установленной периодичностью или при наступлении определенных событий.

Элементы содержания и представления документированных материалов

ADV_TDS_EXT.3.1C Требования к принципам проектирования архитектуры ПО должны содержать информацию, позволяющую на начальном этапе проектирования ПО получить представление о принятых подходах и принципах проектирования архитектуры ПО (например, инкапсуляция, уникальность, разделение задач, применение заимствованных компонентов и т.п.), в том числе с точки зрения безопасности

(«нулевое доверие», «протоколирование событий», «резервное копирование», «формирование перечня недопустимых событий», «приоритетное использование языков с безопасной моделью памяти» и т.п.).

ADV_TDS_EXT.3.2C Описание архитектуры ПО должно включать, как минимум, следующую информацию:

- назначение ПО и сценарии его использования;
- описание среды функционирования;
- ограничения и указания по применению;
- проект ПО на уровне подсистем (модулей), включающий описание их назначения, структуры, особенностей реализации, применяемых языков программирования, взаимодействия друг с другом и другим ПО с указанием соответствующих интерфейсов, сетевых портов, протоколов.

ADV_TDS_EXT.3.3C Критерии необходимости уточнения архитектуры ПО должны содержать информацию о периодичности пересмотра (уточнения) архитектуры ПО в процессе разработки ПО или о событиях, при наступлении которых необходимо уточнять архитектуру ПО.

ADV_TDS_EXT.3.4C Архитектура ПО, уточненная по результатам выполнения требования ADV_TDS_EXT.3.4D, должна содержать информацию об особенностях реализации ПО в процессе разработки ПО,

принятых решениях по корректировкам архитектурных решений в процессе разработки, в том числе связанных с безопасностью, и причинах, их вызвавших.

Элементы действий оценщика

ADV_TDS_EXT.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_TDS_EXT.3.1C – ADV_TDS_EXT.3.4C.

Б.2. Класс AGD «Руководства»

Б.2.1. Руководство пользователя по эксплуатации (AGD_OPE)

AGD_OPE_EXT.1 Правила кодирования

Цели

Обеспечение эффективной и единообразной организации оформления и использования исходного кода в соответствии с предъявляемыми к ПО требованиями.

Зависимости: отсутствуют

Элементы действий разработчика

AGD_OPE_EXT.1.1D Разработчик должен принять и использовать в процессе разработки кода ПО регламент оформления исходного кода и безопасного кодирования для используемых разработчиком языков программирования.

Замечание по применению.

Под безопасным кодированием здесь и далее понимаются практики разработки ПО в соответствии с предъявляемыми в указанном выше регламенте требованиями по безопасности.

AGD_OPE_EXT.1.2D Разработчик должен учитывать при разработке регламента оформления исходного кода и безопасного кодирования примеры опасных и безопасных конструкций для используемых в ПО языков программирования.

AGD_OPE_EXT.1.3D Разработчик должен учитывать при разработке регламента оформления исходного кода и безопасного кодирования общепринятые стандарты и рекомендации разработчиков (экспертов, специалистов) для соответствующих языков программирования.

AGD_OPE_EXT.1.4D Разработчику рекомендуется при разработке ПО использовать программные средства автоматической проверки правил кодирования.

Элементы содержания и представления документированных материалов

AGD_OPE_EXT.1.1C Регламент оформления исходного кода и безопасного кодирования должен содержать информацию о способах оформления исходного кода.

AGD_OPE_EXT.1.2C Регламент оформления исходного кода и безопасного кодирования должен содержать перечень запрещенных способов кодирования, конструкций и т.п. (например, указание паролей в исходном коде ПО в явном виде, использование «магических чисел» и т.п.).

AGD_OPE_EXT.1.3C Регламент оформления исходного кода и безопасного кодирования должен содержать примеры опасных и безопасных конструкций для используемых языков программирования.

AGD_OPE_EXT.1.4C Регламент оформления исходного кода и безопасного кодирования должен содержать область применения правил кодирования.

AGD_OPE_EXT.1.5C Регламент оформления исходного кода и безопасного кодирования должен содержать порядок проверки выполнения правил кодирования для вносимых изменений в исходный код ПО.

AGD_OPE_EXT.1.6C Регламент оформления исходного кода и безопасного кодирования должен содержать рекомендации разработчиков языков программирования по использованию стандартов кодирования (языков программирования, в т.ч. собственной разработки), принятые разработчиком ПО.

Элементы действий оценщика

AGD_OPE_EXT.1.1E Оценщик должен подтвердить, что регламент, представленный заявителем, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в AGD_OPE_EXT.1.1C – AGD_OPE_EXT.1.16C.

Б.3. Класс ALC «Поддержка жизненного цикла»

Б.3.1. Процедуры обновления программного обеспечения (ALC_FPU_EXT)

Цели

Процедуры обновлений программного обеспечения должны быть разработаны, реализованы и подвергнуты контролю оценщиком в целях качественного проведения работ по устранению уязвимостей ОО, а также недопущения внесения уязвимостей в ОО при его обновлении.

ALC_FPU_EXT.1 Процедуры обновления программного обеспечения

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_FPU_EXT.1.1D Разработчик должен разработать и реализовать технологию обновления ОО для [**выбор**:

обновление, направленное на устранение уязвимостей ОО;

иное обновление, оказывающее влияние на безопасность ОО;

обновление, не оказывающее влияния на безопасность ОО

].

ALC_FPU_EXT.1.2D Разработчик должен разработать и поддерживать регламент обновления программного обеспечения.

ALC_FPU_EXT.1.3D Разработчик должен разработать и реализовать процедуру уведомления потребителей о выпуске обновлений ОО, основанную на [назначение: *способы уведомления*].

ALC_FPU_EXT.1.4D Разработчик должен разработать и реализовать процедуру предоставления обновлений потребителям ОО, основанную на [назначение: *способы предоставления обновлений*].

ALC_FPU_EXT.1.5D Разработчик должен разработать и реализовать процедуру представления обновлений оценщику для проведения внешнего контроля, основанную на [назначение: *способы предоставления обновлений для контроля*].

Элементы содержания и представления документированных материалов

ALC_FPU_EXT.1.1C Документация ОО должна содержать описание технологии выпуска обновлений ОО.

ALC_FPU_EXT.1.2C Документация ОО должна содержать регламент обновления ОО, включающий:

а) идентификацию типов выпускаемых обновлений;

б) описание процедуры уведомления потребителей о выпуске обновлений;

в) описание процедуры предоставления обновлений потребителям;

г) описание содержания эксплуатационной документации на выпускаемые обновления;

д) [назначение: *иная информация*].

ALC_FPU_EXT.1.3C Регламент обновления ОО должен предусматривать включение в эксплуатационную документацию на выпускаемые обновления описания следующих процедур:

а) процедуры получения обновления;

б) процедуры контроля целостности обновления;

в) типовой процедуры тестирования обновления;

г) процедуры установки и применения обновления;

д) процедуры контроля установки обновления;

е) процедуры верификации (проверки) применения обновления.

ALC_FPU_EXT.1.4C Документация процедуры представления обновлений для проведения внешнего контроля должна содержать:

а) описание процедуры предоставления обновлений для внешнего контроля;

б) требования к предоставлению и содержанию методики тестирования обновления разработчиком;

в) требования к оформлению и предоставлению результатов тестирования обновления разработчиком;

г) [**назначение**: *иная информация*].

Элементы действий оценщика

ALC_FPU_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в ALC_FPU_EXT.1.1C - ALC_FPU_EXT.1.4C.

ALC_FPU_EXT.1.2E Оценщик должен проверить, что процедура представления обновлений для проведения внешнего контроля позволяет организовать и проводить их внешний контроль.

Б.3.2. Определение жизненного цикла (ALC_LCD)

ALC_LCD_EXT.3 Определенные разработчиком сроки поддержки

Иерархический для: нет подчиненных компонентов. Зависимости: отсутствуют.

Элементы действий заявителя (разработчика, производителя)

ALC_LCD_EXT.3.1D Заявитель, разработчик, производитель должны установить в совместной декларации срок [назначение: *срок*], в течение которого они обязуются выполнять все необходимые действия по поддержке ОО, направленные на обеспечение поддержания сертификата соответствия ОО требованиям безопасности информации.

ALC_LCD_EXT.3.2D Заявитель, разработчик, производитель должны обеспечить представление совместной декларации о сроке поддержки ОО вместе с заявкой на сертификацию ОО.

Элементы содержания и представления документированных материалов

ALC_LCD_EXT.3.1C Декларация о сроке поддержки ОО должна содержать план поддержки ОО на весь задекларированный срок, включающий описание всех предпринимаемых действий по обеспечению поддержания сертификата соответствия ОО требованиям безопасности информации.

ALC_LCD_EXT.3.2C Декларация о сроке поддержки ОО должна содержать сведения о поддерживаемой версии ОО.

Элементы действий оценщика

ALC_LCD_EXT.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_LCD_EXT.3.1C и ALC_LCD_EXT.3.2C.

Б.3.3. Моделирование угроз и разработка описания поверхности атаки (ALC_DVS_EXT.1)

ALC_DVS_EXT.1 Моделирование угроз и разработка описания поверхности атаки

Цели

Создание условий для снижения количества недостатков, связанных с особенностями реализации архитектуры ПО и логики его функционирования, выработка мер по нейтрализации угроз безопасности, связанных с особенностями реализации архитектуры ПО.

Уточнение модели угроз и описания поверхности атаки по результатам разработки кода и его изменений.

Зависимости: ALC_DVS.1 Идентификация мер безопасности

Элементы действий разработчика

ALC_DVS_EXT.1.1D Разработчик должен выполнить первичное моделирование угроз для ПО (разработать модель угроз безопасности информации ОО); для выявленных угроз безопасности информации составить перечень мер по их нейтрализации (снижению вероятности возникновения).

ALC_DVS_EXT.1.2D Разработчик должен выполнить первичное описание поверхности атаки.

