

ООО «ПингВин Софтвер»

УТВЕРЖДАЮ
Генеральный директор
ООО «ПингВин Софтвер»

_____ Д.В. Комиссаров
«15» декабря 2011 г.

УДК 004.03
Инв.№

ДОПОЛНЕНИЕ К ОТЧЕТУ О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

по теме:

**АНАЛИЗ И СРАВНИТЕЛЬНАЯ ОЦЕНКА РАЗЛИЧНЫХ
ВАРИАНТОВ СОЗДАНИЯ И ЭКСПЛУАТАЦИИ
НАЦИОНАЛЬНОЙ ПРОГРАММНОЙ ПЛАТФОРМЫ**

в части:

**АНАЛИЗА ТРЕБОВАНИЙ ОРГАНОВ ФСТЭК РОССИИ И ФСБ
РОССИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ К
СОЗДАВАЕМОЙ СИСТЕМЕ**

Руководитель проекта

В.В. Рубанов
«15» декабря 2011 г.

Ответственный исполнитель

А.А. Тагиев
«15» декабря 2011 г.

Нормоконтролер

А.В. Жмурко
«15» декабря 2011 г.

Москва
2011

1.1 Анализ требований органов ФСТЭК России и ФСБ России по информационной безопасности к создаваемой системе

1.1.1 Общие принципы защиты информации

В настоящее время Российская Федерация приняла направление в сторону усиления защиты своих интересов и интересов своих граждан, что обусловлено разработкой новых нормативно правовых актов и доработки уже введенных в действие ранее по защите информации и различных тайн, определенных федеральными законами.

Кроме этого проведена большая работа по доработке КоАП РФ и УК РФ в части усиления ответственности и расширения зоны контроля в этой области.

Общей целью данных работ является обеспечение конфиденциальности, целостности доступности информации (CIA triade,), а методами — контроль доступа на основе ролей (RBAC, Role-Based Access Control), принцип минимальных привилегий (доступ только к той информации, которая действительно нужна для работы) и комплексный подход к обеспечению ИБ (комплекс организационных и технических мероприятий, направленных на снижение уровня всех выявленных внешних и внутренних угроз).

В большинстве современных международных и национальных стандартов (ISO 27000, NIST 800-30) обеспечение ИБ рассматривается как одна из задач управления рисками для бизнеса. На основе анализа (и классификации) информационных активов и архитектуры АС и построения частной модели угроз/нарушителя можно оценить риски ИБ (цена потери, умноженная на вероятность реализации угрозы), причем «в рублях» и исходя из этого выбирать те или иные средства защиты. Выбор должен быть обоснован экономически. (В более ранних стандартах делалась попытка описания набора одинаковых для всех АС (вне зависимости от сферы применения и масштаба) «лучших практик», что зачастую приводило к выбору избыточных и, как следствие, неоправданно дорогих средств защиты.)

Если говорить о законодательных основах обеспечения ИБ, то следует отметить следующие четыре момента:

1. Законодательная база в области ИБ опирается на Конституцию РФ и включает в себя ряд федеральных законов (Законы «О безопасности», «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», номера и даты принятия можно посмотреть на сайте ФСТЭК http://fstec.ru/_razd/_isp0o.htm), Указов и распоряжений Президента РФ, Постановлений Правительства РФ, документов концептуального характера («Стратегия национальной безопасности Российской Федерации до 2020 года» и «Доктрина информационной безопасности Российской Федерации», см. там же), и целого ряда распорядительных документов в области технической защиты информации (Положений, установленных Постановлениями Правительства РФ, руководящими и методическими документами уполномоченных органов (ФСТЭК, ФСБ, и других). Кроме того принят целый ряд государственных и отраслевых стандартов в этой области.

2. Государство осуществляет функции регулирования в области обеспечения ИБ путем лицензирования деятельности в области ИБ

(на основании закона «О лицензировании отдельных видов деятельности ») и организации системы сертификации технических и программных средств и аттестации автоматизированных систем (на основании закона «О техническом регулировании»).

3. Федеральными органами исполнительной власти, ответственными за осуществление регулирования в области ИБ, являются:

- Федеральная служба по техническому и экспортному контролю (ФСТЭК) – в части обеспечения защиты информации некриптографическими методами,

- Федеральная служба безопасности Российской Федерации (ФСБ) - в части обеспечения защиты информации криптографическими методами.

Уполномоченным органом по контролю за соблюдением требований 152 ФЗ «О

персональных данных» является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

4. В УК, ГК, ТК и КоАП имеется ряд статей, определяющих ответственность физических и юридических лиц за несоблюдение требований законодательства РФ в области защиты информации при обработке ее как с использованием АС, так и без оного.

1.1.2 Нормативная база в области сертификации безопасности автоматизированных систем

Нормативную базу в области сертификации безопасности автоматизированных систем в нашей стране составляют государственные стандарты, руководящие документы ФСТЭК России, Минобороны России и ФСБ России.

Как уже было отмечено в разделе 2.6.1, правовой базой работ по сертификации информационных технологий являются законы РФ «О техническом регулировании», «О сертификации продукции и услуг», «О стандартизации», «Об информатизации и защите информации», «О государственной тайне», «О защите прав потребителей», указы Президента Российской Федерации, постановления Правительства Российской Федерации, а также ряд других подзаконных актов. Национальным органом по сертификации определен Госстандарт Российской Федерации. Процедура сертификации по требованиям безопасности автоматизированных систем, входящая в состав более общей процедуры сертификации качества функционирования АС, должна опираться на государственные стандарты, определяющие систему функциональных показателей, оцениваемых при сертификации, регламентирующие управление проектированием и документирование программного обеспечения. Поскольку комплексы отечественных стандартов, регламентирующих документирование АС на различных стадиях ее создания, представляют во многом морально устаревшие стандарты серий «Информационная технология», «Единая система стандартов

автоматизированной системы управления» и «Единая система программной документации», не имеет смысла приводить их полный перечень.

Указом Президента Российской Федерации от 30.03.94 г. № 614 функции Межведомственной комиссии по защите государственной тайны были временно возложены на Гостехкомиссию при Президенте РФ. В целом же на ФСТЭК России возложены обязанности по координации, организационно-методическому руководству, лицензированию деятельности предприятий и сертификации продукции в области защиты информации, техническому и экспортному контролю. В соответствии с Постановлением Правительства Российской Федерации от 26.06.95 г. № 608 «О сертификации средств защиты информации» созданы системы сертификации Гостехкомиссии России, Минобороны России, разработаны и введены в действие перечни средств защиты информации, подлежащих обязательной сертификации в этих системах. Центральным органом системы сертификации средств криптографической защиты информации является ФСБ России.

В нашей стране методологической базой нормативно-технических и методических документов, посвященных вопросам сертификации безопасности СВТ и АС, является РД Гостехкомиссии «Концепция защиты СВТ и АС от НСД к информации», а также «Защита от НСД к информации. Термины и определения». Эти документы содержат:

- основные термины и определения в области защиты информации;
- определение понятия НСД;
- основные принципы защиты от НСД;
- модель нарушителя в АС;
- основные способы НСД;
- основные направления обеспечения защиты от НСД;
- основные характеристики технических средств защиты от НСД;
- классификация АС;
- организация работ по защите от НСД.

Другим основополагающим РД в области сертификации СЗИ является «Положение о сертификации средств защиты информации по требованиям безопасности информации», устанавливающее организационную структуру системы сертификации, порядок проведения сертификации СЗИ и контроля и основные требования к нормативным и методическим документам по сертификации СЗИ.

Организационную структуру системы сертификации образуют:

- ФСТЭК России (федеральный орган по сертификации средств защиты информации);
- центральный орган системы сертификации средств защиты информации;
- органы по сертификации средств защиты информации;
- испытательные центры (лаборатории);
- заявители (разработчики, изготовители, поставщики, потребители средств защиты информации).

Порядок проведения сертификации включает следующие действия:

- подачу и рассмотрение заявки на сертификацию средств защиты информации;
- испытания сертифицируемых средств защиты информации и аттестация их производства;
- экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия;
- осуществление государственного контроля и надзора, инспекционного контроля соблюдения правил обязательной сертификации и сертифицированных средств защиты информации;
- информирование о результатах сертификации средств защиты информации;
- рассмотрение апелляций.

Критерии оценки безопасности АС и СВТ выражены в РД Гостехкомиссии РФ: «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» и «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ» регламентирует следующие основные вопросы:

- организационную структуру и порядок проведения работ по защите информации от НСД и взаимодействия при этом на государственном уровне;
- систему государственных нормативных актов, стандартов, руководящих документов и требований по этой проблеме;
- порядок разработки и приемки защищенных СВТ, в том числе программных и технических (в частности, криптографических) средств и систем защиты информации от НСД;
- порядок приемки указанных средств и систем перед сдачей в эксплуатацию в составе АС, порядок их эксплуатации и контроля работоспособности этих средств и систем в процессе эксплуатации.

Согласно настоящему временному положению, при разработке средств и систем защиты в АС и СВТ необходимо руководствоваться требованиями следующих руководящих документов:

- концепция защиты СВТ и АС от НСД к информации;
- временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ;
- термины и определения по защите от НСД к информации;
- показатели защищенности СВТ от НСД к информации;
- классификация АС и требования по защите информации от НСД в АС различных классов.

1.1.3 Порядок создания АС ЗИ в Российской Федерации

В соответствии с руководящими документами по защите информации и Российским законодательством в области безопасности информации определена следующая последовательность создания автоматизированных систем (АС).

В ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» описан общий порядок создания АС в защищенном исполнении (ЗИ), а именно: разработка и внедрение вновь создаваемой АС производится в соответствии с ТЗ на АС, которое является основным документом, определяющим требования, предъявляемые к АС, порядок создания АС и приемку АС при вводе в действие. Для вновь создаваемых АС ТЗ разрабатывают на систему в целом, предназначенную для работы самостоятельно или в составе другой системы. Дополнительно могут быть разработаны ЧТЗ на части и подсистемы АС. Поэтому требования по ЗИ при создании АС ЗИ должны включаться разделом в общее ТЗ на АС или могут быть изложены в виде частного ЧТЗ или дополнения к основному ТЗ на АС.

Организации-участники работ по созданию АС ЗИ должны иметь лицензии на право проведения работ в области защиты информации. Лицензирование организаций и предприятий осуществляется в установленном порядке. Работы по созданию, производству и эксплуатации АС ЗИ с использованием ШС для защиты сведений, отнесенных к тайне, организуются в соответствии с положениями нормативных актов Российской Федерации, определяющих порядок разработки, изготовления и обеспечения эксплуатации ШС, систем и комплексов.

Для создания АС ЗИ могут применяться как серийно выпускаемые, так и вновь разработанные технические средства и программные средства обработки информации, а также технические, программные, программно-технические, шифровальные СрЗИ и средства для контроля эффективности. Выпускаемые средства должны иметь сертификаты соответствия, полученные в соответствующих системах сертификации по требованиям безопасности информации. Вновь

разработанные средства должны быть сертифицированы в установленном порядке до начала опытной эксплуатации АС ЗИ.

Сертификация средств, комплексов и систем ЗИ осуществляется в соответствии с требованиями «Положения о сертификации средств защиты информации. Постановление Правительства Российской Федерации от 26.05.95 г. № 608».

В рамках проводимой НИР письмом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 14 октября 2011 года № 240/2/3908 в адрес головного исполнителя ООО «ПингВин Софтвер» было рекомендовано формировать требования по безопасности информации к компонентам программной платформы в виде профилей защиты в соответствии с национальным стандартом ГОСТ Р ИСО/МЭК 15408 «Информационная технология — Методы и средства обеспечения безопасности — Критерии оценки безопасности информационных технологий» и руководящим документом «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002), а также с учетом требований руководящего документа «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999).

В ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» определены следующие требования защита информации в АС ЗИ должна быть:

- целенаправленной, осуществляемой в интересах реализации конкретной цели защиты информации в АС ЗИ;
- комплексной, осуществляемой в интересах защиты всего многообразия структурных элементов АС ЗИ от всего спектра опасных для АС ЗИ угроз;
- управляемой, осуществляемой на всех стадиях жизненного цикла АС ЗИ, в зависимости от важности обрабатываемой информации, состояния ресурсов АС ЗИ, условий эксплуатации АС ЗИ, результатов отслеживания угроз безопасности информации;

– гарантированной; методы и средства защиты информации должны обеспечивать требуемый уровень защиты информации от ее утечки по техническим каналам, несанкционированного доступа к информации, несанкционированным и непреднамеренным воздействиям на нее, независимо от форм ее представления.

В АС ЗИ должна быть реализована система защиты информации, выполняющая следующие функции:

- предупреждение о появлении угроз безопасности информации;
- обнаружение, нейтрализацию и локализацию воздействия угроз безопасности информации;
- управление доступом к защищаемой информации;
- восстановление системы защиты информации и защищаемой информации после воздействия угроз;
- регистрацию событий и попыток несанкционированного доступа к защищаемой информации и несанкционированного воздействия на нее;
- обеспечение контроля функционирования средств и системы защиты информации и немедленное реагирование на их выход из строя.

Необходимый состав функций, которые должны быть реализованы в АС, устанавливают в соответствии со Специальными требованиями и рекомендациями по защите информации, составляющей государственную тайну, от утечки по техническим каналам. Гостехкомиссия России. М.: 1997; и Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К). М.: 2002.

1.1.4 Порядок обращения со служебной информацией

Требования «Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», утвержденные постановлением Правительства РФ от 3 ноября 1994 г. № 1233), распространяются на порядок обращения с документами и другими материальными носителями информации и с иными материальными носителями служебной

информации ограниченного распространения (фото-, кино-, видео- и аудиопленки, машинные носители информации и др.) (п.1, 2 «Положения...»).

Таким образом, требования данного положения неприменимы к создаваемым программным средствам, т. к. эти средства предназначены для обработки и передачи информации в электронном виде, без записи ее на какие-либо машинные носители информации.

В случае если с помощью разрабатываемых средств на какие-либо носители информации помещена информации ограниченного распространения, то на эти носители информации распространяется действие «Положения...».

Кроме того, требования положения неприменимы к создаваемым программным средствам, т. к. информация, имеющаяся на материальных носителях программных средств (компакт-диски с дистрибутивом прототипов и исходными кодами, программная и эксплуатационная документация, программа и методики испытаний) не отнесена к служебной информации ограниченного распространения.