ALC_DVS_EXT.1.3D Разработчик должен сформировать перечень целей (функциональных подсистем, модулей (компонентов) ПО и их интерфейсов) для проведения дальнейших исследований безопасности ПО (например, фаззинг-тестирования) с учетом архитектуры ПО, результатов моделирования угроз и выполнения анализа поверхности атаки.

ALC_DVS_EXT.1.4D Разработчик должен выполнять уточнение модели угроз ПО для изменяемого в ходе разработки ПО кода с определенной периодичностью или при наступлении определенных событий.

ALC_DVS_EXT.1.5D Разработчик должен выполнять уточнение описания поверхности атаки для изменяемого в ходе разработки ПО кода с определенной периодичностью или при наступлении определенных событий.

ALC_DVS_EXT.1.6D Разработчик должен при уточнении описания поверхности атаки выполнять анализ поверхности атаки методом идентификации интерфейсов ПО.

Замечание по применению.

Используемые методы анализа сетевых интерфейсов способствуют получению информации об узлах сети, именах устройств, IP-адресах, операционных системах, запущенных программах и службах, именах пользователей, группах и открытых портах и могут включать анализ локальных и сетевых интерфейсов взаимодействия пользователя с ПО (модулями ПО, компонентами ПО) и взаимодействий модулей (компонентов) ПО между собой, средой функционирования и внешними объектами при их наличии.

ALC_DVS_EXT.1.7D Разработчик должен уточнять перечень целей (функциональных подсистем, модулей (компонентов) ПО и их интерфейсов) для проведения дальнейших исследований безопасности ПО (например, фаззинг-тестирования) с учетом уточненной архитектуры ПО, результатов моделирования угроз и выполнения анализа поверхности атаки для разработанного кода ПО.

Элементы содержания и представления документированных материалов

ALC_DVS_EXT.1.1C Модель угроз безопасности информации ОО должна включать совокупность угроз безопасности, актуальных для разрабатываемого ПО. Каждая угроза безопасности представляется в виде совокупности свойств (характеристик), включающей, как минимум, краткое описание угрозы, предполагаемый объект воздействия и возможные последствия реализации угрозы.

Замечание по применению.

При составлении перечня угроз безопасности и их описания рекомендуется учитывать положения ГОСТ Р 58412-2019, а также угрозы безопасности информации Банка данных угроз безопасности информации ФСТЭК России, других источников. В модели угроз рекомендуется указывать использованную при моделировании методологию, в том числе в случае ее собственной разработки.

ALC_DVS_EXT.1.2C Перечень мер по нейтрализации (снижению вероятности возникновения) угроз безопасности информации содержит перечень необходимых действий (доработок ПО, иных мер). Перечень мер по нейтрализации (снижению вероятности возникновения) угроз безопасности информации должен быть приоритизирован с точки зрения критичности возможного ущерба от реализации угроз безопасности информации.

ALC_DVS_EXT.1.3C Описание поверхности атаки должно включать совокупность потенциальных областей воздействия на информационную (автоматизированную) систему с использованием разрабатываемого ПО, которые могут быть использованы нарушителем для проведения компьютерной атаки. Описание поверхности атаки может быть частью модели угроз.

ALC_DVS_EXT.1.4C Перечень целей должен включать список функциональных подсистем, модулей (компонентов) ПО и их интерфейсов, составляющих поверхность атаки, подлежащих дополнительному анализу с точки зрения безопасности.

ALC_DVS_EXT.1.5C Модель угроз безопасности информации ОО должна дополнительно (в случае применимости) содержать угрозы безопасности ПО, актуальные для выполненных изменений.

ALC_DVS_EXT.1.6C Описание поверхности атаки должно включать перечень функциональных подсистем, модулей (компонентов) ПО и их интерфейсов, составляющих поверхность атаки, актуальных для разработанного кода ПО.

ALC_DVS_EXT.1.7C Перечень целей для проведения дальнейших исследований безопасности ПО должен содержать описание функциональных подсистем, модулей (компонентов) ПО, их интерфейсов, для которых предполагаются дальнейшие исследования в части безопасности при реализации других процессов РБПО.

Элементы действий оценщика

ALC_DVS_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS_EXT.1.1C - ALC_DVS_EXT.1.7C.

Б.3.4. Обеспечение безопасности сборочной среды программного обеспечения (ALC_DVS_EXT.2)

ALC_DVS_EXT.2 Обеспечение безопасности сборочной среды программного обеспечения

Цели

Обеспечение безопасности при сборке ПО, недопущение привнесения в результаты сборки ПО уязвимостей и ошибок со стороны сборочной среды.

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_DVS_EXT.2.1D Разработчик должен разработать регламент обеспечения безопасности сборочной среды.

ALC_DVS_EXT.2.2D Разработчик должен зафиксировать описание ожидаемых результатов сборки ПО, прав доступа к среде сборки ПО и хранилищу результатов сборки ПО и ролей пользователей, участвующих в процессе сборки ПО.

ALC_DVS_EXT.2.3D Разработчик должен разработать схему сборочной среды.

ALC_DVS_EXT.2.4D Разработчик должен обеспечивать регистрацию всех выполняемых действий при сборке ПО в журналах аудита; журналы аудита должны храниться способом, обеспечивающим их целостность; сроки хранения журналов аудита должны быть зафиксированы в регламенте обеспечения безопасности сборочной среды

ALC_DVS_EXT.2.5D Разработчик должен обеспечивать хранение результатов сборки ПО в выделенном хранилище – хранилище результатов сборки ПО.

ALC_DVS_EXT.2.6D Разработчик должен обеспечивать повторяемость сборки ПО (если применимо).

Замечание по применению

Под повторяемостью сборки имеется в виду обеспечение предсказуемости результатов сборок, обеспечение полного бинарного соответствия результатов повторных сборок не требуется.

ALC_DVS_EXT.2.7D Разработчик должен обеспечивать управление доступом к среде сборки ПО и хранилищу результатов сборки ПО на основе ролей пользователей.

ALC_DVS_EXT.2.8D Разработчик должен обеспечивать защиту каналов связи с внешними источниками данных для обеспечения конфиденциальности информации, обрабатываемой в сборочной среде.

Элементы содержания и представления документированных материалов

ALC_DVS_EXT.2.1C Регламент обеспечения безопасности сборочной среды должен содержать, как минимум, следующие сведения:

- обязанности сотрудников и их роли при проведении сборок ПО;
- порядок регистрации событий безопасности при реализации сборок ПО в журналах аудита;
- сроки хранения журналов аудита;
- описание мер безопасности, необходимых для реализации в сборочной среде.

ALC_DVS_EXT.2.2C Информация о безопасности сборочной среды должна содержать:

- описание ожидаемых результатов сборки ПО;
- описание прав доступа к сборочной среде и хранилищу результатов сборки ПО, а также ролей пользователей, участвующих в процессе сборки ПО.

ALC_DVS_EXT.2.3C Схематическое изображение сборочной среды должно содержать:

- элементы сборочной среды (серверы, узлы, виртуальные узлы, элементы среды контейнеризации и т.п.);
- связи между элементами сборочной среды, позволяющие отследить порядок (очередность) выполнения сборочных действий;
- компоненты сборочной среды, реализующие отдельные функции, в том числе меры безопасности (средства защиты информации, инструменты статического анализа и др.).

ALC_DVS_EXT.2.4C Журналы аудита процессов сборки ПО должны содержать следующую информацию:

- дату и время начала и завершения сборки ПО;
- информацию о версии собираемого ПО (модуля ПО, компонента ПО);
- информацию об используемой конфигурации сборки ПО;
- информацию о шагах сборки ПО;
- информацию о событиях безопасности в соответствии с регламентом обеспечения безопасности сборочной среды.

ALC_DVS_EXT.2.5C В качестве артефакта реализации требований, подтверждающих хранение результатов сборки ПО в выделенном хранилище, может использоваться журнал аудита сборки ПО, в котором указано место сохранения собранного модуля (компонента) ПО, результаты контрольного суммирования файлов, скачанных из хранилища результатов сборки ПО, и последующего сравнения их с контрольными суммами, указанными в журнале аудита сборки ПО или в графическом интерфейсе системы хранения результатов сборки ПО.

ALC_DVS_EXT.2.6C В качестве артефактов реализации требований, подтверждающих повторяемость сборки ПО, могут использоваться журналы аудита выполненных сборок, сравненные друг с другом; результаты контрольного суммирования файлов, полученных при разных запусках сборок, и последующего их

сравнения (по контрольным суммам, по бинарному представлению, по наименованию и размеру и др.).

Элементы действий оценщика

ALC_DVS_EXT.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS_EXT.2.1C - ALC_DVS_EXT.2.6C.

Б.3.5. Управление доступом и контроль целостности кода при разработке программного обеспечения (ALC_DVS_EXT.3)

ALC_DVS_EXT.3 Управление доступом и контроль целостности кода при разработке программного обеспечения

Цели

Обеспечение управления доступом к исходному коду и его целостности.

Элементы действий разработчика

ALC_DVS_EXT.3.1D Разработчик должен разработать регламент доступа к исходному коду ПО и обеспечения его целостности.

Замечание по применению

При разработке и реализации регламента доступа к исходному коду ПО рекомендуется руководствоваться принципами минимизации привилегий и разделения полномочий.

ALC_DVS_EXT.3.2D Разработчик должен осуществлять управление доступом к исходному коду ПО на основе выбранной модели управления доступом.

ALC_DVS_EXT.3.3D Разработчик должен осуществлять контроль целостности собственного исходного кода.

Элементы содержания и представления документированных материалов

ALC_DVS_EXT.3.1C Регламент доступа к исходному коду ПО и обеспечения его целостности должен содержать следующие сведения:

- обязанности сотрудников, их права и роли при разработке ПО;
- правила хранения исходного кода ПО, включая правила резервного копирования исходного кода ПО;
- правила внесения изменений (модификации, добавления, удаления) в исходный код ПО;
- критерии выбора способов и инструментов контроля целостности ПО;
- критерии выбора модулей (компонентов) ПО, подлежащих контролю целостности;
- описание процедуры контроля целостности исходного кода ПО.