Положения, определенные в документе «Порядок проведения классификации информационных систем персональных данных», утвержденном приказом Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 определяют порядок проведения классификации информационных систем персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Таким образом, требования данного документа не распространяются на разрабатываемые прототипы эталонной среды разработки, сборки и обновления операционной системы и прикладных приложений, прототип эталонной операционной системы, и прототип программного обеспечения управления базами данных, т. к. они не содержат персональных данных и, следовательно, не могут быть классифицированы как информационные системы персональных данных.

Прототип системы публичного доступа к общесистемным и прикладным компонентам национальной программной платформы, содержащимся в фонде алгоритмов и программ, в свою очередь, может быть отнесен к некой информационной системе, содержащей персональные данные.

Проведем предварительную классификацию данной информационной системы.

Классификация информационных систем проводится государственными органами, муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее операторы).

Уточненная классификация информационной системы должна быть проведена на этапе непосредственного создания информационной системы или в ходе её эксплуатации с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

Проведение классификации информационных систем включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса и его документальное оформление.

В нашем случае исходными данными по прототипу системы публичного доступа к общесистемным и прикладным компонентам национальной программной платформы могут служить только требования, изложенные в техническом задании на выполнение работ.

При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных – Хпд;

- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) - $X_{\text{нпд}}$;
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

Предложения по оценке исходных данных приведены в таблице 2.29.

Таблица 2.29 — Исходные данные к прототипу системы публичного доступа.

Категория исходных данных	Значение	Обоснование
Категория обрабатываемых в информационной системе персональных данных – $X_{\text{пд}}$	$X_{\text{пд}} = \text{Категория 4}$	Примечание 1
Объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) - $X_{\text{нпд}}$	$X_{\text{нпд}} = 1$	Примечание 2
Заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе	Типовые	Примечание 3
Структура информационной системы	Распределенная информационная система	Примечание 4
Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного	Имеющая подключение	Примечание 5

Продолжение таблицы 2.29

информационного обмена		
Режим обработки персональных данных	Многопользовательски й	Примечание 6
Режим разграничения прав доступа пользователей информационной системы	Система с разграничением прав доступа	Примечание 7
Местонахождение технических средств информационной системы	В пределах Российской Федерации	Примечание 8

Примечания

1. Различают четыре категории персональных данных – Хпд:

– категория 1 — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

– категория 2 — персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

– категория 3 — персональные данные, позволяющие идентифицировать субъекта персональных данных;

– категория 4 — обезличенные и (или) общедоступные персональные данные.

К системе публичного доступа фонда алгоритмов и программ должны быть допущены должностные лица государственных органов, муниципальных органов, юридических организаций, следовательно, непосредственно персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни, позволяющих идентифицировать субъекта персональных данных и получить о нем дополнительную информацию для регистрации их в системе, не требуется. Таким образом, в системе могут содержаться обезличенные и (или) общедоступные персональные данные, т. е. отнесенные к категории 4.

2. Различают три значения объема обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) — Хнпд:

1) в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2) в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3) в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Учитывая, что фонд алгоритмов и программ должен функционировать в интересах всех заинтересованных потребителей Российской Федерации, определим значение объема как 1, с одновременной обработкой более чем 100 000 субъектов персональных данных.

3. По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, информационные системы подразделяются на типовые и специальные информационные системы.

Типовые информационные системы – информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

– информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

– информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Таким образом, систему публичного доступа необходимо отнести к типовым информационным системам.

4. По структуре информационные системы подразделяются:

– на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);

– на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

– на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

Таким образом, в соответствии с приведенной классификацией, система публичного доступа однозначно должна относиться к распределенным информационным системам.

5. По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

Система публичного доступа должна быть подключена к сетям связи общего пользования и (или) сетям международного информационного обмена, в частности, к сети Internet, следовательно, она является имеющей подключение.

6. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

Система публичного доступа является многопользовательской системой.

7. По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

Учитывая, что практически в любой системе должны существовать пользователи, выполняющие функции по настройке, обслуживанию и сопровождению системы (администраторы) и имеющие расширенные права на изменение программного обеспечения системы, его конфигурацию и информации содержащейся в системе, то система публичного доступа должна быть однозначно классифицирована как система с разграничением прав доступа.

8. Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

Предполагается, что технические средства системы публичного доступа будут расположены в пределах Российской Федерации.

Класс типовой информационной системы определяется в соответствии со значениями категории обрабатываемых в информационной системе персональных данных – Хпд и объемом обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) Хнпд. Классы типовой информационной системы приведены в таблице 2.30

Таблица 2.30 — Классы типовой информационной системы

Хпд \ Хнпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

- класс 1 (K1) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

- класс 2 (K2) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

- класс 3 (K3) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

- класс 4 (K4) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Вывод: система публичного доступа, имеющая 4 категорию обрабатываемых персональных данных и объем обрабатываемых данных типа 1, относится к классу 4 (K4) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

В случае если заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе, будут изменены с типовых на специальные, то, по результатам анализа исходных данных, класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми согласно пункту 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении

безопасности персональных данных при их обработке в информационных системах персональных данных».

Результаты классификации информационных систем оформляются соответствующим актом оператора.

1.1.5 Порядок сертификации средств защиты информации

Порядок сертификации определен приказом Председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199, которым введено в действие «Положение о сертификации средств защиты информации по требованиям безопасности информации».

Положение устанавливает организационную структуру Системы сертификации средств защиты информации по требованиям безопасности информации, функции субъектов сертификации, порядок сертификации, государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации, общие требования к нормативным и методическим документам по сертификации средств защиты информации. В приложениях к Положению приведены: перечень средств защиты информации, подлежащих сертификации в системе сертификации, формы заявок на проведение сертификации и продление срока действия сертификата, решения по заявке на проведение сертификации (продлению срока действия сертификата), сертификата и лицензии на применение знака соответствия.

Положение разработано в соответствии с Законом Российской Федерации от 10 июня 1993 г. № 5151-1 «О сертификации продукции и услуг» с изменениями и дополнениями, внесенными федеральными законами от 27 декабря 1995 г. № 211-ФЗ, от 2 марта 1998 г. № 30-ФЗ, от 31 июля 1998 г. № 154-ФЗ (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, № 26, ст. 966; Собрание законодательства Российской Федерации, 1996, № 1, ст. 4; 1998, № 10, ст. 1143; 1998, № 31, ст. 3832), Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне», с изменениями

и дополнениями, внесенными постановлением Конституционного Суда Российской Федерации от 27 марта 1996 г. № 8-П, Федеральным законом от 6 октября 1997 г. № 131-ФЗ (Российская газета, от 21 сентября 1993 г., № 182; Собрание законодательства Российской Федерации, 1996, № 15, ст. 1768; Российская газета, от 9 октября 1997 г., № 196), Федеральным законом от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (Собрание законодательства Российской Федерации, 1995, № 8, ст. 609), Законом Российской Федерации от 7 февраля 1992 г. № 2300/1-1 «О защите прав потребителей» с изменениями и дополнениями, внесенными Федеральным законом от 9 января 1996 г. № 2-ФЗ (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, № 15, ст. 766; Собрание законодательства Российской Федерации, 1996, № 3, ст. 140), Федеральным законом «Об участии в международном информационном обмене» от 4 июля 1996 г. № 85-ФЗ, указов Президента Российской Федерации от 19 февраля 1999 г. № 212 и от 29 ноября 1999 г. № 1567, постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» с изменениями и дополнениями, внесенными постановлениями Правительства Российской Федерации от 23 апреля 1996 г. № 509, от 29 марта 1999 г. № 342 (Собрание законодательства Российской Федерации, 1995, № 27, ст. 2579; 1996, № 18, ст. 2142; 1999, № 14, ст. 1722), на основании Правил по проведению сертификации в Российской Федерации, утвержденных постановлением Госстандарта России от 16 февраля 1994 г. № 3 и зарегистрированных в Министерстве юстиции Российской Федерации 21 марта 1994 г., регистрационный номер 521 (Российские вести, от 30 марта 1994 г., № 56) и Порядка проведения сертификации продукции в Российской Федерации, утвержденного постановлением Госстандарта России от 21 сентября 1994 г. № 15 и зарегистрированного в Министерстве юстиции Российской Федерации 5 апреля 1995 г., регистрационный номер 826 (Российские вести, от 1 июня 1995 г., № 100), с изменениями и дополнениями, внесенными постановлением Госстандарта России от 25 июля 1996 г. № 15 и зарегистрированными в

Министерстве юстиции Российской Федерации 1 августа 1996 г., регистрационный номер 1139 (Российские вести, от 8 августа 1996 г., № 147).

Обязательной сертификации подлежат средства защиты информации, предназначенные для защиты сведений, составляющих государственную тайну, а также другой информации с ограниченным доступом, подлежащей защите в соответствии с действующим законодательством, систем управления экологически опасными производствами, объектами, имеющими важное оборонное или экономическое значение и влияющими на безопасность государства, средства общего применения, предназначенные для противодействия техническим разведкам. Основными схемами сертификации средств защиты информации являются:

- для единичных образцов средств защиты информации - проведение испытаний образца на соответствие требованиям по безопасности информации;
- для партии средств защиты информации - проведение испытаний репрезентативной выборки образцов средств на соответствие требованиям по безопасности информации;
- для серийного производства средств защиты информации - проведение типовых испытаний образцов продукции на соответствие требованиям по безопасности информации и последующий инспекционный контроль стабильности характеристик сертифицированной продукции, обеспечивающих (определяющих) выполнение этих требований.

Кроме того, по решению федерального органа по сертификации допускается предварительная проверка (аттестация) производства по утвержденной программе. По согласованию с федеральным органом по сертификации могут быть использованы и другие схемы сертификации, включая применяемые в международной практике.

Сертификация средств защиты информации осуществляется федеральным и аккредитованными органами по сертификации. Сертификационные испытания проводятся аккредитованными испытательными центрами (лабораториями) на их материально-технической базе. В отдельных случаях по согласованию с федеральным органом по сертификации (или органом по сертификации)

допускается проведение испытаний на испытательной базе заявителя данного средства защиты информации.

Правила аккредитации определяются действующим в системе «Положением об аккредитации испытательных центров (лабораторий) и органов по сертификации средств защиты информации».

Органы по сертификации и испытательные центры (лаборатории) несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственной тайны, конфиденциальных сведений, материальных ценностей, предоставленных заявителем, а также за соблюдение авторских прав разработчика при испытаниях его средств защиты информации.

Процедура сертификации включает:

- подачу и рассмотрение заявки на проведение сертификации (продление срока действия сертификата) средств защиты информации;
- сертификационные испытания средств защиты информации и (при необходимости) аттестацию их производства;
- экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия;
- осуществление государственного контроля и надзора, инспекционного контроля соблюдения правил обязательной сертификации и сертифицированных средств защиты информации;
- информирование о результатах сертификации средств защиты информации;
- рассмотрение апелляций.

1.1.5.1 Подача и рассмотрение заявки на проведение сертификации средств защиты информации

Заявитель для получения сертификата направляет в федеральный орган по сертификации заявку на проведение сертификации. Заявка оформляется на бланке заявителя и заверяется печатью.

Федеральный орган по сертификации в месячный срок после получения заявки направляет заявителю в назначенные для проведения сертификации орган по

сертификации и испытательный центр (лабораторию) решения по заявке на проведение сертификации. Орган по сертификации и испытательный центр (лаборатория) могут быть изменены по согласованию с заявителем.

После получения решения заявитель обязан представить в испытательный центр (лабораторию) средства защиты информации в комплектации, согласно техническим условиям или формуляру, на средство защиты, а также комплект необходимой технической и эксплуатационной документации на это средство в соответствии с ЕСКД или ЕСПД.

1.1.5.2 Сертификационные испытания средств защиты информации и аттестация их производства

Сертификационные испытания средств защиты информации проводятся в испытательных центрах (лабораториях) на образцах, конструкция, состав и технология изготовления которых должны быть аналогичны образцам средств защиты информации, поставляемым потребителю, по программам и методикам испытаний, утвержденным органом по сертификации. Количество образцов, порядок их отбора и идентификации должен соответствовать требованиям нормативных и методических документов.

В случае отсутствия на момент сертификации испытательных центров (лабораторий) с соответствующей областью аккредитации федеральный орган по сертификации определяет возможность, место и условия проведения испытаний, обеспечивающих объективность их результатов.

Сроки проведения испытаний устанавливаются договором между заявителем и испытательным центром (лабораторией). По просьбе заявителя его представителям должна быть предоставлена возможность ознакомиться с условиями хранения и испытаний средств защиты информации и предоставленной документации на эти средства в испытательном центре (лаборатории). По результатам испытаний оформляются протоколы и технические заключения, которые направляются испытательным центром (лабораторией) в орган по сертификации, а копия технического заключения — заявителю.

При внесении изменений в конструкцию (состав) средств защиты информации или технологию их производства заявитель (разработчик, изготовитель) извещает об этом орган по сертификации. Последний принимает решение о необходимости проведения новых сертификационных испытаний этих средств.

Сертификация средств защиты информации зарубежного производства проводится по тем же правилам, что и отечественной.

При несоответствии результатов испытаний требованиям нормативных документов федеральный орган по сертификации принимает решение об отказе в выдаче сертификата и направляет заявителю мотивированное заключение. В случае несогласия с отказом в выдаче сертификата заявитель имеет право обратиться в апелляционный совет федерального органа по сертификации для дополнительного рассмотрения материалов сертификации.

1.1.5.3 Получение изготовителем средств защиты информации сертификата дает ему право получить в федеральном органе по сертификации лицензию на применение знака соответствия

В случае сертификации единичных образцов или партии средств защиты информации лицензия на применение знака соответствия заявителю не выдается. Маркирование знаками соответствия средств защиты информации в этом случае производится испытательной лабораторией, проводившей сертификационные испытания.

Владелец лицензии на применение знака соответствия несет ответственность за поставку маркированных средств защиты информации.

1.1.5.4 Требования к нормативным и методическим документам по сертификации средств защиты информации

Сертификация средств защиты информации отечественного и зарубежного производства проводится на соответствие требованиям нормативных документов, действующих в системе сертификации средств защиты информации по требованиям

безопасности информации, и в соответствии с утвержденными органом по сертификации программами и методиками сертификационных испытаний.

В рамках проводимой НИР письмом от Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 14 октября 2011 года № 240/2/3908 в адрес головного исполнителя ООО «ПингВин Софтвер» было рекомендовано формировать требования по безопасности информации к компонентам программной платформы в виде профилей защиты в соответствии с национальным стандартом ГОСТ Р ИСО/МЭК 15408 «Информационная технология Методы и средства обеспечения безопасности Критерии оценки безопасности информационных технологий» и руководящим документом «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002), а также с учетом требований руководящего документа «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999).

Руководящий документ «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» введен в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187 и содержит систематизированный каталог требований к безопасности информационных технологий (ИТ), порядок и методические рекомендации по его использованию при задании требований, разработке, оценке и сертификации продуктов и систем информационных технологий по требованиям безопасности информации.

Руководящий документ разработан в развитие РД Гостехкомиссии России по защите информации от несанкционированного доступа и соответствует ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий», далее по тексту РД – Общие критерии (ОК).

Разработка настоящего руководящего документа направлена на обеспечение практического использования ГОСТ Р ИСО/МЭК 15408-2002 в деятельности заказчиков, разработчиков и пользователей продуктов и систем ИТ при

формировании ими требований, разработке, приобретении и применении продуктов и систем информационных технологий, предназначенных для обработки, хранения или передачи информации, подлежащей защите в соответствии с требованиями нормативных правовых документов или требованиями, устанавливаемыми собственником информации. Руководящий документ предназначен также для органов сертификации и испытательных лабораторий, аккредитованных в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 (Гостехкомиссии России), для использования при проведении оценки и сертификации безопасности ИТ.

Основной целью руководящего документа является повышение доверия к безопасности продуктов и систем информационных технологий. Положения руководящего документа направлены на создание продуктов и систем информационных технологий с уровнем безопасности, адекватным имеющимся по отношению к ним угрозам и проводимой политике безопасности, с учетом условий применения, что должно обеспечить оптимизацию продуктов и систем ИТ по критерию «эффективность-стоимость».

Под безопасностью информационной технологии понимается состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений.

Доверие к безопасности ИТ обеспечивается как реализацией в них необходимых функциональных возможностей, так и осуществлением комплекса мер по обеспечению безопасности при разработке продуктов и систем ИТ, проведением независимых оценок их безопасности и контролем ее уровня при эксплуатации.

Требования к безопасности конкретных продуктов и систем ИТ устанавливаются исходя из имеющихся и прогнозируемых угроз безопасности, проводимой политики безопасности, а также с учетом условий их применения. При формировании требований должны в максимальной степени использоваться компоненты требований, представленные в настоящем руководящем документе.

Допускается также использование и других требований безопасности, при этом уровень детализации и способ выражения требований, представленных в настоящем руководящем документе, должны использоваться в качестве образца. Требования безопасности могут задаваться Заказчиком в техническом задании на разработку продуктов и систем ИТ или формироваться Разработчиком при создании им продуктов ИТ самостоятельно.

Требования безопасности, являющиеся общими для некоторого типа продуктов или систем ИТ, могут оформляться в виде представленной в настоящем руководящем документе структуры, именуемой «Профиль защиты». Профили защиты, прошедшие оценку в установленном порядке, регистрируются и помещаются в каталог оцененных профилей защиты.

Оценка и сертификация безопасности ИТ проводится на соответствие требованиям, представляемым Разработчиком продукта или системы ИТ в Задании по безопасности. Требования заданий по безопасности продуктов и систем ИТ, предназначенных для использования в областях применения, регулируемых государством, должны соответствовать требованиям установленных профилей защиты.

Руководящий документ состоит из трех частей:

- часть 1 РД определяет виды требований безопасности (функциональные и требования доверия), основные конструкции представления требований безопасности (профиль защиты, задание по безопасности) и содержит основные методические положения по оценке безопасности ИТ;

- часть 2 РД содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам;

- часть 3 РД содержит систематизированный каталог требований доверия к безопасности и оценочные уровни доверия, определяющие меры, которые должны быть приняты на всех этапах жизненного цикла продуктов или систем ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям.

Требования безопасности, содержащиеся в руководящем документе, могут уточняться и дополняться по мере совершенствования правовой и нормативной базы, развития информационных технологий и совершенствования методов обеспечения безопасности. Внесение изменений в руководящий документ осуществляется в порядке, устанавливаемом Гостехкомиссией России.

Руководящий документ определяет критерии, за которыми исторически закрепилось название «Общие критерии» (ОК). ОК предназначены для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий (ИТ). Устанавливая общую базу критериев, ОК делают результаты оценки безопасности ИТ значимыми для более широкой аудитории.

ОК дают возможность сравнения результатов независимых оценок безопасности. Это достигается предоставлением общего набора требований к функциям безопасности продуктов и систем ИТ и к мерам доверия, применяемых к ним при оценке безопасности. В процессе оценки достигается определенный уровень уверенности в том, что функции безопасности таких продуктов или систем, а также предпринимаемые меры доверия отвечают предъявляемым требованиям. Результаты оценки помогут потребителям решить, являются ли продукты или системы ИТ достаточно безопасными для их предполагаемого применения, и приемлемы ли прогнозируемые риски при их использовании.

ОК полезны в качестве руководства как при разработке продуктов или систем с функциями безопасности ИТ, так и при приобретении коммерческих продуктов и систем с такими функциями. При оценке такой продукт или систему ИТ называют объектом оценки (ОО). К таким ОО, например, относятся операционные системы, вычислительные сети, распределенные системы и приложения.

ОК направлены на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью соответственно. ОК могут быть также применены к тем аспектам безопасности ИТ, которые выходят за

пределы этих трех понятий. ОК сосредоточены на угрозах информации, возникающих в результате действий человека, как злоумышленных, так и иных, но возможно также применение ОК и для некоторых угроз, не связанных с человеческим фактором. Кроме того, ОК могут быть применены и в других областях ИТ, но не декларируется их правомочность вне строго ограниченной сферы безопасности ИТ.

ОК применимы к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами. Если предполагается, что отдельные аспекты оценки применимы только для некоторых способов реализации, это будет отмечено при изложении соответствующих критериев.

Некоторые вопросы рассматриваются как лежащие вне области действия ОК, поскольку они требуют привлечения специальных методов или являются смежными по отношению к безопасности ИТ. Часть из них перечислена ниже:

- ОК не содержат критериев оценки безопасности, касающихся административных мер безопасности, непосредственно не относящихся к мерам безопасности ИТ. Известно, однако, что безопасность ОО в значительной степени может быть достигнута административными мерами, такими как организационные меры, управление персоналом, физическая защита и процедурный контроль. Административные меры безопасности в среде эксплуатации ОО рассматриваются в качестве предположений о безопасном использовании там, где они влияют на способность мер безопасности ИТ противостоять установленным угрозам;

- оценка специальных физических аспектов безопасности ИТ, таких как контроль электромагнитного излучения, прямо не затрагивается, хотя многие концепции ОК применимы и в этой области. В частности, рассмотрены некоторые аспекты физической защиты ОО;

- в ОК не рассматривается ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки. Тем не менее, ожидается, что ОК будут использоваться для целей оценки в контексте такой структуры и такой методологии;

– процедуры использования результатов оценки при аттестации продуктов и систем ИТ находятся вне области действия ОК. Аттестация продукта или системы ИТ является административным процессом, посредством которого предоставляются полномочия на их использование в конкретной среде эксплуатации. Оценка концентрируется на тех аспектах безопасности продукта или системы ИТ и на тех аспектах среды эксплуатации, которые могут непосредственно влиять на безопасное использование элементов ИТ. Результаты процесса оценки являются, следовательно, важными исходными материалами для процесса аттестации. Однако, поскольку для оценки не связанных с ИТ характеристик безопасности продукта или системы, а также их соотнесения с аспектами безопасности ИТ более приемлемы другие способы, аттестующим следует предусмотреть для этих аспектов особый подход;

– критерии для оценки специфических качеств криптографических алгоритмов не входят в ОК. Если требуется независимая оценка математических свойств криптографии, встроенной в ОО, то в системе оценки, в рамках которой применяются ОК, необходимо предусмотреть проведение таких оценок.

В соответствии с письмом Федеральной службы по техническому и экспортному контролю, приведенному в приложении А, в приложениях Б, В, Г и Д к научно-техническому отчету представлены рекомендованные ФСТЭК России Профили защиты по требованиям безопасности, которым должны будут удовлетворять разработанные в рамках будущей ОКР программные изделия из состава НПП.

Изложенные в Профилях защиты требования достаточны при использовании изделий для защиты конфиденциальной информации и персональных данных.

Требования для защиты информации, содержащей государственную тайну, должны быть представлены в специальном разделе технического задания на ОКР или в специальном техническом задании на ОКР.

2 ОБОБЩЕНИЕ И ОЦЕНКА РЕЗУЛЬТАТОВ. АНАЛИЗ РАЗЛИЧНЫХ ВАРИАНТОВ СОЗДАНИЯ И ЭКСПЛУАТАЦИИ НАЦИОНАЛЬНОЙ ПРОГРАММНОЙ ПЛАТФОРМЫ

2.1 Защита информации и соблюдение требований ФСТЭК и ФСБ

Анализ существующих данных показал следующие предложения по данной теме:

1) подачу заявки на проведение сертификации средств защиты информации целесообразно делать по окончании разработки программного средства и проведения предварительных испытаний, на этапе доработки изделия по результатам испытаний, когда заказчик имеет удовлетворяющие его результаты работы и не требует внесения дополнительных конструктивных улучшений и изменений. Сроки рассмотрения заявок составляют в среднем 1 месяц;

2) непосредственно сертификационные испытания средств защиты информации и (при необходимости) аттестацию их производства целесообразно выполнять отдельным этапом ОКР продолжительностью от 4 до 6 месяцев. В ходе работы программное средство и документация могут подвергаться доработке с целью удовлетворения требований по сертификации и устранения выявленных недостатков. Результатом выполнения работ по этапу являются заключения испытательной лаборатории, направленные в орган по сертификации, доработанная программная и эксплуатационная документация, доработанный опытный образец программного средства;

3) экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия в этапность ОКР можно не включать, если результатом ОКР не ставить получение именно сертифицированного средства (т. е. получение сертификата соответствия). В противном случае необходимо увеличить срок выполнения ОКР на 3-4 месяца, так как экспертиза требует привлечения значительного числа экспертов в данной области, и по ее выводам может потребоваться не только уточнение результатов

сертификационных испытаний от испытательной лаборатории, но и доработка образца программного средства;

4) в планах будущих ОКР, в рамках создания НПП, предусматривающих создание и сертификацию средств защиты информации после завершения разработки и испытаний необходимо предусматривать этап проведения сертификационных испытаний продолжительностью от 7 до 10 месяцев, без права исполнителя изменить минимальный срок выполнения работ;

5) запросы на проведение сертификации по требованиям безопасности ФСБ России смогут быть предъявлены к программным средствам, техническим средствам и информационным системам, разрабатываемым в рамках НИОКР по тематике НПП, в случаях встраивания в них СКЗИ или других случаях, попадающих в зону ответственности ФСБ России;

6) технические задания на разработку вновь создаваемых средств и систем в рамках реализации Национальной программной платформы должны в обязательном порядке согласовываться с ФСТЭК России и ФСБ России, в части правильного определения требований по безопасности, необходимости сертификации на соответствие им, а также порядка встраивания в действующие информационные системы органов государственного управления и вновь создаваемые.

ПРИЛОЖЕНИЕ А

(обязательное)

Письмо Федеральной службы по техническому и экспортному контролю
(ФСТЭК России) № И111010-01 от 10.10.2011 г. «О требованиях по безопасности
информации» генеральному директору ООО «ПингВин Софтвер»



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК РОССИИ)

Генеральному директору
ООО «ПингВин Софтвер»
Д.В.КОМИССАРОВУ

Пресненский Вал ул., д. 14,
Москва, 123557

“ 14 ” октября 2011 г.
№ 240/ 2/3908

105175 г. Москва, ул. Старая Басманная, д.17

На исх. № И111010-01 от 10.10.2011
О требованиях по безопасности информации

Уважаемый Дмитрий Владимирович!

Обращение ООО «ПингВин Софтвер» по вопросу получения рекомендаций по руководящим, нормативным и методическим документам, определяющим требования по безопасности информации к программным средствам национальной программной платформы, в ФСТЭК России рассмотрено.

Сообщаем, что формирование требований по безопасности информации к указанным компонентам программной платформы рекомендуется осуществлять в виде профилей защиты в соответствии с национальным стандартом ГОСТ Р ИСО/МЭК 15408 «Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий» и руководящим документом «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002), а также с учетом требований руководящего документа «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999).

С уважением,

Начальник 2 управления

А.Куц

ПРИЛОЖЕНИЕ Б

(обязательное)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИЗДЕЛИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ОПЕРАЦИОННАЯ СИСТЕМА

Профиль защиты

ИЗД_ИТ.ОС.ПЗ

Версия 1.0

СОДЕРЖАНИЕ

Б 1 Введение ПЗ	38
Б 1.1 Идентификация ПЗ.....	38
Б 1.2 Аннотация ПЗ	39
Б 1.3 Соглашения.....	39
Б 1.4 Термины и определения.....	41
Б 1.5 Организация ПЗ	43
Б 2 Описание ОО	44
Б 2.1 Тип изделия ИТ	44
Б 2.2 Основные функциональные возможности ОО	44
Б 3 Среда безопасности ОО	50
Б 3.1 Предположения безопасности	50
Б 3.2 Угрозы.....	52
Б 3.3 Политика безопасности объекта эксплуатации	58
Б 4 Цели безопасности	60
Б 4.1 Цели безопасности для ОО	60
Б 4.2 Цели безопасности для среды.....	62
Б 5 Требования безопасности ИТ	65
Б 5.1 Требования безопасности для ОО	65
Б 6 Обоснование	106
Б 6.1 Обоснование целей безопасности	106
Б 6.2 Обоснование требований безопасности.....	112

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БИТ	– безопасность информационных технологий
ЗБ	– задание по безопасности
ИС	– информационная система
ИТ	– информационная технология
НСД	– несанкционированный доступ
ОДФ	– область действия функции безопасности объекта оценки
ОО	– объект оценки
ОС	– операционная система
ОУД	– оценочный уровень доверия
ПБО	– политика безопасности объекта оценки
ПЗ	– профиль защиты
ПФБ	– политика функции безопасности
УК	– управление конфигурацией
ФБО	– функции безопасности объекта оценки
ФТБ	– функциональные требования безопасности

Б 1 ВВЕДЕНИЕ ПЗ

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

Б 1.1 Идентификация ПЗ

Название ПЗ:	Безопасность информационных технологий. Изделия информационных технологий. Операционная система. Профиль защиты.
Семейство ПЗ:	Изделия ИТ.
Функциональная группа:	Операционные системы.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИЗД_ИТ.ОС.ОУД4.ПЗ.
Идентификация ОО:	Операционные системы.
Уровень доверия:	ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий».
Идентификация РД БИТ:	Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 1: Введение и общая модель, ФСТЭК (Гостехкомиссия) России, 2002.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 2: Функциональные требования безопасности, ФСТЭК (Гостехкомиссия) России, 2002.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 3: Требования доверия к безопасности, ФСТЭК (Гостехкомиссия) России, 2002.