ALC_DVS_EXT.3.2C Описание модели управления доступом к исходному коду ПО должно включать:

- перечень сотрудников, их права и обязанности при разработке ПО;

- описание выбранной модели управления доступом и используемых инструментов управления доступом.

ALC_DVS_EXT.3.3C Результаты выполнения контроля целостности собственного исходного кода должны обеспечивать соответствие требованиям регламента доступа к исходному коду ПО и обеспечения его целостности и позволять сделать однозначный вывод о целостности собственного исходного кода.

Элементы действий оценщика

ALC_DVS_EXT.3.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS_EXT.3.1C - ALC_DVS_EXT.3.3C.

Б.3.6. Статический анализ исходного кода (ALC_TAT_EXT.1)

ALC_TAT_EXT.1 Статический анализ исходного кода

Цели

Предотвращение внесения потенциально опасных конструкций и ошибок в ПО, а также использования опасных конструкций и уязвимостей из заимствованного кода.

Зависимости: ADV_TDS.3 Базовый модульный проект

Элементы действий разработчика

ALC_TAT_EXT.1.1D Разработчик должен разработать регламент проведения статического анализа исходного кода ПО.

ALC_TAT_EXT.1.2D Разработчик должен определить инструменты статического анализа для каждого используемого в ПО языка программирования.

ALC_TAT_EXT.1.3D Разработчик должен определить конфигурацию и параметры настройки инструментов статического анализа.

ALC_TAT_EXT.1.4D Разработчик должен проводить статический анализ с использованием инструментов статического анализа с регистрацией всех предупреждений о потенциальных ошибках, полученных по результатам работы инструментов статического анализа.

ALC_TAT_EXT.1.5D Разработчик должен осуществлять пересмотр конфигурации и параметров настройки инструментов статического анализа при выполнении установленных событий (изменениях в правилах сборки, применяемых статических анализаторах, получении информации об уязвимостях и т.п.).

ALC_TAT_EXT.1.6D Разработчик должен осуществлять повторный статический анализ ПО после устранения ранее выявленных ошибок и уязвимостей; внесения изменений в ходе разработки в исходные тексты ПО; изменения используемых версий компиляторов, сред выполнения (для компилируемого в промежуточное представление или интерпретируемого кода), обновлений используемых инструментов статического анализа.

Элементы содержания и представления документированных материалов

ALC_TAT_EXT.1.1C Регламент проведения статического анализа исходного кода ПО должен содержать следующие сведения:

- обязанности сотрудников и их роли при проведении статического анализа;
- критерии выбора инструментов статического анализа;
- критерии выбора ПО (модулей ПО, компонентов ПО, функциональных подсистем ПО), подлежащих проведению статического анализа;
- правила обработки срабатываний средств статического анализа;
- типы и критичность ошибок (уязвимостей), выявляемых статическим анализатором, подлежащих устранению, и приоритеты устранения ошибок (уязвимостей);
- периодичность проведения статического анализа или события, при наступлении которых необходимо выполнять повторный статический анализ;
- критерии пересмотра конфигурации и параметров настройки инструментов статического анализа.

ALC_TAT_EXT.1.2C Перечень инструментов статического анализа должен включать наименования инструментов статического анализа, их версии и информацию о соответствии используемым языкам программирования.

ALC_TAT_EXT.1.3C Конфигурации и параметры настройки инструментов статического анализа должны обеспечивать выполнение требований регламента проведения статического анализа в части выявления типов и критичности ошибок (уязвимостей), периодичности проведения статического анализа или событий, при наступлении которых необходимо выполнять повторный статический анализ.

ALC_TAT_EXT.1.4C Отчеты по результатам проведения статического анализа должны включать:

- срабатывания инструментов статического анализа;
- результаты анализа (разметки) выявленных ошибок (срабатываний статического анализатора).

ALC_TAT_EXT.1.5C Конфигурации и параметры настройки инструментов статического анализа должны обеспечивать выполнение требований регламента проведения статического анализа в части выполнения критериев их пересмотра.

Элементы действий оценщика

ALC_TAT_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_TAT_EXT.1.1C - ALC_TAT_EXT.1.5C.

Б.3.7. Динамический анализ кода программы (ALC_TAT_EXT.2)

ALC_TAT_EXT.2 Динамический анализ кода программы

Цели

Обнаружение недостатков и уязвимостей в коде ПО в процессе его выполнения.

Зависимости: ADV_TDS.3 Базовый модульный проект, ALC_DVS_EXT.1 Моделирование угроз и разработка описания поверхности атаки.

Элементы действий разработчика

ALC_TAT_EXT.2.1D Разработчик должен разработать регламент проведения динамического анализа кода ПО.

ALC_TAT_EXT.2.2D Разработчик должен определить инструменты динамического анализа и фаззинг-тестирования, порядок их применения.

ALC_TAT_EXT.2.3D Разработчик должен определить перечень модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование.

ALC_TAT_EXT.2.4D Разработчик должен определить сценарии проведения тестирования для каждого исследуемого модуля (компонента) ПО средствами динамического анализа, включая инструменты проведения фаззинг-тестирования.

ALC_TAT_EXT.2.5D Разработчик должен проводить динамический анализ с использованием инструментов динамического анализа.

ALC_TAT_EXT.2.6D Разработчик должен проводить повторный динамический анализ модулей (компонентов) ПО с целью контроля устранения ошибок.

ALC_TAT_EXT.2.7D Разработчик должен проводить фаззинг-тестирование.

ALC_TAT_EXT.2.8D При проведении фаззинг-тестирования использовать тестовые коллекции входных данных, подлежащие дальнейшим мутациям, для каждого из подвергаемых фаззинг-тестированию модуля (компонента) ПО (при использовании инструментов выполнения фаззинг-тестирования, использующих коллекции входных данных), вызывающие использование различных функциональных возможностей тестируемого модуля (компонента) ПО.

ALC_TAT_EXT.2.9D Разработчик должен устранять выявленные в процессе динамического анализа, включая фаззинг-тестирование, ошибки в соответствии с принятыми процедурами устранения найденных средствами динамического анализа ошибок

Элементы содержания и представления документированных материалов

ALC_TAT_EXT.2.1C Регламент проведения динамического анализа кода ПО должен содержать следующие сведения:

- обязанности сотрудников и их роли при проведении динамического анализа и фаззинг-тестирования;
- критерии выбора инструментов динамического анализа, включая инструменты проведения фаззинг-тестирования;
- критерии выбора методов и способов динамического анализа;

- критерии выбора модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование;
- правила обработки срабатываний средств динамического анализа, требующих обработки (аварийная остановка, зависание и т.п.);
- процедуры устранения найденных средствами динамического анализа ошибок;
- периодичность проведения динамического анализа или события, при наступлении которых необходимо выполнять повторный динамический анализ (критерии проведения повторного динамического анализа);
- периодичность проведения фаззинг-тестирования и критерии его завершения.

ALC_TAT_EXT.2.2C Перечень инструментов динамического анализа, включая инструменты проведения фаззинг-тестирования, должен включать:

- наименования инструментов динамического анализа, их версии и их соответствие исследуемым модулям (компонентам) ПО;
- параметры эксплуатации инструментов динамического анализа (для платформ, языков программирования и т.п.).

ALC_TAT_EXT.2.3C Перечень модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование, отвечающий требованиям регламента проведения динамического анализа, отвечающий требованиям регламента проведения динамического анализа, должен включать:

- наименование модуля (компонента) ПО;
- идентификатор модуля (компонента) ПО.

ALC_TAT_EXT.2.4C Сценарии проведения тестирования для каждого исследуемого модуля (компонента) ПО средствами динамического анализа, включая инструменты проведения фаззинг-тестирования, обеспечивающие выполнение требований регламента проведения динамического анализа, должен включать:

- идентификатор модуля (компонента) ПО;
- наименование используемого инструмента;
- параметры настройки инструмента;
- критерии запуска и остановки тестирования.

ALC_TAT_EXT.2.5C Отчеты по результатам проведения динамического анализа должны включать:

- срабатывания инструментов динамического анализа;

- результаты анализа (обработки) выявленных ошибок (срабатываний динамического анализатора) для определенных регламентом типов ошибок, требующих обработки (аварийная остановка, зависание и т.п.).

ALC_TAT_EXT.2.6C Отчеты по результатам проведения фаззинг-тестирования должны включать:

- сведения о результатах работы инструментов фаззинг-тестирования (длительность проведения фаззинг-тестирования, количество аварийных завершений работы ПО, количество найденных путей выполнения и др.);
- результаты анализа (обработки) аварийных завершений работы ПО, выявленных при проведении фаззинг-тестирования.

Элементы действий оценщика

ALC_TAT_EXT.2.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DVS_EXT.2.1C - ALC_DVS_EXT.2.6C.

Б.3.8. Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок (ALC_DEL_EXT.1)

ALC_DEL_EXT.1 Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок

Цели

Создание условий для снижения рисков внедрения вредоносного ПО посредством воздействий на ПО или механизмы его доставки до получения ПО конечными пользователями и недопущение компрометации данных (информации) или информационной системы, использующей такое ПО.

Зависимости: ADV_TDS.3 Базовый модульный проект, ALC_DVS_EXT.1 Моделирование угроз и разработка описания поверхности атаки, ACO_COR.1 Обоснование композиции.

Элементы действий разработчика

ALC_DEL_EXT.1.1D Разработчик должен осуществлять контроль зависящих от сторонних поставщиков элементов разработки (процессов; компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков; компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков).

ALC_DEL_EXT.1.2D Разработчик должен осуществлять контроль договорных обязательств со сторонними поставщиками.

ALC_DEL_EXT.1.3D Разработчик должен осуществлять выявление элементов инфраструктуры разработчика, воздействие на которые может повлиять на возникновение недекларированных возможностей в ПО.

ALC_DEL_EXT.1.4D Разработчик должен осуществлять контроль использования предсобранного поставщиком ПО (кода, для которого отсутствуют исходные тексты).

ALC_DEL_EXT.1.5D Разработчик должен осуществлять анализ кода ПО, полученного через цепочки поставок, на предмет внедрения вредоносного программного обеспечения.

Элементы содержания и представления документированных материалов

ALC_DEL_EXT.1.1C Перечень процессов, компонентов инфраструктуры, частей разрабатываемого ПО, зависящих от сторонних поставщиков, должен содержать следующие сведения:

- описание внутренних процессов, зависящих от сторонних поставщиков;
- описание компонентов инфраструктуры разработки ПО, зависящих от сторонних поставщиков;
- описание компонентов, являющихся частью разрабатываемого ПО, которые поставляются или заимствуются от сторонних поставщиков.

ALC_DEL_EXT.1.2C Сведения о договорных обязательствах со сторонними поставщиками могут включать следующую информацию:

- перечень поставщиков с указанием поставляемых продуктов (услуг);
- сведения о заключенных договорах со сторонними поставщиками, включающие информацию о поставляемых продуктах (услугах), сроках начала и окончания договоров, иную информацию.

ALC_DEL_EXT.1.3C Сведения о критичных и вероятных с точки зрения внедрения недекларированных возможностей элементах инфраструктуры (компонентах инфраструктуры разработки ПО, зависящих от сторонних поставщиков) должны содержать следующую информацию:

- перечень элементов инфраструктуры разработчика, воздействие на которые может повлиять на возникновение недекларированных возможностей в ПО;
- информацию о поставщиках продуктов (услуг) для указанных в перечне элементов инфраструктуры разработчика.

ALC_DEL_EXT.1.4C Результаты контроля использования предсобранного поставщиком ПО должны содержать информацию, позволяющую определить наличие предсобранных поставщиком ПО компонентов и осуществить их идентификацию (по свойствам файлов, контрольным суммам файлов и т.п.).

ALC_DEL_EXT.1.5C Результаты анализа кода ПО, полученного через цепочки поставок, на предмет внедрения вредоносного программного обеспечения должны содержать, как минимум, отчеты сканирования средств антивирусной защиты.

Элементы действий оценщика

ALC_DEL_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ALC_DEL_EXT.1.1C - ALC_DEL_EXT.1.5C.

Б.4. Класс AVA «Оценка уязвимостей»

Б.4.1. Анализ скрытых каналов (AVA_CCA_EXT)

Цели

Анализ скрытых каналов является частью анализа уязвимостей и проводится с целью сделать заключение о существовании и потенциальной пропускной способности каналов передачи сигналов (коммуникационных каналов), которые не предусмотрены для передачи защищаемой информации (данных пользователя и иной информации), или неразрешенных сигналов, которые могут быть для этого использованы потенциальными нарушителями (в нарушение установленных политик управления информационными потоками, управления доступом или иных установленных ограничений).

В качестве скрытых каналов рассматриваются:

- каналы передачи, которые предназначены для управления, но (в нарушение политики управления доступом или политики управления потоками) потенциально могут использоваться для передачи данных пользователя;
- каналы передачи, которые предназначены для передачи данных пользователя, но потенциально могут использоваться для передачи сигналов нарушителя (в том числе с использованием модуляции передачи данных);
- каналы передачи, которые (в нарушение установленных ограничений) потенциально могут использоваться для наблюдения одним пользователем за действиями другого пользователя;
- иные типы скрытых каналов.

AVA_CCA_EXT.1 Анализ скрытых каналов

Иерархический для: нет подчиненных компонентов.

Зависимости: AVA_VAN.4 Методический анализ уязвимостей;

ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации;

ADV_IMP.2 Полное отображение представления реализации функций безопасности ОО;

AGD_OPE.1 Руководство пользователя по эксплуатации;

AGD_PRE.1 Подготовительные процедуры;

[FDP_ACC.1 Ограниченное управление доступом

или

FDP_IFC.1 Ограниченное управление информационными потоками].

Элементы действий разработчика

AVA_CCA_EXT.1.1D Разработчик должен провести поиск скрытых каналов для реализуемых ОО [выбор:

политики управления информационными потоками;

политики управления доступом;

[назначение: иные политики]

].

AVA_CCA_EXT.1.2D Разработчик должен представить документацию по анализу скрытых каналов.

Элементы содержания и представления документированных материалов

AVA_CCA_EXT.1.1C В документации по анализу скрытых каналов должны быть идентифицированы скрытые каналы и должна содержаться оценка их пропускной способности.

AVA_CCA_EXT.1.2C Документация по анализу скрытых каналов должна содержать описание процедур, использованных для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

AVA_CCA_EXT.1.3C Документация по анализу скрытых каналов должна содержать описание всех предположений (быстродействие процессора, системная конфигурация, объем памяти и (или) иных), сделанных при анализе скрытых каналов.

AVA_CCA_EXT.1.4C Документация по анализу скрытых каналов должна содержать описание метода, использованного для оценки пропускной способности канала для наиболее опасного сценария.

AVA_CCA_EXT.1.5C Документация по анализу скрытых каналов должна содержать описание наиболее опасного сценария использования каждого идентифицированного скрытого канала.

Элементы действий оценщика

AVA_CCA_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и

представлению документированных материалов, изложенным в AVA_CCA_EXT.1.1C - AVA_CCA_EXT.1.5C.

AVA_CCA_EXT.1.2E Оценщик должен подтвердить, что результаты анализа скрытых каналов, выполненного заявителем, свидетельствуют об удовлетворении ОО соответствующих функциональных требований (по управлению информационными потоками, управлению доступом и (или) иных).

AVA_CCA_EXT.1.3E Оценщик должен подтвердить полноту, достаточность, непротиворечивость, повторяемость, достоверность и подлинность результатов анализа скрытых каналов, выполненного заявителем (разработчиком, производителем).

Б.4.2. Реагирование на информацию об уязвимостях (AVA_VAN_EXT)

Цели

Обеспечение выявления и устранения уязвимостей при эксплуатации ПО.

AVA_VAN_EXT.1 Реагирование на информацию об уязвимостях

Иерархический для: нет подчиненных компонентов.

Зависимости: AVA_VAN.5 Усиленный методический анализ.

Элементы действий разработчика

AVA_VAN_EXT.1.1D Разработчик должен разработать регламент реагирования на информацию об уязвимостях.

AVA_VAN_EXT.1.2D Разработчик должен осуществлять обработку поступающих запросов от пользователей (через службу технической поддержки, по иным каналам взаимодействия) с последующим анализом ошибок функционирования на предмет наличия уязвимостей (в случае получения таких запросов).

AVA_VAN_EXT.1.3D Разработчик должен, при обработке поступающих запросов и при последующем анализе, использовать средства автоматизации (например, систему управления изменениями, систему отслеживания ошибок, систему управления задачами и т.п.).

AVA_VAN_EXT.1.4D Разработчик должен осуществлять анализ информации о найденных уязвимостях в ПО на предмет подтверждения наличия/отсутствия уязвимостей и принимать решение о необходимости их устранения по результатам оценки.

AVA_VAN_EXT.1.5D Разработчик должен осуществлять оценку актуальности и критичности уязвимости с точки зрения безопасности ПО (в случае получения информации об уязвимости ПО из внешнего источника) и принимать решение о необходимости ее устранения по результатам оценки.

Элементы содержания и представления документированных материалов

AVA_VAN_EXT.1.1C Регламент реагирования на информацию об уязвимостях должен содержать:

- обязанности сотрудников и их роли при реагировании на информацию об уязвимостях ПО;
- правила реагирования на информацию об уязвимостях;
- правила оценки актуальности и критичности уязвимости с точки зрения безопасности ПО;
- периодичность проведения поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО.

AVA_VAN_EXT.1.2C Артефакты реализации требований, подтверждающие получение и обработку запросов от пользователей, должны содержать следующие сведения:

- информацию о запросах пользователей об ошибках (уязвимостях) ПО (дата, время запроса, идентификатор пользователя, статус запроса);
- результат анализа ошибок функционирования на предмет наличия уязвимостей.

AVA_VAN_EXT.1.3C Артефакты реализации требований, подтверждающие выполнение анализа информации о найденных уязвимостях в ПО, должны содержать следующие сведения:

- информацию о результатах тестирования ПО на предмет применимости информации об уязвимости ПО;
- проект (шаблон) ответа пользователям на запросы пользователей об ошибках (уязвимостях) ПО (о применимости информации о найденных уязвимостях);
- решение по результатам анализа информации о найденных уязвимостях в ПО.

AVA_VAN_EXT.1.4C Артефакты реализации требований, подтверждающие выполнение оценки актуальности и критичности уязвимости с точки зрения безопасности, должны содержать следующие сведения:

- информацию об оценке актуальности уязвимости;
- информацию об оценке уровня критичности уязвимости ПО;
- решение по результатам анализа актуальности и критичности уязвимости.

Элементы действий оценщика

AVA_VAN_EXT.1.1E Оценщик должен подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в AVA_VAN_EXT.1.1C - AVA_VAN_EXT.1.4C.

Б.5. Класс AMA «Поддержка доверия»

Б.5.1. Анализ влияния на безопасность (AMA_SIA)

Цели

Назначение семейства AMA_SIA состоит в том, чтобы убедиться в поддержке доверия к ОО посредством анализа, проводимого разработчиком, по определению влияния на безопасность всех изменений, воздействующих на ОО после его сертификации.

AMA_SIA_EXT.3 Анализ влияния обновлений на безопасность ПО

Иерархический для: нет подчиненных компонентов.

Зависимости: ALC_FPU_EXT.1 Процедуры обновления программного обеспечения ПО.

Элементы действий разработчика

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

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность ОО должны содержать краткое описание влияния обновлений на задание по безопасности, реализацию ОО функциональных возможностей или логическое обоснование отсутствия такого влияния, подтверждение устранения уязвимости (уязвимостей), на устранение которой (которых) направлен выпуск данных обновлений, и невнесения иных уязвимостей в ОО.

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

Элементы действий оценщика

AMA_SIA_EXT.3.1E Оценщик должен подтвердить, что информация, представленная в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в AMA_SIA_EXT.3.1C, AMA_SIA_EXT.3.2C.

AMA_SIA_EXT.3.2E Оценщик должен подтвердить влияние (отсутствие влияния) обновлений на безопасность ОО.