Ключевые слова:

Операционная система, средство защиты информации, дискреционное управление доступом, профиль защиты, ОУД4.

Б 1.2 Аннотация ПЗ

Настоящий ПЗ определяет требования безопасности для Операционной системы (далее – объект оценки).

Б 1.3 Соглашения

Руководящий документ ФСТЭК (Гостехкомиссии) России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (далее – РД БИТ) допускает выполнение определенных в части 2 РД БИТ операций над функциональными требованиями. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор», «назначение» и «итерация».

Операция «уточнение» используется для добавления к требованию некоторых подробностей (деталей) и, таким образом, ограничивает диапазон возможностей его

удовлетворения. Результат операции «**уточнение**» в настоящем ПЗ обозначается **полужирным текстом**.

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

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

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

В настоящем ПЗ используются компоненты функциональных требований безопасности, включающие незавершенные операции «**назначение**» в которых область предполагаемых значений уточнена по отношению к исходному компоненту из части 2 РД БИТ. В данных компонентах операции «**назначения**» с уточненной областью предполагаемых значений обозначаются как [**назначение: уточненная область предполагаемых значений**].

Операция «**итерация**» используется для более чем однократного использования компонента функциональных требований безопасности ИТ при различном выполнении разрешенных операций (уточнение, выбор, назначение). Выполнение «итерации» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

Замечания по применению предназначены либо для разъяснения назначения некоторого требования, идентификации вариантов реализации, либо для определения условий выполнения требования. В случае использования, замечания по применению следуют за компонентом требования.

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

Б 1.4 Термины и определения

В настоящем ПЗ применяются следующие термины с соответствующими определениями.

Активы: Информация и ресурсы, подлежащие защите.

Аутентификационные данные: информация, используемая для верификации предъявленного идентификатора.

Аутентификация: Процесс установления подлинности информации, предъявленной администратором безопасности и пользователем ИС при регистрации.

Данные ФБО: Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО.

Доступность: Состояние безопасности активов (информации), характеризующее их готовностью к использованию по запросу уполномоченных лиц, объектов или субъектов, а также возможностью их восстановления в случае сбоя (отказа).

Задание по безопасности: Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного изделия ИТ.

Конфиденциальность: Состояние безопасности активов (информации), характеризующее их защищенностью от несанкционированного доступа и/или раскрытия их содержания неуполномоченным лицам, объектам или процессам.

Область действия ФБО: Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО.

Объект оценки: подлежащее оценке изделие ИТ с документацией.

Политика безопасности объекта эксплуатации: Совокупность

руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

Политика безопасности ОО: Совокупность правил, определяющих режим обеспечения безопасности ОО и представляемых в виде набора функциональных требований безопасности.

Политика функции безопасности: Политика безопасности, осуществляемая ФБ.

Пользователь: Любая сущность (человек-пользователь или внешний объект изделия ИТ) вне ОО, которая взаимодействует с ОО.

Изделие ИТ: Программное, программно-аппаратное или аппаратное обеспечение изделий ИТ, специально разработанное для использования в составе ИС

Профиль защиты: Совокупность требований безопасности для некоторого типа изделий ИТ.

Уполномоченный администратор: Уполномоченный пользователь, ответственный за эксплуатацию ОО.

Функция безопасности: Функциональные возможности части или частей изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных функциональных требований безопасности.

Целостность: Состояние безопасности активов (информации), характеризующее их полнотой и защищенностью от несанкционированного изменения (модификации).

Б 1.5 Организация ПЗ

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

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

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

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

В разделе 5 «Требования безопасности ИТ» на основе частей 2 и 3 РД БИТ определены, соответственно, функциональные требования безопасности ИТ и требования доверия к безопасности ОО.

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

Б 2 ОПИСАНИЕ ОО

Объектом оценки в настоящем ПЗ является операционная система.

Б 2.1 Тип изделия ИТ

Объект оценки представляет собой операционную систему общего назначения. Объект оценки располагает возможностями по управлению используемыми аппаратными и вычислительными ресурсами, такими как процессорное время, оперативная память, устройства ввода-вывода и др.

Объект оценки должен обеспечить централизованное, надежное и гибкое управление всей сетевой средой, реализовать единое представление идентификационной информации.

Объект оценки должен характеризоваться как управляемая, надежная и безопасная ОС. Данные свойства ОО должны достигаться за счет использования файловой системы, обеспечивающей поддержку дисковых томов значительного размера, списков управления доступом и других функции безопасности, а также за счет средств управления приложениями и расширенных возможностей обеспечения безопасности, таких как управляемый доступ к сети, единый вход в систему и др.

Б 2.2 Основные функциональные возможности ОО

В ОО должен быть реализован ряд функциональных возможностей и средств, позволяющих обеспечить безопасность ИТ, надежность ОО, а также упрощающих администрирование ОО и управление ОО. В данном подразделе представлено краткое описание предполагаемых функциональных возможностей и средств.

Б 2.2.1 Основные функциональные возможности обеспечения безопасности

В ОО должны быть включены средства, позволяющие защитить выбранные файлы, приложения и ресурсы. В число таких средств входят списки управления доступом, группы безопасности и механизмы централизованного управления

параметрами безопасности, а также инструменты, позволяющие настраивать эти средства и управлять ими. Вместе они обеспечивают мощную и гибкую инфраструктуру управления доступом.

Б 2.2.1.1 Механизмы централизованного управления параметрами безопасности

Объект оценки должен располагать механизмами, используемыми для управления конфигурацией безопасности клиентских компьютеров в конкретной ИС и параметрами безопасности, затрагивающими учетные записи пользователей. Использование данного механизма должно также позволять обеспечить контроль использования пользователями сетевых ресурсов и централизованного задания единых параметров безопасности управляемых операционных систем.

Задание соответствующих параметров безопасности в сочетании с разрешениями файловой системы и другими средствами безопасности ОО, должно обеспечить безопасную среду для пользователей ИС, ограничив их доступ к запрещенным программам и данным, системным параметрам ОО, исключить возможность модификации файлов системной конфигурации.

Б 2.2.1.2 Группы

Объект оценки должен обеспечивать поддержку механизма групп. Группы должны позволять упростить управление доступом к активам, позволяя назначать разрешения на доступ группе пользователей, а не отдельной учетной записи. Таким образом, исходя из потребностей в доступе к новой информации, учетная запись может быть просто добавлена или удалена из соответствующей группы.

После установки в ОО по умолчанию должен создаваться ряд встроенных групп, предоставляющих право выполнять предопределенные системные задачи.

Б 2.2.1.3 Защита данных пользователя

Объект оценки должен осуществлять функции и политику избирательного (дискреционного) управления доступом, а также располагать механизмами защиты остаточной информации. Избирательное управление доступом должно предоставлять возможность ограничивать и контролировать доступ к системе, приложениям и ресурсам, таким как файлы, папки, принтеры.

Каждый пользователь, пытающийся получить доступ к системе, сначала должен проходить процедуру идентификации и аутентификации, а затем, при попытках получения доступа к активам, – авторизацию, т.е. проверку разрешений пользователя по отношению к какому-либо защищаемому активу.

В ОО доступ к активам должен быть разрешен только уполномоченным на это пользователям. Модель защиты ОО должна включать компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый объект доступа, представленный в ОО, должен быть однозначно ассоциирован с набором атрибутов безопасности, определяющих безопасность защищаемого объекта. Данный набор атрибутов должен формироваться при создании объекта и впоследствии может меняться. Изменение их значений должно быть обеспечено только пользователям, имеющим статус владельца объекта, а также субъектам, которым предоставлены соответствующие полномочия.

Права доступа субъектов к объекту должны определяться посредством дискреционного списка управления доступом. Список управления доступом должен включать перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

Объект оценки должен обеспечивать защиту данных пользователя посредством механизма, обеспечивающего обезличивание (обнуление) остаточной информации в свободных блоках памяти (оперативной и дисковой) перед их предоставлением каким-либо процессам, выполняющимся в режиме пользователя.

Б 2.2.1.4 Аудит событий безопасности

Объект оценки должен обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в ИС. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к ОО или доступа к защищаемым активам. В частности, определяя политику аудита, уполномоченный администратор ОО должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как создание и удаление пользователей ОО или неудачные попытки подключения пользователей к ОО. Запись результатов аудита событий безопасности должна осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору ОО. Просмотр журналов регистрации событий аудита должен выполняться с использованием средств ОО (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

Объект оценки обеспечивает защиту данных аудита от потери, используя различные виды реакции (оповещение администратора ОО, возможность аварийного завершения работы ОО и т.д.) при условии невозможности внесения в журнал аудита записи о событиях безопасности.

Б 2.2.1.5 Идентификация и аутентификация

Объект оценки должен требовать, чтобы все субъекты доступа уникально идентифицировались и аутентифицировались при доступе к ОО с помощью ввода идентификатора и пароля. Идентификация и аутентификация должны осуществляться до выполнения субъектом доступа каких-либо действий. ОО должен поддерживать аутентификацию пользователей вместе с их авторизацией. Предусматривается, что авторизация пользователей представляет начальный

уровень для разрешения доступа к локальным и сетевым ресурсам. При доступе пользователя к ОО для безопасной передачи его идентификационной и аутентификационной информации должен предоставляться доверенный маршрут.

Объект оценки должен поддерживать локальную базу данных и каталог безопасности, хранящие информацию об учетных записях пользователей. Каждая учетная запись должна быть представлена идентификатором пользователя, однозначно связанным с его неким уникальным идентификатором, аутентификационной информацией, информацией о членстве в группах, ассоциированными правами и полномочиями (привилегиями).

Объект оценки должен обеспечивать хранение паролей в преобразованном формате. ОО должен предоставлять средства усиления безопасности паролей через использование механизмов, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторяемости) и время смены пароля.

Пользователям предоставляется возможность согласованной однократной регистрации. Если пользователю необходимо получить доступ к приложению в сети, то при осуществлении его первой попытки потребуются выполнить проверку подлинности, в ходе которой пользователю будет предложено ввести свои учетные данные. После ввода эти данные должны связываться с запрошенным приложением. При осуществлении в будущем попыток доступа к этому приложению сохраненные учетные данные должны использоваться повторно, и не требовать повторного ввода.

Объект оценки должен предоставлять механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором ОО или по истечении времени действия, заданного для счетчика блокировки.

Б 2.2.1.6 Защита системных файлов ОО

В ОО должна быть реализована поддержка механизма, обеспечивающего защиту от перезаписи и удаления защищаемых системных файлов. Средства защиты файлов должны работать в фоновом режиме и предотвращать возможность изменения или замещения системных файлов другими программами. Данный механизм должен исключить вероятность аварийного завершения работы системы или отказа приложений в случаях модификации, перемещения или удаления системных файлов, произошедших по неосторожности или в результате воздействия системных вирусов и других вредоносных программ.

Б 2.2.1.7 Защита ФБО

Объект оценки должен предоставлять ряд возможностей для обеспечения защиты функций безопасности ОО. Изоляция процессов и поддержания домена безопасности должны обеспечивать безопасное выполнение функций безопасности ОО. Возможность осуществления периодического тестирования среды функционирования ОО (аппаратной части) и собственно самих функций безопасности ОО должно обеспечивать поддержание уверенности администратора ОО в целостности и корректности функционирования функций безопасности ОО.

Б 2.2.2 Основные функциональные возможности повышения надежности

Объект оценки должен обеспечивать надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

Б 2.2.3 Средства администрирования, управления и поддержки

В состав ОО должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг).

Б 3 СРЕДА БЕЗОПАСНОСТИ ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

- предположений относительно предопределенного использования ОО и аспектов безопасности среды ОО;
- угроз безопасности, которым нужно противостоять средствами ОО;
- политики безопасности объекта эксплуатации, которой должен следовать ОО.

Б 3.1 Предположения безопасности

Б 3.1.1 Предположения относительно предопределенного использования ОО

Предположение-1

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Предположение-2

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположение-3

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Предположение-4

Загрузка ОО должна проходить в доверенной среде, предотвращающей несанкционированное прерывание процесса загрузки ОО и использование

инструментальных средств, позволяющих осуществить доступ к защищаемым активам ОО в обход механизмов защиты.

Предположение-5

Для предотвращения несанкционированного доступа к системным компонентам ОО должна быть исключена возможность запуска встроенных программ отладки.

Б 3.1.2 Предположения относительно среды функционирования ОО

Предположение, связанное с физической защитой ОО

Предположение-6

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположения, имеющие отношение к персоналу

Предположение-7

Персонал, ответственный за администрирование ОО, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

Предположение-8

Уполномоченные на доступ к ОО пользователи должны быть доверенными, руководствоваться в своей работе эксплуатационной документацией на ОО, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

Б 3.2 Угрозы

В настоящем ПЗ определены следующие угрозы, которым противостоит ОО.

Угроза-1

1. **Аннотация угрозы** – осуществление доступа к пользовательским данным неуполномоченными на это пользователями ОО.

2. **Источники угрозы** – пользователи ОО.

3. **Способ реализации угрозы** – осуществление доступа к пользовательским данным локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

4. **Используемые уязвимости** – недостатки механизмов разграничения доступа к пользовательским данным, связанные с возможностью предоставления доступа к пользовательским данным неуполномоченным на это пользователям ОО.

5. **Вид активов, потенциально подверженных угрозе** – пользовательские данные.

6. **Нарушаемые свойства безопасности активов** – конфиденциальность, целостность, достоверность, доступность.

7. **Возможные последствия реализации угрозы** – несанкционированное ознакомление с пользовательскими данными; несанкционированная модификация (в том числе подмена) пользовательских данных; несанкционированное удаление пользовательских данных.