Б.6. Класс ATE «Тестирование»

Б.6.1. Независимое тестирование (ATE_IND)

ATE_IND.EXT.1 Нефункциональное тестирование

Цели

Подтверждение того, что поверхность атаки, модель угроз безопасности информации ОО и архитектура ПО содержат необходимую информацию.

Обнаружение недостатков программы путем выполнения нефункциональных тестов, в том числе имитирующих действия потенциального нарушителя.

Зависимости: ADV_FSP.4 Полная функциональная спецификация, ALC_DVS_EXT.1 Моделирование угроз и разработка описания поверхности атаки, AGD_PRE.1 Подготовительные процедуры

Элементы действий разработчика

ATE_IND.EXT.1.1D Разработчик должен проводить нефункциональное тестирование в отношении ПО (модулей ПО, компонентов ПО) в определенных объемах.

Замечание по применению

В настоящем разделе под нефункциональным тестированием понимаются проверки, не относящиеся к тестированию функциональных возможностей ПО. В рамках нефункционального тестирования могут выполняться следующие проверки:

- сетевых взаимодействий ПО;
- локальных интерфейсов взаимодействия ПО;
- производительности функционирования ПО;
- операций, выполняемых с высокими привилегиями;
- работы с конфиденциальными данными;
- корректности выполнения файловых операций;
- реализации защищенности бинарных файлов;
- реализации системы управления секретами;
- реализации безопасности сетевых протоколов;
- работы системы развертывания продукта;
- реализации мер по устранению или снижению критичности угроз, выявленных при моделировании угроз;
- возможности нарушения логики работы программы;
- безопасности реализации механизмов аутентификации и авторизации;
- безопасности обработки данных, полученных от потенциального нарушителя;

- безопасности реализации клиентской и серверной частей ПО.

ATE_IND.EXT.1.2D Разработчик должен разработать регламент нефункционального тестирования.

ATE_IND.EXT.1.3D Разработчик должен проводить нефункциональное тестирование с целью выявления локальных и сетевых интерфейсов взаимодействия с ПО (модулями ПО, компонентами ПО) пользователя и взаимодействий модулей (компонентов) ПО между собой, средой функционирования и внешними объектами.

ATE_IND.EXT.1.4D Разработчик должен осуществлять выполнение нефункциональных тестов, в том числе имитирующих действия потенциального нарушителя.

ATE_IND.EXT.1.5D Разработчик должен осуществлять корректировку описания поверхности атаки, модели угроз и архитектуры ПО по результатам выполнения нефункционального тестирования.

Элементы содержания и представления документированных материалов

ATE_IND.EXT.1.1C Регламент нефункционального тестирования должен содержать следующие сведения:

- критерии выбора версий ПО (модулей ПО, компонентов ПО), подлежащих нефункциональному тестированию, и определения периодичности тестирования;
- перечень используемых для нефункционального тестирования методов и средств;
- обязанности сотрудников и их роли при проведении нефункционального тестирования;

- описание типовых сценариев тестирования;
- описание возможностей и мотивации потенциального нарушителя, в соответствии с результатами моделирования угроз разрабатываемого ПО;
- описание типовых сценариев проведения компьютерных атак для основных сценариев работы ПО (модулей ПО, компонентов ПО).

ATE_IND.EXT.1.2C Отчет по результатам нефункционального тестирования должен содержать следующую информацию:

- краткое описание тестируемого ПО и его инфраструктуры развертывания;
- описание выполненных сценариев тестирования и последовательности их выполнения;
- набор целей (модулей ПО, компонентов ПО) тестирования;
- перечень выполненных действий и ограничений (описание отдельных аспектов, которые не проверялись);
- результаты нефункционального тестирования (снимки экрана (скриншоты), рабочие файлы инструментов нефункционального тестирования и т.п.);
- выводы, включающие следующую информацию: найденные недостатки (уязвимости) программ, средства и методы их выявления, результаты оценки опасности уязвимостей, описание возможных последствий эксплуатации уязвимостей, рекомендации по устранению найденных уязвимостей.

ATE_IND.EXT.1.3C Результаты сравнения архитектуры ПО, модели угроз и описания поверхности атаки с полученными фактическими результатами, перечень необходимых изменений в указанных артефактах реализации требований (при необходимости).

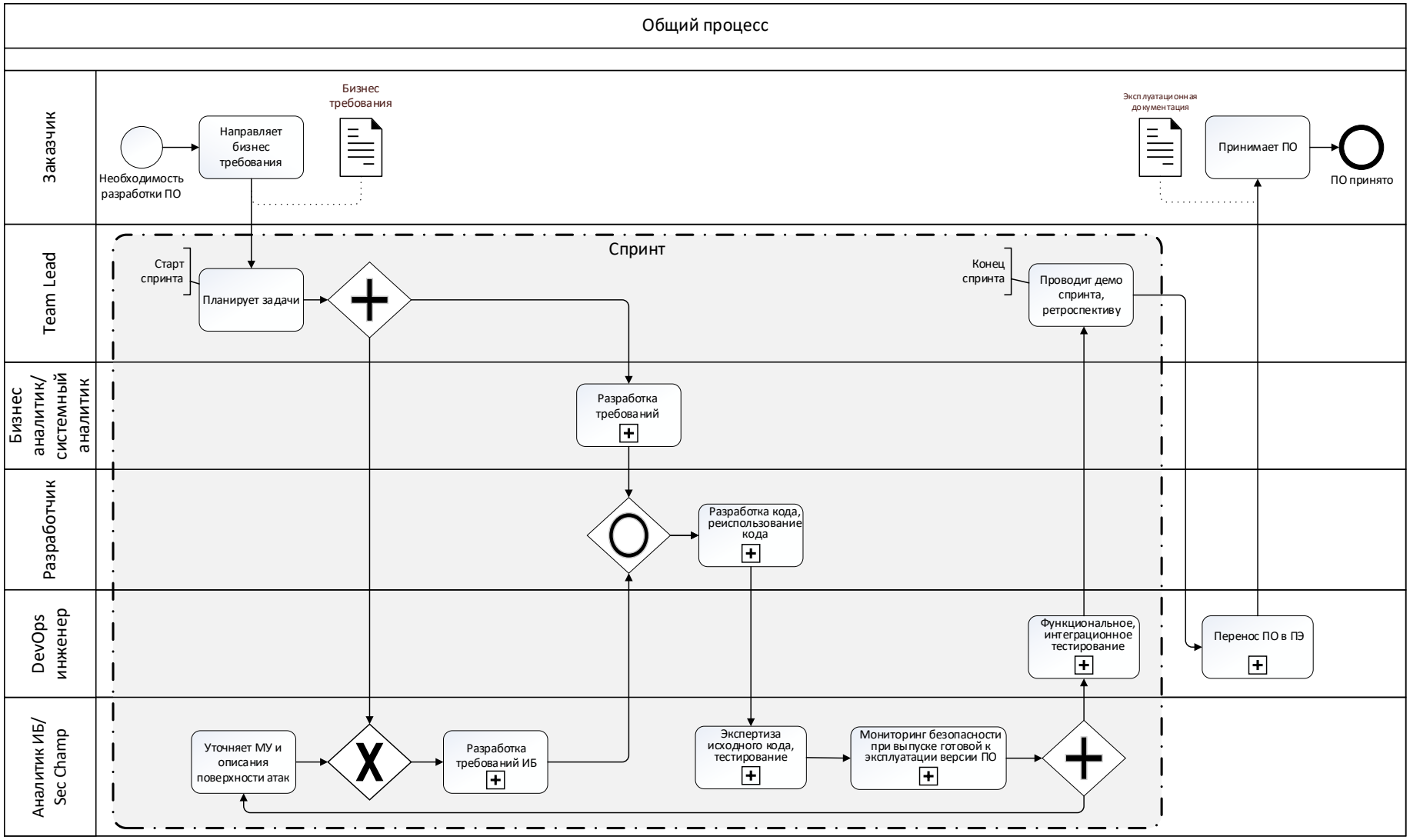
Элементы действий оценщика

ATE_IND.EXT.1.1E Оценщик должен подтвердить, что информация, представленная в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированных материалов, изложенным в ATE_IND.EXT.1.1C – ATE_IND.EXT.1.3C.

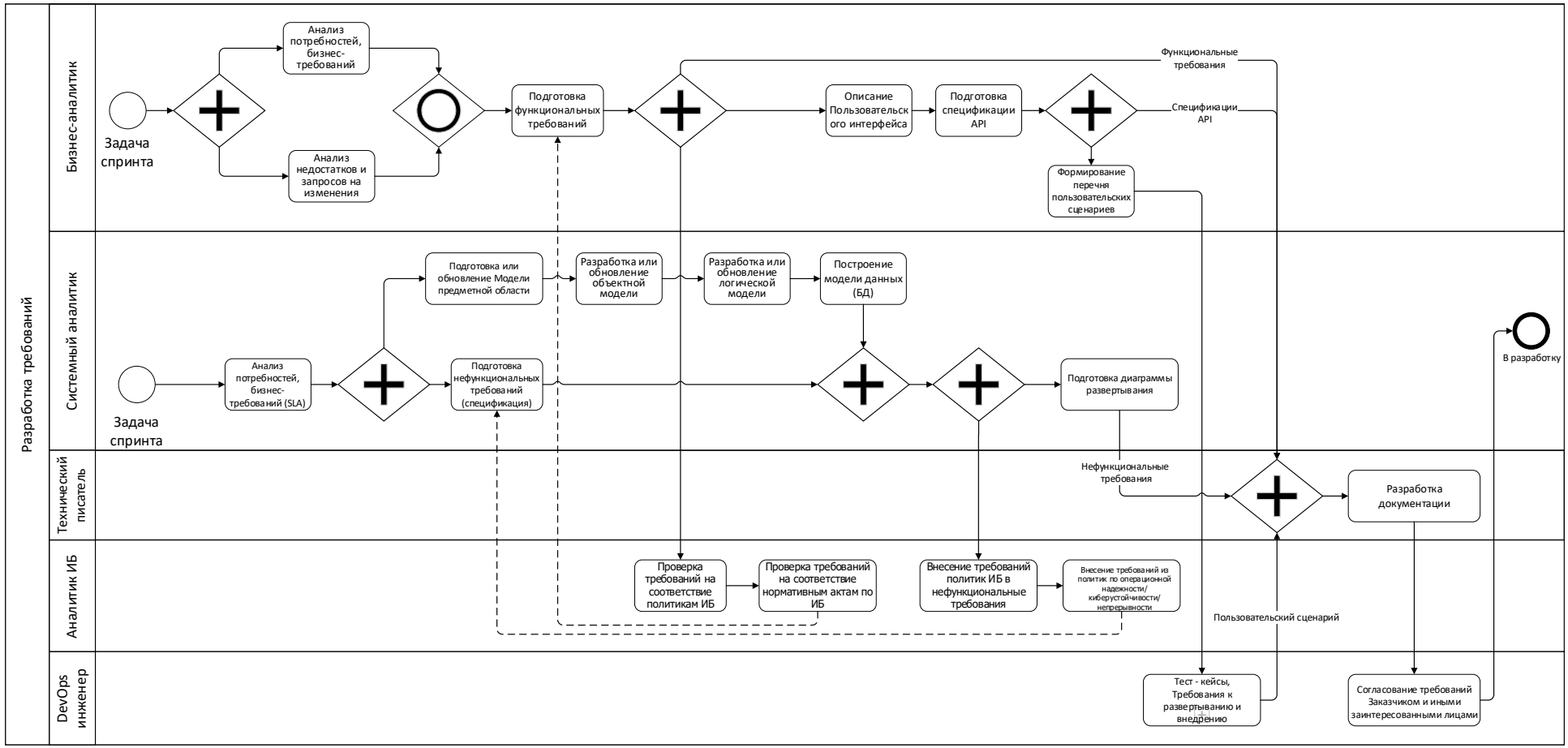
Приложение В

(справочное)

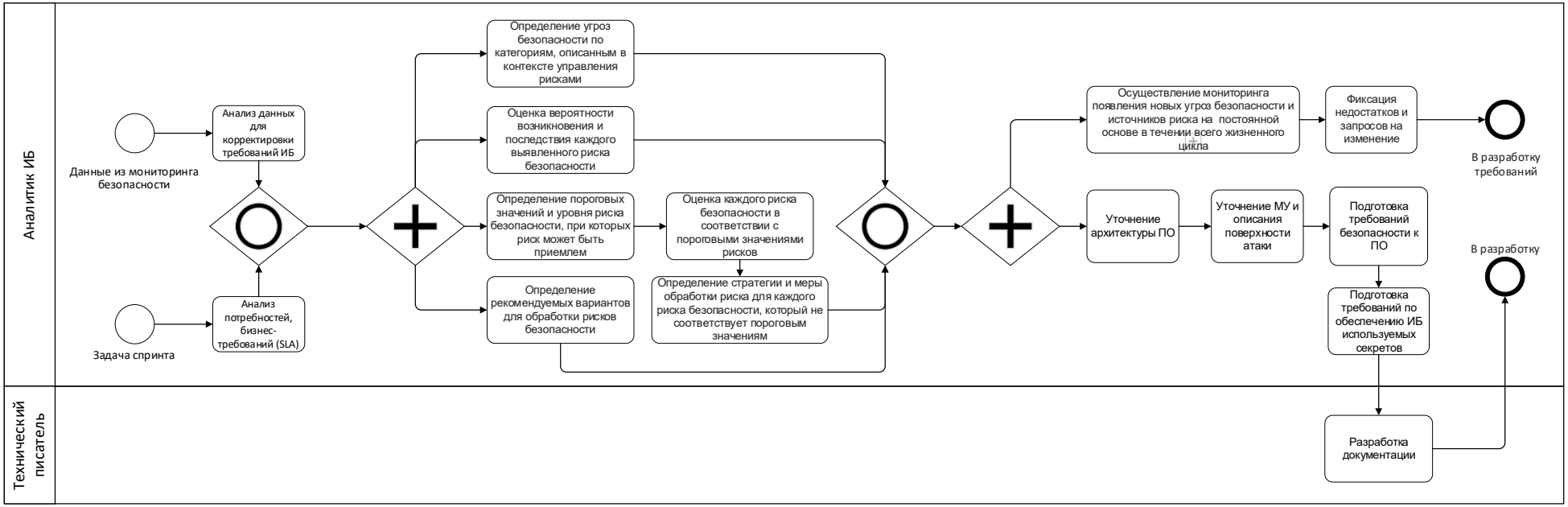
Ориентировочный процесс безопасного жизненного цикла ОО