Угроза-2

1. **Аннотация угрозы** – осуществление доступа и выполнение исполняемых программ неуполномоченными на это пользователями ОО.

2. **Источники угрозы** – пользователи ОО.

3. **Способ реализации угрозы** – осуществление доступа и выполнение исполняемых программ локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

4. **Используемые уязвимости** – недостатки механизмов разграничения доступа к исполняемым программам, связанные с возможностью доступа и

выполнения исполняемых программ неуполномоченными на это пользователями ОО.

5. Вид активов, потенциально подверженных угрозе – исполняемые программы.

6. Нарушаемое свойство безопасности активов – несанкционированное выполнение.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, выдаваемой после отработки исполняемых программ; нарушение режимов функционирования ОО.

Угроза-3

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся на объектах ОО (файлах, папках, и т.п.).

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем (в том числе ОС)).

3. Способ реализации угрозы – осуществление удаленного доступа к ОО с использованием средств, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; пользовательские данные.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемыми данными ФБО и пользовательскими данными.

Угроза-4

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; пользовательские данные.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемыми данными ФБО и пользовательскими данными; невозможность однозначного сопоставления совершенных в ОО действий с пользователем, совершившим данные действия.

Угроза-5

1. Аннотация угрозы – осуществление доступа к данным аудита ОО пользователями ОО и неуполномоченными на это администраторами ОО и возможность несанкционированного удаления и модификации данных аудита ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способы реализации угрозы – осуществление доступа к данным аудита ОО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к данным аудита, связанные с возможностью осуществления доступа к данным аудита пользователями ОО и неуполномоченными на это администраторами ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – подконтрольность, целостность, конфиденциальность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля действий пользователей ОО и администраторов ОО, а также контроля процесса функционирования ОО в целом; навязывание администраторам ОО, ответственным за контроль данных аудита ОО, ложных (модифицированных) данных аудита; несанкционированное ознакомление о произошедших в ОО событиях.

Угроза-6

1. Аннотация угрозы – потеря данных аудита ОО вследствие переполнения выделенного для задач аудита хранилища информации.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – переполнение выделенного для задач аудита хранилища информации.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за переполнения хранилища данных аудита ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

Угроза-7

1. Аннотация угрозы – осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к данным ФБО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств управляемых клиентских и серверных ОС.

4. Используемые уязвимости – недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

5. Вид активов, потенциально подверженных угрозе – данные ФБО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, доступность, достоверность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными ФБО (конфигурационные файлы, служебная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

Угроза-8

1. Аннотация угрозы – осуществление доступа к ОО и защищаемым активам неуполномоченными пользователями ОО или администраторами ОО путем использования открытой сессии, незавершенной во время работы с ОО другим уполномоченным пользователем ОО или администратором ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – использование открытой сессии, незавершенной во время работы с ОО другим уполномоченным пользователем ОО или администратором ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью использования открытой сессии, незавершенной во время работы с ОО другим уполномоченным пользователем ОО или администратором ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; пользовательские данные.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемыми данными ФБО и пользовательскими данными.

Угроза-9

1. Аннотация угрозы – нарушение режимов функционирования ОО, а также потеря или искажение данных ФБО и пользовательских данных вследствие сбоев и отказов программного обеспечения и оборудования ОО.

2. Источники угрозы – программное обеспечение и оборудование ОО.

3. Способ реализации угрозы – сбои и отказы программного обеспечения и оборудования ОО.

4. Используемые уязвимости – недостатки механизмов защиты ОО от сбоев и отказов программного обеспечения и оборудования ОО; недостатки механизмов безопасного восстановления ОО после сбоев и отказов программного обеспечения и оборудования ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; пользовательские данные; программное обеспечение ОО.

6. Нарушаемое свойство безопасности активов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; потеря и искажение данных ФБО и пользовательских данных.

Б 3.3 Политика безопасности объекта эксплуатации

Объект оценки должен следовать приведенным ниже правилам политики безопасности объекта эксплуатации.

Политика безопасности-1

Должно быть обеспечено наличие надлежащих корректно функционирующих средств администрирования ОО, доступных только уполномоченным администраторам ОО. Уполномоченным пользователям ОО должна быть предоставлена возможность модификации собственных аутентификационных данных.

Политика безопасности-2

Должны быть обеспечены надлежащая регистрация и предупреждение администратора ОО о любых событиях, относящихся к безопасности ОО. Должна быть обеспечена возможность для администратора ОО выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

Политика безопасности-3

Должна быть обеспечена возможность для уполномоченных на это пользователей ОО ограничивать права доступа к защищаемым активам для других пользователей ОО и администраторов ОО.

Политика безопасности-4

Должна быть обеспечена невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

Политика безопасности-5

Должна быть обеспечена недоступность информационного содержания освобождаемой памяти, выделяемой процессам.

Политика безопасности-6

Должна быть обеспечена возможность периодического контроля целостности ФБО и его данных, а также возможность регламентного тестирования ОО и среды функционирования ОО на предмет корректности функционирования.

Политика безопасности-7

Должен быть предоставлен механизм аутентификации.

Б 4 ЦЕЛИ БЕЗОПАСНОСТИ

Б 4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Разграничение доступа к защищаемым активам

ОО должен обеспечивать доступ к защищаемым активам только уполномоченным на это пользователям ОО и администраторам ОО. ОО должен обеспечивать возможность уполномоченным на это пользователям ОО и администраторам ОО ограничивать права доступа к защищаемым активам для других пользователей ОО и администраторов ОО.

Цель безопасности-2

Разграничение доступа к ОО

ОО должен обеспечивать доступ к ОО только уполномоченным на это пользователям ОО и администраторам ОО. Должны быть предусмотрены механизмы блокирования сеанса пользователя ОО и администратора ОО, осуществляемого по их инициативе, а также иницилируемого ФБО и основанного на интервале времени бездействия пользователя ОО или администратора ОО.

Цель безопасности-3

Аудит событий

ОО должен располагать надлежащими механизмами регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации должны предоставлять уполномоченным администраторам ОО возможность выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

Цель безопасности-4

Защита данных аудита

ОО должен обеспечивать защиту данных аудита от несанкционированного использования, предоставляя доступ к данным аудита только уполномоченным администраторам ОО, и предотвращать потерю данных аудита в случае переполнения их хранилища.

Цель безопасности-5

Защита остаточной информации

ОО должен обеспечивать недоступность информационного содержания освобождаемой памяти, выделяемой процессам.

Цель безопасности-6

Наличие средств администрирования

ОО должен располагать надлежащими корректно функционирующими средствами администрирования ОО, доступными только уполномоченным администраторам ОО. ОО должен предоставить для уполномоченных пользователей ОО возможность модификации собственных аутентификационных данных.

Цель безопасности-7

Защита данных ФБО

ОО должен обеспечивать защиту данных ФБО, поддерживая домен для функционирования ФБО.

Цель безопасности-8

Доверенная аутентификация

ОО должен обеспечить невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

Цель безопасности-9

Безопасное восстановление

Должна быть обеспечена возможность безопасного восстановления ОО после сбоев и отказов программного обеспечения и оборудования ОО.

Цель безопасности-10

Контроль функционирования

ОО должен предоставлять возможность периодического контроля целостности ФБО и его данных, а также возможность собственного регламентного тестирования и тестирования среды функционирования ОО на предмет корректности функционирования.

Цель безопасности-11

Функция безопасности

ОО должен предоставлять механизм аутентификации.

Б 4.2 Цели безопасности для среды

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

Цель для среды функционирования ОО-1

Доверительная среда функционирования

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Цель для среды функционирования ОО-2

Контролируемые точки доступа

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и

системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-3

Эксплуатация ОО

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Цель для среды функционирования ОО-4

Физическая защита ОО

Должна быть исключена возможность несанкционированного физического доступа к компьютеру с установленным ОО.

Цель для среды функционирования ОО-5

Требования к администраторам ОО

Персонал, ответственный за администрирование ОО, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

Цель для среды функционирования ОО-6

Требования к пользователям ОО

Уполномоченные на доступ к ОО пользователи должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на ОО, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

Цель для среды функционирования ОО-7

Доверенная загрузка

Должна быть обеспечена загрузка ОО в доверенной среде, предотвращающей несанкционированное прерывание процесса загрузки ОО и использование

инструментальных средств, позволяющих осуществить доступ к защищаемым активам ОО в обход механизмов защиты.

Цель для среды функционирования ОО-8

Отключение встроенных программ отладки

Для предотвращения несанкционированного доступа к системным компонентам ОО должна быть исключена возможность запуска встроенных программ отладки.

Б 5 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ

В данном разделе ПЗ представлены требования безопасности ИТ, которым должен удовлетворять ОО. Функциональные требования безопасности, представленные в настоящем ПЗ, основаны на функциональных компонентах из части 2 РД БИТ, а также включают один функциональный компонент, сформулированный в явном виде. Требования доверия основаны на компонентах требований доверия из части 3 РД БИТ и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД⁴, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий». Функция безопасности «Аутентификация» реализуется механизмом паролей.

Б 5.1 Требования безопасности для ОО

Б 5.1.1 Функциональные требования безопасности ОО

Функциональные компоненты из части 2 РД БИТ, на которых основаны функциональные требования безопасности ОО, а также компонент сформулированных в явном виде расширенных ФТБ приведены в таблице 5.1.

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.4	Предотвращение потери данных аудита

Идентификатор компонента требований	Название компонента требований
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_RIP.1	Ограниченная защита остаточной информации
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.2	Идентификация до любых действий пользователя
FIA_USB.1 (EXT)	Связывание пользователь-субъект
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_MTD.2	Управление ограничениями данных ФБО
FMT_REV.1	Отмена
FMT_SAE.1	Ограниченная по времени авторизация
FMT_SMR.1	Роли безопасности
FPT_AMT.1	Тестирование абстрактной машины
FPT_RCV.1	Ручное восстановление
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_STM.1	Надежные метки времени
FPT_TST.1	Тестирование ФБО
FTA_SSL.1	Блокирование сеанса, инициированное ФБО
FTA_SSL.2	Блокирование, инициированное пользователем
FTA_TSE.1	Открытие сеанса с ОО
FTP_TRP.1	Доверенный маршрут

Б 5.1.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

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

- а) запуск и завершение выполнения функций аудита;
- б) [события, приведенные во втором столбце таблицы 5.2, а также [назначение: *другие специально определенные события, потенциально подвергаемые аудиту*]].

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

- а) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);
- б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ, [информацию, определенную в третьем столбце таблицы 5.2, а также [назначение: *другую относящуюся к аудиту информацию*]].

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_SAR.1	Чтение информации из записей аудита	
FAU_SAR.2	Неуспешные попытки читать информацию из записей аудита	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во время сбора данных аудита	
FAU_STG.3	Формирование предупреждения после превышения порога заполнения журнала	

Компонент	Событие	Детализация
	аудита	
FAU_STG.4	Предотвращение регистрации событий или выполнение останова ОО при переполнении журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на объекте, на который распространяется политика дискреционного управления доступом	Идентификатор объекта
FIA_AFL.1	Достижение определенного уполномоченным администратором числа неуспешных попыток доступа к ОО	
FIA_SOS.1	Отклонение или принятие ФБО любого проверенного пароля	
FIA_UAU.2	Все случаи использования механизма аутентификации	
FIA_UID.2	Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	
FIA_USB.1 (EXT)	Успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта)	
FMT_MOF.1	Все модификации режимов функционирования функций, указанных в компоненте FMT_MOF.1	
FMT_MSA.1	Все модификации значений атрибутов безопасности, перечисленных в элементе FDP_ACF.1.1 компонента FDP_ACF.1	
FMT_MSA.3	Модификации настройки по умолчанию ограничительных правил политики дискреционного управления доступом. Все модификации начальных значений	

Компонент	Событие	Детализация
	атрибутов безопасности, используемых в политике дискреционного управления доступом	
FMT_MTD.1	Все модификации значений данных ФБО	
FMT_MTD.2	Модификация порогового значения количества неуспешных попыток аутентификации	
FMT_REV.1 (1)	Все попытки отменить атрибуты безопасности, ассоциированные с пользователями ОО	
FMT_REV.1 (2)	Все попытки отменить атрибуты безопасности, ассоциированные с объектами	
FMT_SAE.1	Назначение срока действия для аутентификационных данных. Блокирование ассоциированной с пользователем учетной записи	
FMT_SMR.1	Модификация группы пользователей – исполнителей роли пользователя ОО и администратора ОО. Каждое использование прав, предоставляемых ролью пользователя ОО и администратора ОО	Роль
FPT_AMT.1	Выполнение тестирования аппаратной среды и результаты тестирования	
FPT_RCV.1	Сбой и прерывание обслуживания	Тип сбоя и прерывания
FPT_STM.1	Изменения внутреннего представления времени	
FPT_TST.1	Выполнение и результаты самотестирования ФБО	
FTA_SSL.1	Все попытки разблокирования интерактивного сеанса	

Компонент	Событие	Детализация
FTA_SSL.2	Все попытки разблокирования интерактивного сеанса	
FTA_TSE.1	Все попытки открытия сеанса пользователя	
FTP_TRP.1	Попытки аутентификации и разблокирования	

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 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.2 «Идентификация до любых действий пользователя».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченному администратору ОО] возможность читать [всю информацию аудита] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **уполномоченному администратору ОО** 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 **уполномоченных администраторов ОО**, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны **предоставлять** возможность выполнить поиск, сортировку данных аудита, основанные на [

следующих атрибутах:

- а) идентификатор пользователя;
- б) [назначение: *другие критерии*]

].

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SEL.1 Избирательный аудит

FAU_SEL.1.1 ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой совокупности по следующим атрибутам:

- а) идентификатор пользователя;
- б) [назначение: *список дополнительных атрибутов, на которых основана избирательность аудита*].

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FMT_MTD.1 «Управление данными ФБО».

FAU_STG.1 Защищенное хранение журнала аудита

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

FAU_STG.1.2 ФБО должны быть способны к предотвращению модификации записей 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, направленные на сохранение данных журнала аудита и обеспечивающие*

непрерывность процесса аудита], если журнал аудита **превысит** [установленный уполномоченным администратором ОО размер].

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны *предотвращать события, подвергающиеся аудиту, исключая предпринимаемые уполномоченным администратором ОО* и [назначение: *действия, направленные на невозможность совершения дальнейших событий, связанных с безопасностью ОО*], при переполнении журнала аудита.

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

Б 5.1.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] для [а) [назначение: *список субъектов ОО*], действующих от имени пользователей;
б) [назначение: *список именованных объектов ОО*];
в) [назначение: *список операций между субъектами и объектами*]].

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 дискреционного управления доступом] к объектам, основываясь на [

следующем:

- а) ассоциированные с субъектом идентификатор учетной записи пользователя, принадлежность к группе (группам);
- б) следующие, ассоциированные с объектами, атрибуты управления доступом: [**назначение:** *список атрибутов управления доступом, которые должны обеспечить возможность:*
 - ♣ *ассоциировать разрешение или запрет на выполнение операций с идентификаторами одного или более пользователей;*
 - ♣ *ассоциировать разрешение или запрет на выполнение операций с идентификаторами одной или более групп;*
 - ♣ *ассоциировать разрешение или запрет на выполнение операций по умолчанию]*

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: [**назначение:** *набор правил, определяющих политику дискреционного управления доступом, в которых:*

- а) *для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда идентификатор субъекта соответствует идентификатору, определенному в атрибутах управления доступом объекта;*
- б) *для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда субъект входит в состав группы, идентификатор которой, определен в атрибутах управления доступом объекта;*
- в) *для каждой операции должно быть определено правило или правила использования атрибутов разрешения по умолчанию в случаях, когда идентификатор субъекта не соответствует определенному в атрибутах управления доступом объекта и*

субъект входит в состав группы, идентификатор которой, не определен в атрибутах управления доступом объекта

].

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».

FDP_RIP.1 Ограниченная защита остаточной информации

FDP_RIP.1.1 ФБО должны обеспечить недоступность любого предыдущего информационного содержания **памяти** при освобождении памяти [процессами].

Зависимости: отсутствуют.

Б 5.1.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [назначение: *определенное уполномоченным администратором ОО число*] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

FIA_AFL.1.2 При **достижении** определенного в элементе FIA_AFL.1.1 числа неуспешных попыток аутентификации ФБО должны: [назначение: *список действий, направленных на дальнейшее предотвращение*

попыток доступа со стороны субъекта, ограниченное временным интервалом].

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

Замечание по применению:

Конкретизация данного требования совместно с требованием FIA_SOS.1 в ЗБ должна обеспечивать возможность для механизмов безопасности, реализующих функции безопасности «Аутентификация», предоставлять адекватную защиту от нарушения безопасности ОО нарушителем с низким потенциалом нападения.

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

- [
- а) идентификатор пользователя;
 - б) принадлежность к группе;
 - в) [**назначение:** *другие атрибуты безопасности пользователя*]
-].

Зависимости: отсутствуют.

Замечание по применению:

Под пользователями в настоящем компоненте требований понимаются все идентифицированные в FMT_SMR.1 роли.

FIA_SOS.1 Верификация секретов

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

Зависимости: отсутствуют.

Замечание по применению:

Конкретизация данного требования совместно с требованием FIA_AFL.1 в ЗБ должна обеспечивать возможность для механизмов безопасности, реализующих функции безопасности «Аутентификация», предоставлять адекватную защиту от нарушения безопасности ОО нарушителем с низким потенциалом нападения.

FIA_UAU.2 Аутентификация до любых действий пользователя

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

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

FIA_UAU.7 Аутентификация с защищенной обратной связью

FIA_UAU.7.1 ФБО должны предоставлять **субъекту доступа** [возможность ввода аутентификационной информации в скрытом виде] во время выполнения аутентификации.

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

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый **субъект доступа** был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: отсутствуют.

FIA_USB.1 (EXT) Связывание пользователь-субъект

FIA_USB.1.1 (EXT) ФБО должны ассоциировать следующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя:

- а) идентификатор пользователя, который ассоциируется с возможными для аудита событиями;
- б) идентификатор или идентификаторы пользователя, используемые для осуществления политики дискреционного управления доступом;
- в) принадлежность к группе или группам, используемая для осуществления политики дискреционного управления доступом;
- г) [назначение: *любые другие атрибуты безопасности пользователя*].

FIA_USB.1.2 (EXT) ФБО должны устанавливать следующие правила начальной ассоциации атрибутов безопасности пользователя с субъектами, действующими от имени пользователя:

- а) [назначение: *правила начальной ассоциации*].

FIA_USB.1.3 (EXT) ФБО должны устанавливать следующие правила, определяющие возможность изменения атрибутов безопасности пользователя, ассоциированных с субъектами, действующими от имени пользователя:

- а) [назначение: *правила изменения атрибутов*].

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

Б 5.1.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность определять режим выполнения, модифицировать режим выполнения функций, **связанных с:**

[

- а) аудитом;

б) [**назначение:** *другие функции*]

]

только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предоставляющую** возможность модифицировать атрибуты безопасности, [перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1], только [**назначение:** *уполномоченные идентифицированные роли*].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,

FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предусматривающую** ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления **политики дискреционного управления доступом**.

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

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 [выполнения операций, указанных во втором столбце таблицы 5.3, а также [**назначение:** *другие операции*]] **над данными**, [указанными в третьем столбце

таблицы 5.3, а также **[назначение: список других данных ФБО]** только **[назначение: уполномоченные идентифицированные роли]**.

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.3 – Управляемые данные ФБО

Компонент	Операция	Данные ФБО
FAU_GEN.1	удаление, очистка, создание	журнал аудита
FAU_STG.3	установление, модификация	размер журнала аудита
FIA_ATD.1	установление, модификация	атрибуты безопасности пользователя
FIA_UAU.2	установление, модификация	аутентификационные данные (пароль)
FIA_UID.2	установление, модификация	идентификатор пользователя
FIA_USB.1 (EXT)	переопределение	заданные по умолчанию атрибуты безопасности пользователя
FPT_STM.1	модификация	представление времени

FMT_MTD.2 Управление ограничениями данных ФБО

FMT_MTD.2.1 ФБО должны предоставлять определение ограничений для [порогового значения количества неуспешных попыток аутентификации] только **[назначение: уполномоченные идентифицированные роли]**.

FMT_MTD.2.2 ФБО должны предпринять следующие действия при достижении или превышении данными ФБО установленных выше ограничений: **[назначение: список действий, направленных на предотвращение попыток аутентификации]**.

Зависимости: FMT_MTD.1 «Управление данными ФБО»,
FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с **пользователями ОО, администраторами ОО и объектами**, в пределах ОДФ только [уполномоченному администратору ОО].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

- а) отмена полномочий у пользователей ОО и администраторов ОО на доступ к объектам должна вступать в силу при следующем сеансе работы пользователя ОО и администратора ОО;
- б) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;
- в) [**назначение: другие правила отмены**]

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с **объектами**, в пределах ОДФ только [назначение: **пользователи, уполномоченные на изменение атрибутов безопасности в соответствии с политикой дискреционного управления доступом**].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

- а) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;

б) [**назначение:** *другие правила отмены*]

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_SAE.1 Ограниченная по времени авторизация

FMT_SAE.1.1 ФБО должны **предоставлять** возможность назначать срок действия для [аутентификационных данных] только [**назначение:** *уполномоченные идентифицированные роли*].

FMT_SAE.1.2 Для каждого из этих атрибутов безопасности ФБО должны быть способны к [блокированию ассоциированной с пользователем учетной записи] по истечении ее срока действия.

Зависимости: FMT_SMR.1 «Роли безопасности»,
FPT_STM.1 «Надежные метки времени».

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

[

а) администратор ОО;

б) пользователь ОО;

в) [**назначение:** *другие уполномоченные идентифицированные роли*]

].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать **субъектов доступа** с ролями.

Зависимости: FIA_UID.2 «Выбор момента идентификации».

Б 5.1.1.5 Защита ФБО (FPT)

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ при первоначальном запуске, периодически во время нормального

функционирования, по запросу уполномоченного администратора ОО

для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая **является базовой для ФБО.**

Зависимости: отсутствуют.

FPT_RCV.1 Ручное восстановление

FPT_RCV.1.1 После сбоя или прерывания обслуживания ФБО должны перейти в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию.

Зависимости: FPT_TST.1 «Тестирование ФБО»,
AGD_ADM.1 «Руководство администратора».

FPT_RVM.1 Невозможность обхода ПБО

FPT_RVM.1.1 ФБО должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 Отделение домена ФБО

FPT_SEP.1.1 ФБО должны поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 ФБО должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 ФБО должны быть способны предоставлять надежные метки времени для собственного использования.

Зависимости: отсутствуют.

FPT_TST.1 Тестирование ФБО

FPT_TST.1.1 ФБО должны выполнять пакет программ самотестирования при запуске и периодически в процессе нормального функционирования для демонстрации правильного выполнения ФБО.

FPT_TST.1.2 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность данных ФБО.

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

Зависимости: FPT_AMT.1 «Тестирование абстрактной машины».

Б 5.1.1.6 Доступ к ОО (FTA)

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

FTA_SSL.1.1 ФБО должны блокировать интерактивный сеанс после [истечения интервала времени бездействия пользователя ОО или администратора ОО], для чего предпринимаются следующие действия:

- а) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;
- б) блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса.

FTA_SSL.1.2 ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [повторная аутентификация пользователя ОО или администратора ОО].

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

FTA_SSL.2 Блокирование, инициированное пользователем

FTA_SSL.2.1 ФБО должны допускать инициированное пользователем **ОО или администратором ОО** блокирование своего собственного

интерактивного сеанса, для чего предпринимаются следующие действия:

- а) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;
- б) блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса.

FTA_SSL.2.2 ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [повторная аутентификация пользователя ОО или администратора ОО].

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

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса, основываясь на **следующем**:

- [
- а) идентификатор пользователя;
 - б) [**назначение:** *другие атрибуты*]
-].

Зависимости: отсутствуют.

Б 5.1.1.7 Доверенный маршрут/канал (FTP)

FTP_TRP.1 Доверенный маршрут

FTP_TRP.1.1 ФБО должны предоставлять маршрут связи между собой и локальным пользователем **ОО** или **администратором ОО**, который логически отличим от других маршрутов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту передаваемых данных от модификации или раскрытия.

FTP_TRP.1.2 ФБО должны позволить локальным пользователям ОО или администраторам ОО инициировать связь через доверенный маршрут.

FTP_TRP.1.3 ФБО должны требовать использования доверенного маршрута для начальной аутентификации пользователя **ОО** или администратора **ОО** [и разблокирования сеанса].

Зависимости: отсутствуют.

Б 5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 РД БИТ и образуют ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий» (см. таблицу 5.5).

Таблица 5.5 – Требования доверия к безопасности ОО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Управление конфигурацией	ACM_AUT.1	Частичная автоматизация УК
	ACM_CAP.4	Поддержка генерации, процедуры приемки
	ACM_SCP. 2	Охват УК отслеживания проблем
Поставка и эксплуатация	ADO_DEL.2	Обнаружение модификации
	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP. 2	Полностью определенные внешние интерфейсы
	ADV_HLD. 2	Детализация вопросов безопасности в проекте верхнего уровня
	ADV_IMP.1	Подмножество реализации ФБО
	ADV_LLD.1	Описательный проект нижнего уровня
	ADV_RCR. 1	Неформальная демонстрация соответствия
	ADV_SPM. 1	Неформальная модель политики безопасности ОО
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Поддержка жизненного цикла	ALC_DVS.1	Идентификация мер безопасности
	ALC_FLR. 1	Базовое устранение недостатков
	ALC_LCD. 1	Определение модели жизненного цикла разработчиком
	ALC_TAT. 1	Полностью определенные инструментальные средства разработки
Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.1	Тестирование: проект верхнего уровня
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_MSU.2	Подтверждение правильности анализа
	AVA_SOF.1	Оценка стойкости функции безопасности ОО
	AVA_VLA. 3	Умеренно стойкий

Б 5.1.3 Управление конфигурацией (АСМ)

АСМ_AUT.1 Частичная автоматизация УК

Элементы действий разработчика

АСМ_AUT.1.1D Разработчик должен использовать систему УК.

АСМ_AUT.1.2D Разработчик должен представить план УК.

Элементы содержания и представления свидетельств

АСМ_AUT.1.1C Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО производятся только санкционированные изменения.

АСМ_AUT.1.2C Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.

АСМ_AUT.1.3C План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.

АСМ_AUT.1.4С План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.

Элементы действий оценщика

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

АСМ_CAP.4 Поддержка генерации, процедуры приемки

Элементы действий разработчика

АСМ_CAP.4.1D Разработчик должен предоставить маркировку для ОО.

АСМ_CAP.4.2D Разработчик должен использовать систему УК.

АСМ_CAP.4.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

АСМ_CAP.4.1С Маркировка ОО должна быть уникальна для каждой версии ОО.

АСМ_CAP.4.2С ОО должен быть помечен маркировкой.

АСМ_CAP.4.3С Документация УК должна включать в себя список конфигурации, план УК и план приемки.

АСМ_CAP.4.4С Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

АСМ_CAP.4.5С Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

АСМ_CAP.4.6С Система УК должна уникально идентифицировать все элементы конфигурации.

АСМ_CAP.4.7С План УК должен содержать описание, как используется система УК.

АСМ_CAP.4.8С Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

АСМ_CAP.4.9С Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

АСМ_САР.4.10С Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

АСМ_САР.4.11С Система УК должна поддерживать генерацию ОО.

АСМ_САР.4.12С План приемки должен содержать описание процедур, используемых для приемки модифицированного или вновь созданного элемента конфигурации как части ОО.

Элементы действий оценщика

АСМ_САР.4.1Е Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АСМ_SCP.2 Охват УК отслеживания проблем

Элементы действий разработчика

АСМ_SCP.3.1D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

АСМ_SCP.2.1С Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора, документацию УК **и недостатки безопасности.**

АСМ_SCP.2.2С Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.

Элементы действий оценщика

АСМ_SCP.2.1Е Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

Б 5.1.4 Поставка и эксплуатация (ADO)

ADO_DEL.2 Обнаружение модификации

Элементы действий разработчика

ADO_DEL.2.1D Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

ADO_DEL.2.2 Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ADO_DEL.2.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий к местам использования.

ADO_DEL.2.2C Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.

ADO_DEL.2.3C Документация поставки должна содержать описание, как различные процедуры позволяют обнаружить попытку подмены от имени разработчика, даже в тех случаях, когда разработчик ничего не отсылал к месту использования.