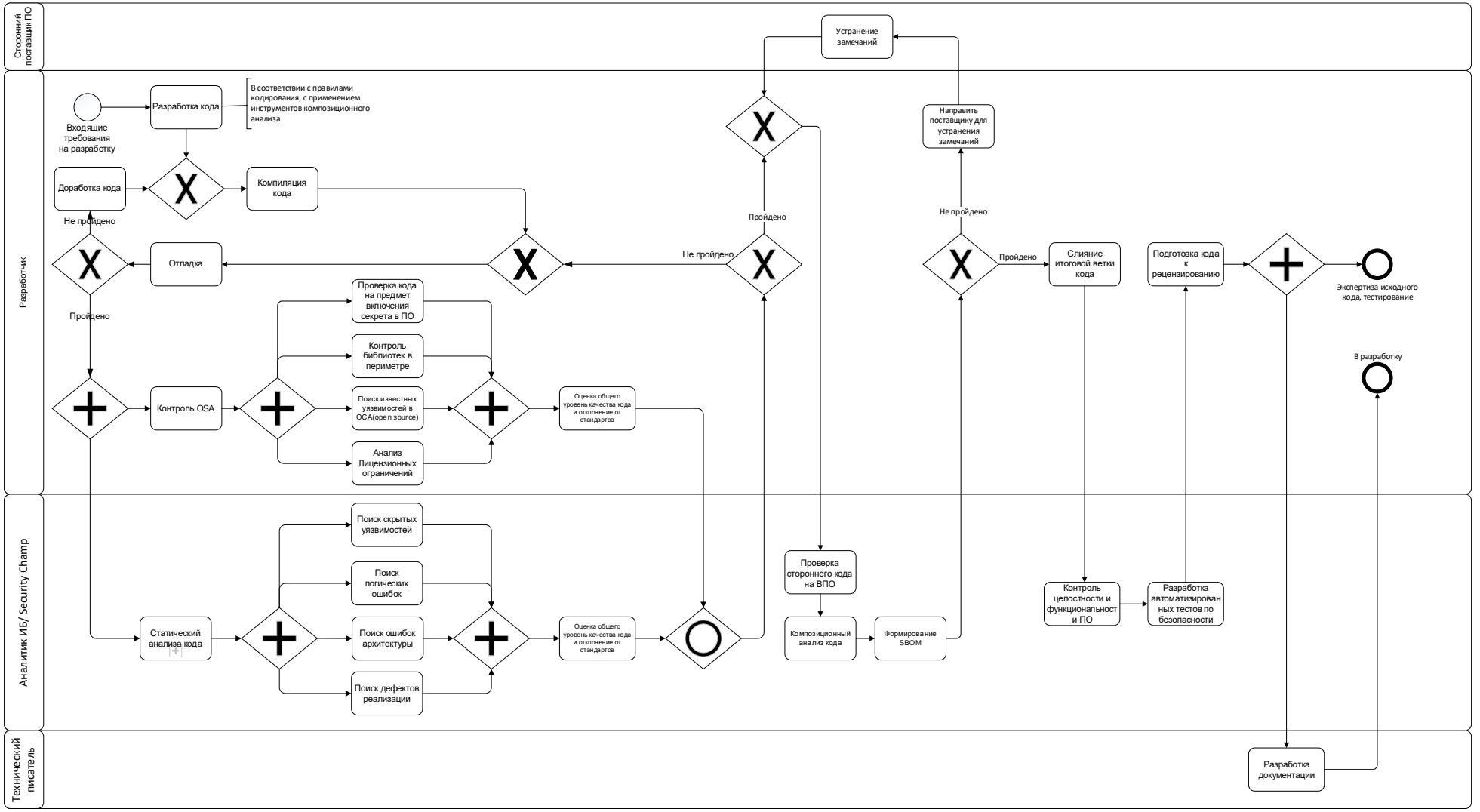
Разработка требований



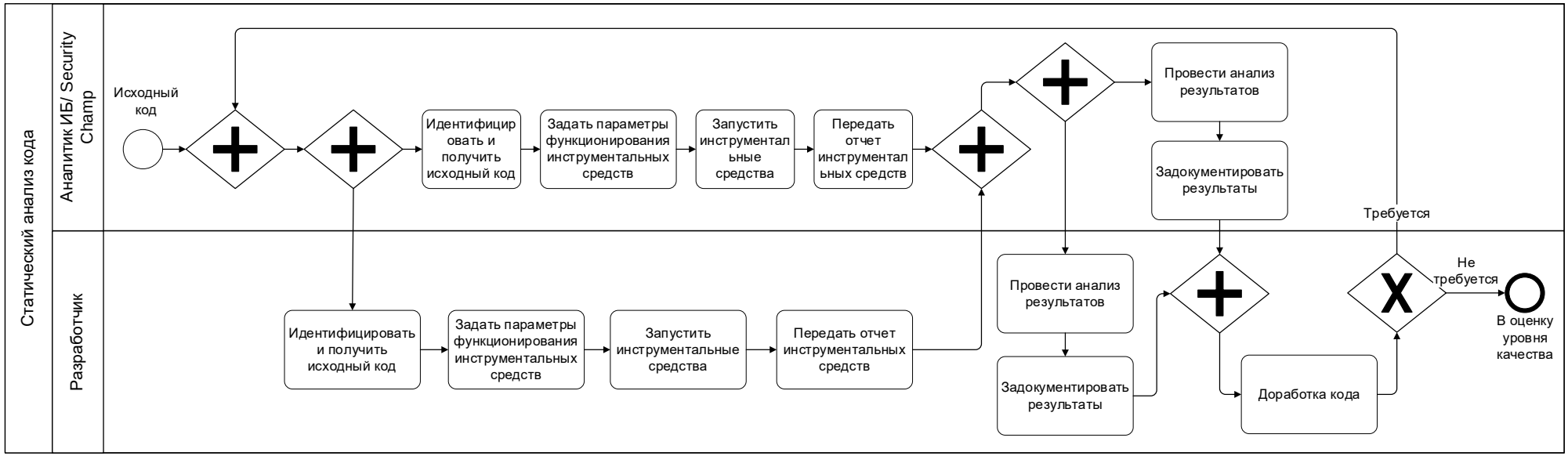
Разработка требований ИБ



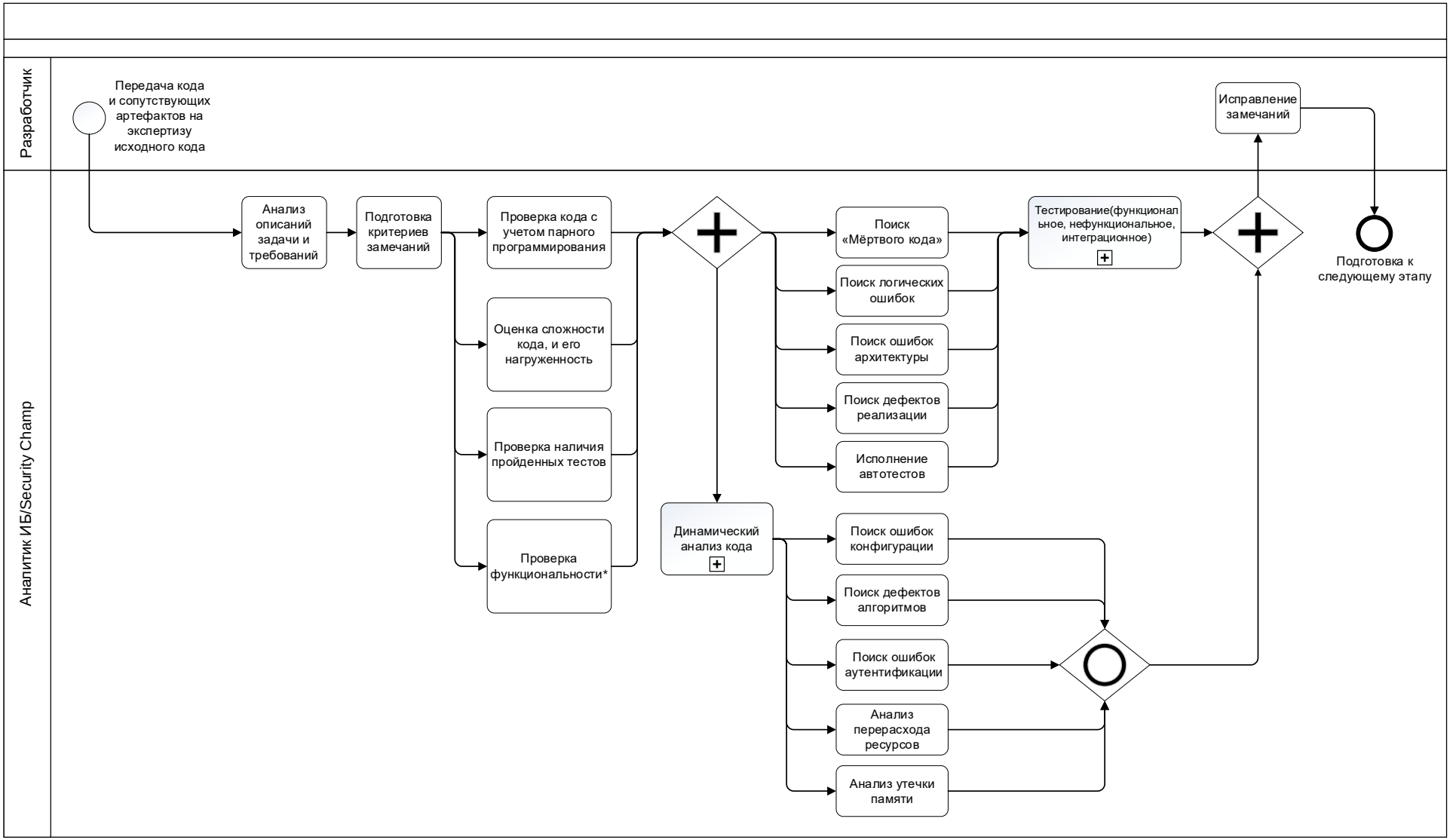
Разработка кода, реиспользование кода



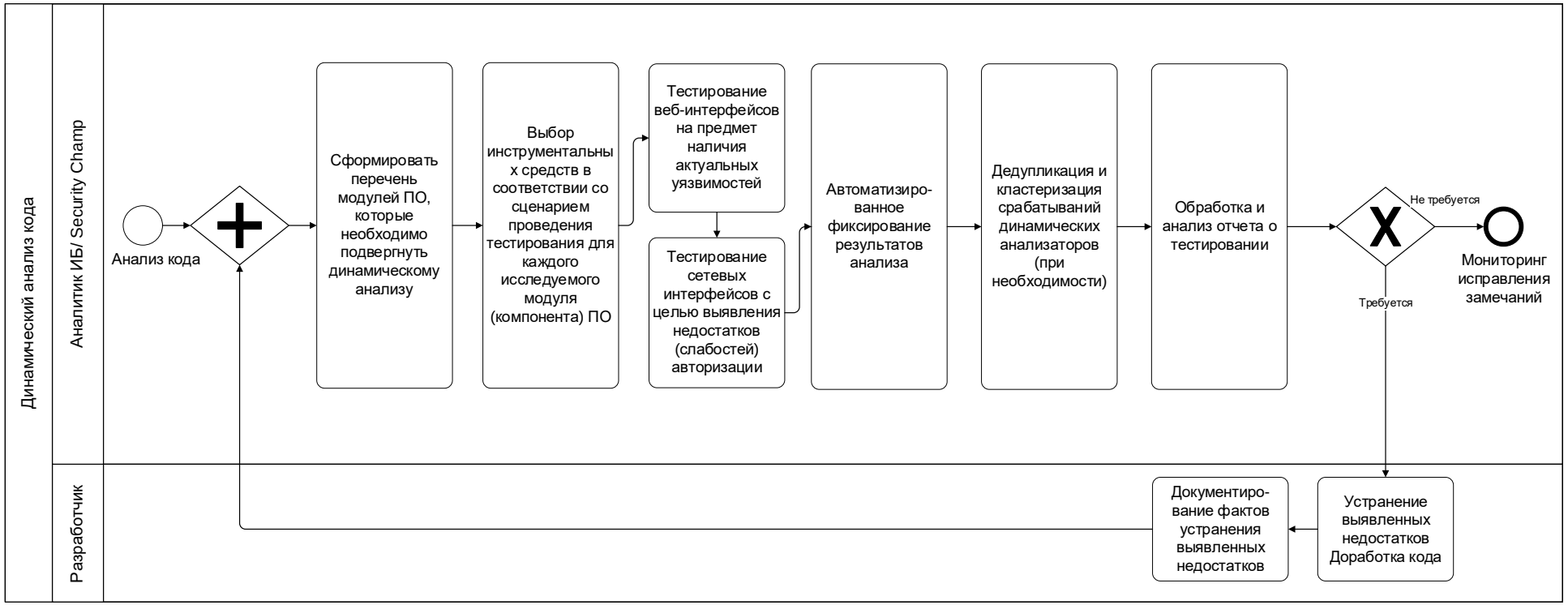
Статический анализ исходного кода



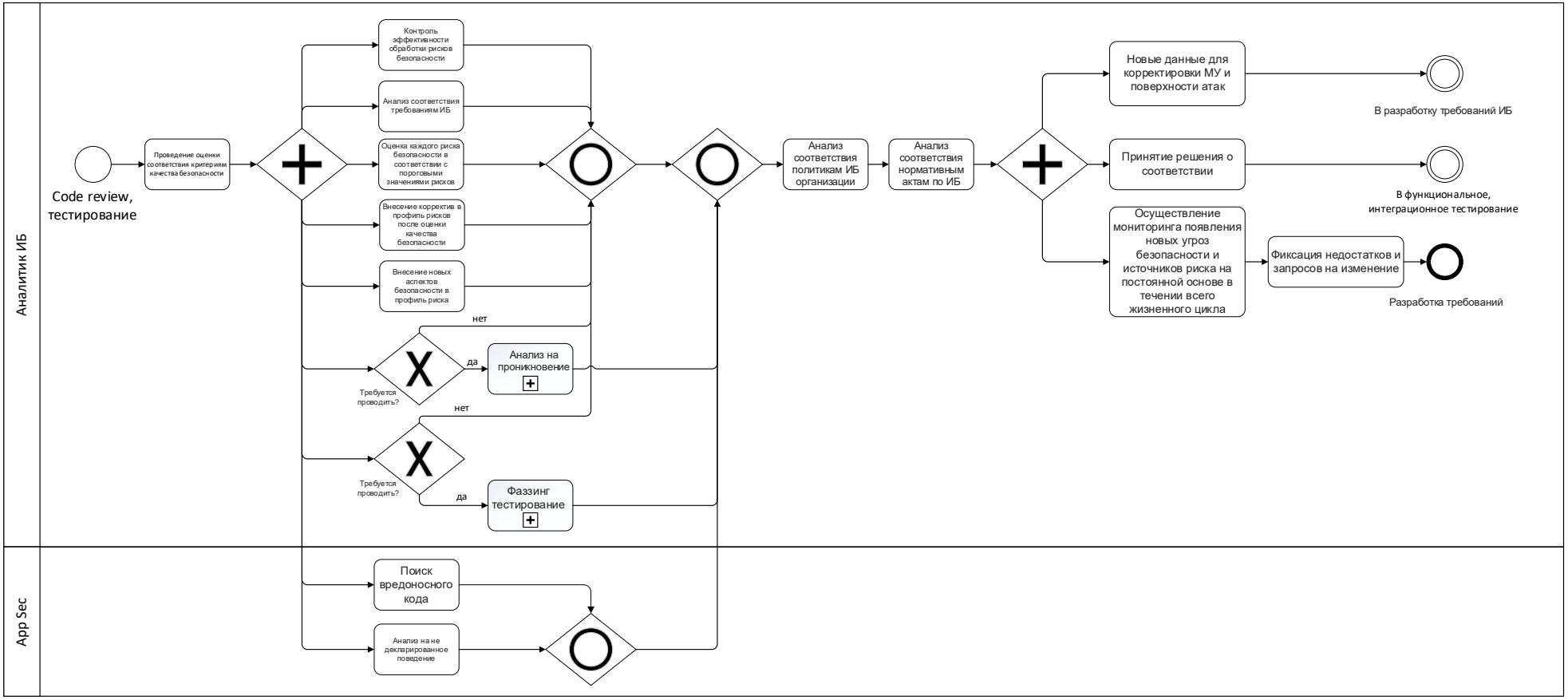
Процесс тестирования с проведением экспертизы исходного кода