Элементы действий оценщика

ADO_DEL.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

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

Б 5.1.5 Разработка (ADV)

ADV_FSP.2 Полностью определенные внешние интерфейсы

Элементы действий разработчика

ADV_FSP.2.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.2.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.2.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.2.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая **полную** детализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.2.4C Функциональная спецификация должна полностью представить ФБО.

ADV_FSP.2.5C Функциональная спецификация должна включать в себя логическое обоснование, что ФБО полностью представлены.

Элементы действий оценщика

ADV_FSP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.2.2E Оценщик должен сделать независимое заключение, что функциональная спецификация - точное и полное отображение функциональных требований безопасности ОО.

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

Элементы действий разработчика

ADV_HLD.3.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.2.1C Представление проекта верхнего уровня должно быть неформальным.

ADV_HLD.2.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.2.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.2.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.2.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.2.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.2.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.2.8C Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_HLD.2.9C Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

Элементы действий оценщика

ADV_HLD.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.2.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня - точное и полное отображение функциональных требований безопасности ОО.

ADV_IMP.1 Подмножество реализации ФБО

Элементы действий разработчика

ADV_IMP.1.1D Разработчик должен обеспечить представление реализации для выбранного подмножества ФБО.

Элементы содержания и представления свидетельств

ADV_IMP.1.1C Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.

ADV_IMP.1.2C Представление реализации должно быть внутренне непротиворечивым.

Элементы действий оценщика

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

ADV_IMP.1.2E Оценщик должен сделать независимое заключение, что наименее абстрактное представление ФБО – точное и полное отображение функциональных требований безопасности ОО.

ADV_LLD.1 Описательный проект нижнего уровня

Элементы действий разработчика

ADV_LLD.1.1D Разработчик должен представить проект нижнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_LLD.1.1C Представление проекта нижнего уровня должно быть неформальным.

ADV_LLD.1.2C Проект нижнего уровня должен быть внутренне непротиворечивым.

ADV_LLD.1.3C Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

ADV_LLD.1.4C Проект нижнего уровня должен содержать описание назначения каждого модуля.

ADV_LLD.1.5C Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

ADV_LLD.1.6C Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.

ADV_LLD.1.7C Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

ADV_LLD.1.8C Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

ADV_LLD.1.9C Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя, при необходимости, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_LLD.1.10C Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

Элементы действий оценщика

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

ADV_LLD.1.2E Оценщик должен сделать независимое заключение, что проект нижнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

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

ADV_SPM.1 Неформальная модель политики безопасности ОО

Элементы действий разработчика

ADV_SPM.1.1D Разработчик должен представить модель ПБО.

ADV_SPM.1.2D Разработчик должен демонстрировать или доказать, где это требуется, соответствие между функциональной спецификацией и моделью ПБО.

Элементы содержания и представления свидетельств

ADV_SPM.1.1C Модель ПБО должна быть неформальной.

ADV_SPM.1.2C Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.1.3C Модель ПБО должна включать в себя логическое обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.1.4C Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.

Элементы действий оценщика

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

Б 5.1.6 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

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

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

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

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

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

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

Элементы действий оценщика

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

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

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

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

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

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

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

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

Элементы действий оценщика

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

Б 5.1.7 Поддержка жизненного цикла (ALC)

ALC_DVS.1 Идентификация мер безопасности

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

ALC_DVS.1.2C Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.

Элементы действий оценщика

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

ALC_DVS.1.2E Оценщик должен подтвердить применение мер безопасности.

ALC_FLR.1 Базовое устранение недостатков

Элементы действий разработчика

ALC_FLR.1.1D Разработчик должен задокументировать процедуры устранения недостатков.

Элементы содержания и представления свидетельств

ALC_FLR.1.1C Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждой редакции ОО.

ALC_FLR.1.2C Процедуры устранения недостатков должны содержать требование представления описания природы и проявлений каждого недостатка безопасности, а также статуса завершения исправления этого недостатка.

ALC_FLR.1.3C Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

ALC_FLR.1.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

Элементы действий оценщика

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

ALC_LCD.1 Определение модели жизненного цикла разработчиком

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 свидетельств

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

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

Элементы действий оценщика

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

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Элементы действий разработчика

ALC_TAT.1.1D Разработчик должен идентифицировать инструментальные средства разработки ОО.

ALC_TAT.1.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.

Элементы содержания и представления свидетельств

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

ALC_TAT.1.2C Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

ALC_TAT.1.3C Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.

Элементы действий оценщика

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

Б 5.1.8 Тестирование (ATE)

ATE_COV.2 Анализ покрытия

Элементы действий разработчика

ATE_COV.2.1D Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

ATE_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

ATE_COV.2.2C Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.

Элементы действий оценщика

ATE_COV.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_DPT.1 Тестирование: проект верхнего уровня

Элементы действий разработчика

ATE_DPT.1.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE_DPT.1.1C Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня.

Элементы действий оценщика

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

ATE_FUN.1 Функциональное тестирование

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 свидетельств

ATE_FUN.1.1C Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.

ATE_FUN.1.2C Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей тестирования.

ATE_FUN.1.3C Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.

ATE_FUN.1.4C Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.

ATE_FUN.1.5C Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.

Элементы действий оценщика

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

ATE_IND.2 Выборочное независимое тестирование

Элементы действий разработчика

ATE_IND.2.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

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 представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.2.2E Оценщик должен протестировать подмножество ФБО, **как необходимо**, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

ATE_IND.2.3E Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

Б 5.1.9 Оценка уязвимостей (AVA)

AVA_MSU.2 Подтверждение правильности анализа

Элементы действий разработчика

AVA_MSU.2.1D Разработчик должен представить руководства по применению ОО.

AVA_MSU.2.2D Разработчик должен задокументировать анализ руководств.

Элементы содержания и представления свидетельств

AVA_MSU.2.1C Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.2.2C Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

AVA_MSU.2.3C Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.2.4C Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

AVA_MSU.2.5C Документация анализа должна демонстрировать, что руководства полны.

Элементы действий оценщика

AVA_MSU.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_MSU.2.2E Оценщик должен повторить все процедуры конфигурирования и установки и выборочно другие процедуры для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

AVA_MSU.2.3E Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

AVA_MSU.2.4E Оценщик должен подтвердить, что документация анализа показывает обеспечение руководствами безопасного функционирования во всех режимах эксплуатации ОО.

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

Элементы действий оценщика

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

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

AVA_VLA.3 Умеренно стойкий

Элементы действий разработчика

AVA_VLA.3.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску путей, которыми пользователь может нарушить ПБО.

AVA_VLA.3.2D Разработчик должен задокументировать местоположение идентифицированных уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.3.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.3.2C Документация должна содержать строгое обоснование, что ОО с идентифицированными уязвимостями является стойким к явным нападениям проникновения.

AVA_VLA.3.3C Свидетельство должно показать, что поиск уязвимостей является систематическим.

Элементы действий оценщика

AVA_VLA.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_VLA.3.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.

AVA_VLA.3.3E Оценщик должен выполнить независимый анализ уязвимостей.

AVA_VLA.3.4E Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.

AVA_VLA.3.5E Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим **умеренным** потенциалом нападения.

Б 6 ОБОСНОВАНИЕ

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

Б 6.1 Обоснование целей безопасности

Б 6.1.1 Обоснование целей безопасности для ОО

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

Таблица 6.1 – Отображение целей безопасности на угрозы и политику безопасности объекта эксплуатации

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10	Цель безопасности-11
Угроза-1	X										
Угроза-2	X										
Угроза-3		X									
Угроза-4		X									
Угроза-5				X							
Угроза-6				X							
Угроза-7							X				
Угроза-8		X									
Угроза-9									X		
Политика безопасности-1						X					
Политика безопасности-2			X								
Политика безопасности-3	X										
Политика безопасности-4								X			
Политика безопасности-5					X						
Политика безопасности-6										X	
Политика безопасности-7											X

Цель безопасности-1

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1**, **Угроза-2** и реализацией политики безопасности организации **Политика безопасности-3**, так как обеспечивает доступ к защищаемым активам только уполномоченным на это пользователям ОО и администраторам ОО, а также обеспечивает возможность уполномоченным пользователям ОО ограничивать права доступа к защищаемым активам для других пользователей ОО и администраторов ОО.

Цель безопасности-2

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-3**, **Угроза-4** и **Угроза-8**, так как обеспечивает доступ к ОО только уполномоченным на это пользователям ОО и администраторам ОО, а также блокирование сеанса пользователя ОО и администратора ОО, осуществляемое по их инициативе, а также инициируемое ФБО и основанное на интервале времени бездействия пользователя ОО или администратора ОО.

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-2**, так как обеспечивает наличие надлежащих механизмов регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации предоставляют администраторам ОО возможность выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-5** и **Угроза-6**, так как обеспечивает доступ к данным аудита только

уполномоченным администраторам ОО и предотвращает потерю данных аудита в случае переполнения их хранилища.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-5**, так как обеспечивает недоступность информационного содержания освобождаемой памяти, выделяемой процессам.

Цель безопасности-6

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-1**, так как обеспечивает наличие надлежащих корректно функционирующих средств администрирования ОО, управляемых клиентских и серверных ОС, доступных только уполномоченным администраторам ОО, а также возможность модификации собственных аутентификационных данных уполномоченными пользователями ОО.

Цель безопасности-7

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-7**, так как обеспечивает защиту данных ФБО, поддерживая домен для функционирования ФБО.

Цель безопасности-8

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-4**, так как обеспечивает невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

Цель безопасности-9

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-9**, так как обеспечивает возможность безопасного восстановления ОО после сбоя и отказов программного обеспечения и оборудования ОО.

Цель безопасности-10

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-6**, так как обеспечивает возможность периодического контроля целостности ФБО и его данных, а также возможность собственного регламентного тестирования и тестирования среды функционирования ОО на предмет корректности функционирования.

Цель безопасности-11

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-7**, так как обеспечивает наличие механизма аутентификации, обеспечивающего адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения

Б 6.1.2 Обоснование целей безопасности для среды

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

Таблица 6.2 – Отображение целей безопасности для среды на предположения безопасности

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-6	Цель для среды функционирования ОО-7	Цель для среды функционирования ОО-8
Предположение-1								
Предположение-2		X						
Предположение-3			X					
Предположение-4							X	
Предположение-5								X
Предположение-6				X				
Предположение-7					X			
Предположение-8						X		

Цель для среды функционирования ОО-1

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-1**, так как обеспечивает отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Цель для среды функционирования ОО-2

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-2**, так как обеспечивает осуществление доступа к ОО только из санкционированных точек доступа,

размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-3

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-3**, так как обеспечивает установку конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-6**, так как обеспечивает исключение возможности несанкционированного физического доступа к компьютеру с установленным ОО.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-7**, так как обеспечивает, что персонал, ответственный за администрирование ОО, является благонадежным и компетентным, и руководствуется в своей деятельности соответствующей документацией.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-8**, так как обеспечивает, что уполномоченные на доступ к ОО пользователи являются благонадежными, руководствуются в своей работе эксплуатационной документацией на ОО, а их совместные действия направлены исключительно на выполнение своих функциональных обязанностей.

Цель для среды функционирования ОО-7

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-4**, так как обеспечивает выполнение загрузки ОО в доверенной среде, предотвращающей несанкционированное прерывание процесса загрузки ОО и использование инструментальных средств, позволяющих осуществить доступ к защищаемым активам ОО в обход механизмов защиты.

Цель для среды функционирования ОО-8

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-5**, так как для предотвращения несанкционированного доступа к системным компонентам ОО обеспечивает исключение возможности запуска встроенных программ отладки.

Б 6.2 Обоснование требований безопасности

Б 6.2.1 Обоснование требований безопасности для ОО

Б 6.2.1.1 Обоснование функциональных требований безопасности ОО

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

Таблица 6.3 – Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10	Цель безопасности-11
FAU_GEN.1			X								
FAU_GEN.2			X								
FAU_SAR.1			X								
FAU_SAR.2			X								
FAU_SAR.3			X								
FAU_SEL.1			X								
FAU_STG.1				X							
FAU_STG.3				X							
FAU_STG.4				X							
FDP_ACC.1	X										
FDP_ACF.1	X										
FDP_RIP.1					X						
FIA_AFL.1		X									X
FIA_ATD.1	X	X	X			X					
FIA_SOS.1											X
FIA_UAU.2	X	X									
FIA_UAU.7		X									
FIA_UID.2	X	X									
FIA_USB.1 (EXT)	X	X	X								
FMT_MOF.1						X					
FMT_MSA.1	X					X					
FMT_MSA.3	X					X					
FMT_MTD.1						X					
FMT_MTD.2						X					
FMT_REV.1 (1)						X					

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10	Цель безопасности-11
FMT_REV.1 (2)	X										
FMT_SAE.1						X					
FMT_SMR.1	X			X		X	X				
FPT_AMT.1										X	
FPT_RCV.1									X		
FPT_RVM.1							X				
FPT_SEP.1							X				
FPT_STM.1			X			X					
FPT_TST.1										X	
FTA_SSL.1		X									
FTA_SSL.2		X									
FTA_TSE.1		X									
FTP_TRP.1								X			

FAU_GEN.1

Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_GEN.2

Ассоциация идентификатора пользователя

Выполнение требований данного компонента обеспечивает возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором учетной записи пользователя или идентификатором регистрационной записи пользователя, который был инициатором этого события.

Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления уполномоченному администратору ОО всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает запрет всем пользователям доступ к чтению записей аудита, за исключением уполномоченных администраторов ОО, которым явно предоставлен доступ для чтения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает выполнение поиска и сортировки данных аудита, основанных на определенных критериях (идентификатор пользователя). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SEL.1 Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, уполномоченным администратором ОО по определенным атрибутам (идентификатор пользователя). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_STG.1**Защищенное хранение журнала аудита**

Выполнение требований данного компонента обеспечивает защиту хранимых записей аудита от несанкционированного удаления и предотвращает модификацию записей аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_STG.3**Действия в случае возможной потери данных аудита**

Выполнение требований данного компонента обеспечивает выполнение действий, направленных на сохранение данных журнала аудита и обеспечивающих непрерывность процесса аудита, если журнал аудита превысит определенный уполномоченным администратором ОО размер. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_STG.4**Предотвращение потери данных аудита**

Выполнение требований данного компонента обеспечивает предотвращение событий, подвергающихся аудиту, и выполнение других действий, направленных на невозможность совершения дальнейших событий, связанных с безопасностью ОО, при переполнении журнала аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FDP_ACC.1**Ограниченное управление доступом**

Выполнение требований данного компонента обеспечивает реализацию политики дискреционного доступа для субъектов, именованных объектов и всех операций между субъектами и объектами. 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 осуществление политики дискреционного доступа, основываясь на атрибутах безопасности, определении правил доступа субъектов к объектам. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FDP_RIP.1 Ограниченная защита остаточной информации

Выполнение требований данного компонента обеспечивает недоступность любого предыдущего информационного содержания памяти при ее освобождении процессами. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** 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 ОО. При достижении определенного администратором ОО числа неуспешных попыток аутентификации некоторого лица, ОО предпринимаются действия, направленные на дальнейшее предотвращение попыток доступа со стороны данного лица, ограниченное временным интервалом. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2, Цель безопасности-11** и способствует их достижению.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя (пользователя ОО и администратора ОО) ряда атрибутов безопасности (идентификатора пользователя, принадлежность к группе). Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3, Цель безопасности-6** и способствует их 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-11** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2** и способствует их достижению.