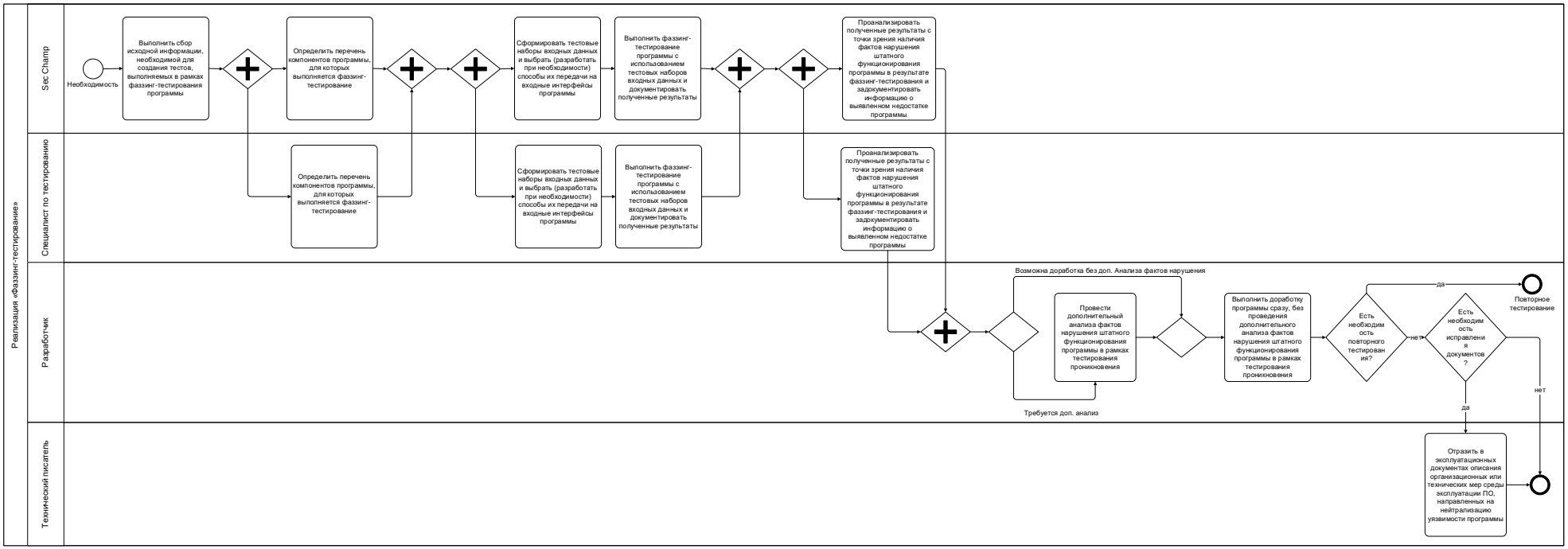
Динамический анализ кода



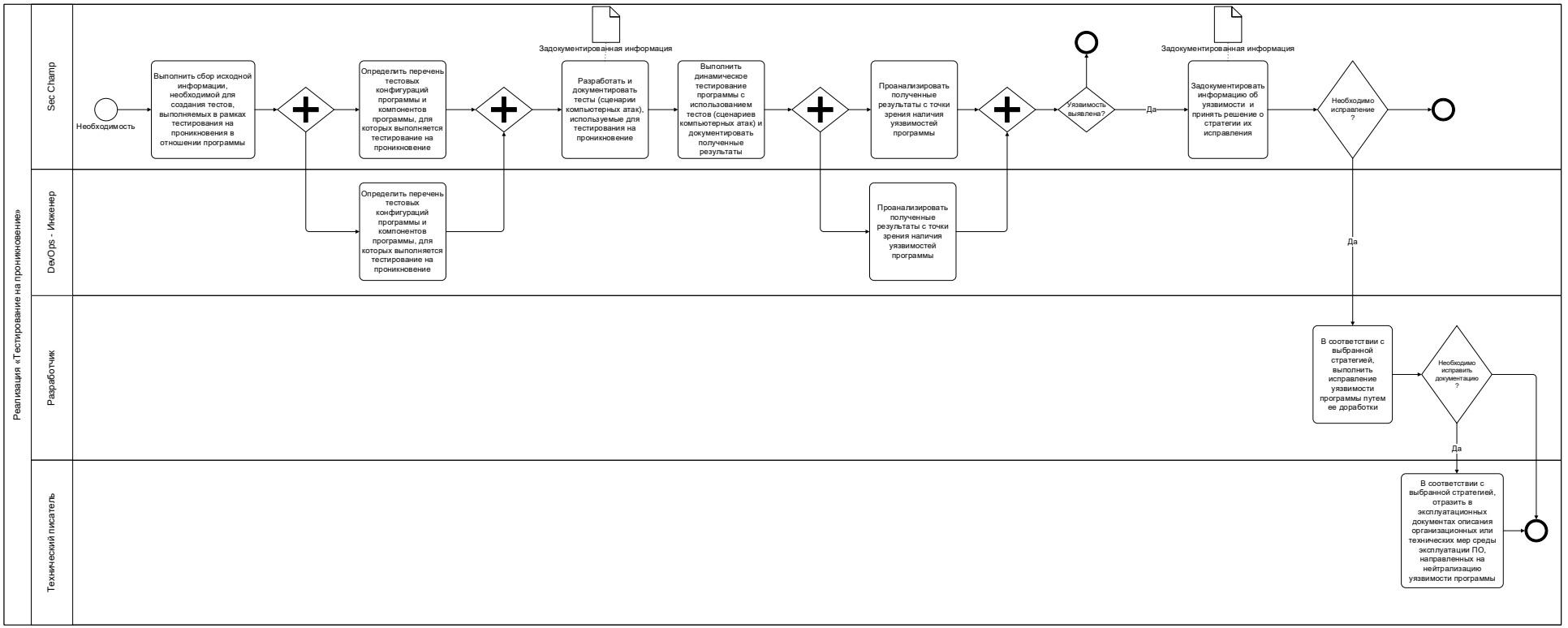
Мониторинг безопасности при выпуске готовой к эксплуатации версии ПО



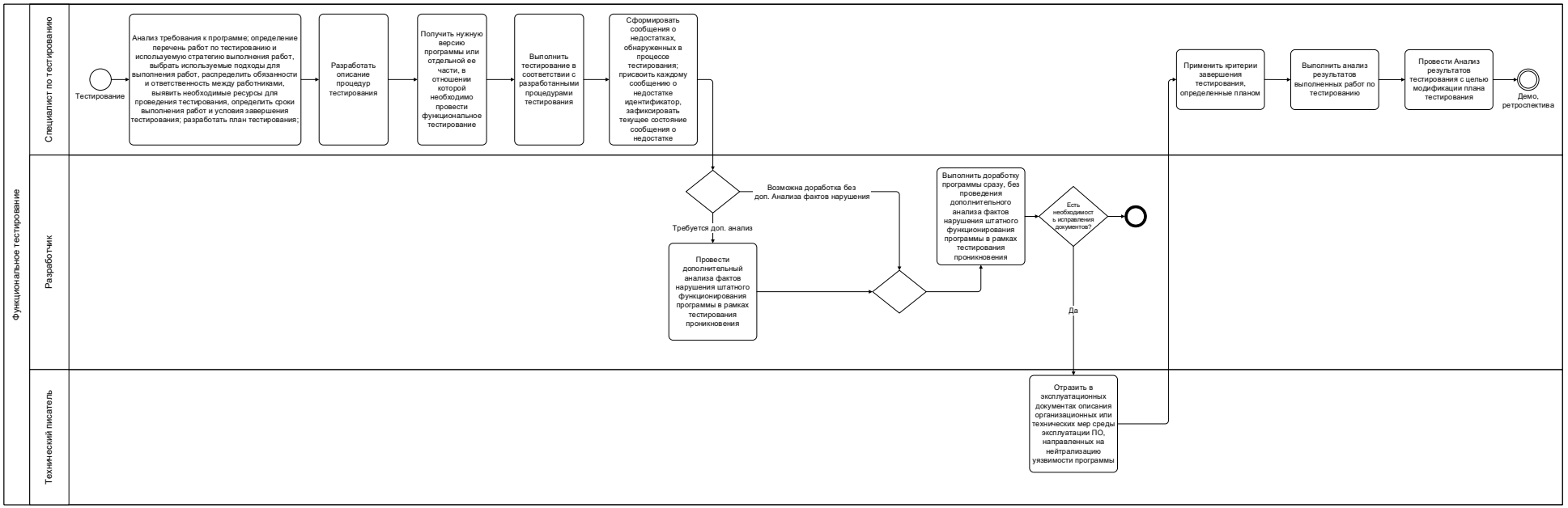
Фаззинг-тестирование



Тестирование на проникновение



Тестирование (функциональное, нефункциональное, интеграционное)



Перенос ПО в промышленную эксплуатацию