FIA_UAU.7 Аутентификация с защищенной обратной связью

Выполнение требований данного компонента обеспечивает, что во время выполнения аутентификации вводимый пользователем пароль отображается в скрытом виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение идентификации субъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1, Цель безопасности-2** и способствует их достижению.

FIA_USB.1 (EXT) Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами, действующими от имени этого субъекта доступа. Рассматриваемый компонент

сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3** и способствует их достижению.

FMT_MOF.1 Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает определенные действия над функциями из числа ФБО только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только уполномоченным ролям. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-6** и способствует их достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом, и возможность для уполномоченных ролей определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-6** и способствует их достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность осуществлять определенные операции над данными ФБО только уполномоченным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует их достижению.

FMT_MTD.2

Управление ограничениями данных ФБО

Выполнение требований данного компонента предоставляет возможность определения ограничений для порогового значения количества неуспешных попыток аутентификации только уполномоченной роли. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует их достижению.

FMT_REV.1 (1) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО, в пределах ОДФ только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FMT_REV.1 (2) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с объектами, в пределах ОДФ только пользователю ОО, уполномоченному согласно политике дискреционного управления доступом модифицировать атрибуты безопасности объекта. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_SAE.1

Ограниченная по времени авторизация

Выполнение требований данного компонента предоставляет возможность назначать срок действия для аутентификационных данных только уполномоченным ролям. По истечении срока действия аутентификационных данных ФБО осуществляют блокирование ассоциированной с пользователем учетной записи. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FMT_SMR.1

Роли безопасности

Данный компонент включен в ПЗ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту ролей администратора ОО и пользователя ОО, а также других возможных ролей. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-4, Цель безопасности-6, Цель безопасности-7** и способствует их достижению.

FPT_AMT.1 Тестирование абстрактной машины

Данный компонент включен в ПЗ, для того, чтобы учесть зависимости выполнения требований компонента FPT_TST.1. Выполнение требований данного компонента обеспечивает тестирование правильности выполнения предположений безопасности, представленных базовой абстрактной машиной, при первоначальном запуске, периодически и по запросу уполномоченного администратора ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-10** и способствует ее достижению.

FPT_RCV.1 Ручное восстановление

Выполнение требований данного компонента обеспечивает переход ФБО в режим аварийной поддержки для последующего возврата ОО в безопасное состояние после сбоя или прерывания обслуживания. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-9** и способствует ее достижению.

FPT_RVM.1 Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FPT_SEP.1 Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ПЗ, для того, чтобы учесть зависимости выполнения требований компонента FAU_GEN.1 от наличия в записях аудита точного указания даты и времени и для учета зависимости выполнения требований компонента FMT_SAE.1 от наличия времени для определения срока действия аутентификационных данных. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-3, Цель безопасности-6** и способствует их достижению.

FPT_TST.1 Тестирование ФБО

Выполнение требований данного компонента обеспечивает целостность выполнения ФБО и предоставляет администратору ОО средства верификации целостности кода и данных ФБО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-10** и способствует ее достижению.

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

Выполнение требований данного компонента обеспечивает блокирование сеанса пользователя ОО или администратора ОО после истечения интервала времени бездействия. Определяются действия, необходимые для разблокирования. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FTA_SSL.2

Блокирование, инициированное пользователем

Выполнение требований данного компонента обеспечивает блокирование сеанса, инициированное пользователем ОО или администратором ОО. Определяются действия, необходимые для разблокирования. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FTA_TSE.1

Открытие сеанса с ОО

Выполнение требований данного компонента обеспечивает способность отказа ОО в открытии сеанса доступа к ОО, основываясь на идентификаторе пользователя, а также других атрибутах. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FTP_TRP.1

Доверенный маршрут

Выполнение требований данного компонента обеспечивает установление доверенной связи между ФБО и локальным пользователем ОО или администратором ОО для целей начальной аутентификации и разблокирования сеанса. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-8** и способствует ее достижению.

Б 6.2.1.2 Обоснование требований доверия к безопасности ОО

Включение в настоящий ПЗ ОУД4, усиленный компонентом ALC_FLR.1 «Базовое устранение недостатков» AVA_VLA.3 «Умеренно стойкий», является достаточным при определении допустимости использования ОО в информационных системах, в которых обрабатывается информация ограниченного доступа.

Б 6.2.2 Обоснование зависимостей требований

В таблице 6.4 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворены

в настоящем ПЗ либо включением компонентов, определенных в части 2 РД БИТ под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в части 2 РД БИТ под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 6.4 является справочным и содержит компоненты, определенные в части 2 РД БИТ в описании компонентов требований, приведенных в столбце 1 таблицы 6.4, под рубрикой «Зависимости».

Столбец 3 таблицы 6.4 показывает, какие компоненты требований были реально включены в настоящий ПЗ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 6.4. Компоненты требований в столбце 3 таблицы 6.4 либо совпадают с компонентами в столбце 2 таблицы 6.4, либо иерархичны по отношению к ним.

Таблица 6.4 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по РД БИТ	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.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.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
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2

Функциональные компоненты	Зависимости по РД БИТ	Удовлетворение зависимостей
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_USB.1 (EXT)	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1 (1)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	FMT_MTD.1, FMT_SMR.1
FMT_REV.1 (1)	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_SAE.1	FMT_SMR.1, FPT_STM.1	FMT_SMR.1, FPT_STM.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RCV.1	FPT_TST.1, AGD_ADM.1, ADV_SPM.1	FPT_TST.1, AGD_ADM.1, <i>обосновано невключение ADV_SPM.1</i>
FPT_TST.1	FPT_AMT.1	FPT_AMT.1
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2
FTA_SSL.2	FIA_UAU.1	FIA_UAU.2

ПРИЛОЖЕНИЕ В

(обязательное)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИЗДЕЛИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ СИСТЕМА ПУБЛИЧНОГО ДОСТУПА К ОБЩЕСИСТЕМНЫМ И ПРИКЛАДНЫМ КОМПОНЕНТАМ ПРОГРАММНОЙ ПЛАТФОРМЫ, СОДЕРЖАЩИМСЯ В ФОНДЕ АЛГОРИТМОВ И ПРОГРАММ

Профиль защиты

ИЗД_ИТ.РПЗТ.Оуд4.ПЗ

Версия 1.0

СОДЕРЖАНИЕ

В 1	Введение ПЗ	129
В 1.1	Идентификация ПЗ.....	129
В 1.2	Аннотация ПЗ	131
В 1.3	Соглашения.....	131
В 1.4	Термины и определения.....	132
В 1.5	Организация ПЗ	134
В 2	Описание ОО	136
В 2.1	Тип изделия ИТ	136
В 2.2	Основные функциональные возможности ОО	137
В 3	Среда безопасности ОО	141
В 3.1	Предположения безопасности	141
В 3.2	Угрозы.....	142
В 3.3	Политика безопасности объекта эксплуатации	147
В 4	Цели безопасности	149
В 4.1	Цели безопасности для ОО	149
В 4.2	Цели безопасности для среды.....	151
В 5	Требования безопасности ИТ	153
В 5.1	Требования безопасности для ОО	153
В 6	Обоснование	194
В 6.1	Обоснование целей безопасности	194
В 6.2	Обоснование требований безопасности.....	200

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БИТ	– безопасность информационных технологий
ЗБ	– задание по безопасности
ИС	– информационная система
ИТ	– информационная технология
НСД	– несанкционированный доступ
ОДФ	– область действия функции безопасности объекта оценки
ОО	– объект оценки
ОУД	– оценочный уровень доверия
ПБО	– политика безопасности объекта оценки
ПЗ	– профиль защиты
ПФБ	– политика функции безопасности
УК	– управление конфигурацией
ФБО	– функции безопасности объекта оценки
ФТБ	– функциональные требования безопасности

В 1 ВВЕДЕНИЕ ПЗ

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

В 1.1 Идентификация ПЗ

Название ПЗ: Безопасность информационных технологий. Изделия информационных технологий. Система публичного доступа к общесистемным и прикладным компонентам программной платформы, содержащимся в фонде алгоритмов и программ. Профиль защиты.

Семейство ПЗ: Изделия ИТ.

Функциональная группа: Система публичного доступа к общесистемным и прикладным компонентам национальной программной платформы, содержащимся в фонде алгоритмов и программ.

Версия ПЗ: Версия 1.0.

Обозначение ПЗ: ИЗД_ИТ.РПЗТ.ОУД4.ПЗ.

Идентификация Система публичного доступа к общесистемным и

<i>я ОО:</i>	прикладным компонентам национальной программной платформы, содержащимся в фонде алгоритмов и программ.
<i>Уровень доверия:</i>	ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий».
<i>Идентификация РД БИТ:</i>	Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель, ФСТЭК (Гостехкомиссия) России, 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, ФСТЭК (Гостехкомиссия) России, 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, ФСТЭК (Гостехкомиссия) России, 2002.
<i>Ключевые слова:</i>	Система публичного доступа к общесистемным и прикладным компонентам национальной программной платформы, содержащимся в фонде алгоритмов и программ, репозиторий, средство защиты информации, дискреционное управление доступом, профиль защиты, ОУД4.

В 1.2 Аннотация ПЗ

Настоящий ПЗ определяет требования безопасности для Системы публичного доступа к общесистемным и прикладным компонентам национальной программной платформы, содержащимся в фонде алгоритмов и программ (далее – объект оценки).

В 1.3 Соглашения

Руководящий документ ФСТЭК (Гостехкомиссии) России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (далее – РД БИТ) допускает выполнение определенных в части 2 РД БИТ операций над функциональными требованиями. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор», «назначение» и «итерация».

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

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

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

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

В настоящем ПЗ используются компоненты функциональных требований безопасности, включающие незавершенные операции **«назначение»** в которых область предполагаемых значений уточнена по отношению к исходному компоненту из части 2 РД БИТ. В данных компонентах операции **«назначения»** с

уточненной областью предполагаемых значений обозначаются как [назначение: *уточненная область предполагаемых значений*].

Операция «**итерация**» используется для более чем однократного использования компонента функциональных требований безопасности ИТ при различном выполнении разрешенных операций (уточнение, выбор, назначение). Выполнение «итерации» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

Замечания по применению предназначены либо для разъяснения назначения некоторого требования, идентификации вариантов реализации, либо для определения условий выполнения требования. В случае использования, замечания по применению следуют за компонентом требования.

Настоящий профиль защиты содержит ряд незавершенных операций над компонентами функциональных требований безопасности. Эти операции должны быть завершены в задании по безопасности на конкретную реализацию Системы публичного доступа к общесистемным и прикладным компонентам национальной программной платформы, содержащимся в фонде алгоритмов и программ.

В 1.4 Термины и определения

В настоящем ПЗ применяются следующие термины с соответствующими определениями.

Активы: Информация и ресурсы, подлежащие защите.

Аутентификационные данные: информация, используемая для верификации предъявленного идентификатора.

Аутентификация: Процесс установления подлинности информации, предъявленной администратором безопасности и пользователем ИС при регистрации.

Данные ФБО: Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО.

Доступность: Состояние безопасности активов (информации),

характеризуемое их готовностью к использованию по запросу уполномоченных лиц, объектов или субъектов, а также возможностью их восстановления в случае сбоя (отказа).

Задание по безопасности: Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного изделия ИТ.

Конфиденциальность: Состояние безопасности активов (информации), характеризующее их защищенностью от несанкционированного доступа и/или раскрытия их содержания неуполномоченным лицам, объектам или процессам.

Область действия ФБО: Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО.

Объект оценки: подлежащее оценке изделие ИТ с документацией.

Политика безопасности объекта эксплуатации: Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

Политика безопасности ОО: Совокупность правил, определяющих режим обеспечения безопасности ОО и представляемых в виде набора функциональных требований безопасности.

Политика функции безопасности: Политика безопасности, осуществляемая ФБ.

Пользователь: Любая сущность (человек-пользователь или внешний объект изделия ИТ) вне ОО, которая взаимодействует с ОО.

Изделие ИТ: Программное, программно-аппаратное или аппаратное обеспечение изделий ИТ, специально разработанное для использования в составе ИС

Профиль защиты: Совокупность требований безопасности для некоторого типа изделий ИТ.

Репозиторий: Место хранения и поддержки данных. Чаще всего

данные в репозитории хранятся в виде файлов, доступных для дальнейшего распространения по сети.

Уполномоченный администратор: Уполномоченный пользователь, ответственный за эксплуатацию ОО.

Функция безопасности: Функциональные возможности части или частей изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных функциональных требований безопасности.

Целостность: Состояние безопасности активов (информации), характеризующее их полнотой и защищенностью от несанкционированного изменения (модификации).

В 1.5 Организация ПЗ

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

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

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

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

В разделе 5 «Требования безопасности ИТ» на основе частей 2 и 3 РД БИТ определены, соответственно, функциональные требования безопасности ИТ и требования доверия к безопасности ОО.

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

В 2 ОПИСАНИЕ ОО

Объектом оценки в настоящем ПЗ является система публичного доступа к общесистемным и прикладным компонентам национальной программной платформы, содержащимся в фонде алгоритмов и программ.

Назначение Объекта оценки - доставка общесистемных и прикладных компонентов национальной программной платформы на компьютер пользователя.

В 2.1 Тип изделия ИТ

Объект оценки представляет собой систему публичного доступа к общесистемным и прикладным компонентам национальной программной платформы, содержащимся в фонде алгоритмов и программ общего назначения (репозиторию). Репозиторий - место хранения общесистемных и прикладных компонент национальной программной платформы, в виде файлов, доступных для дальнейшего распространения, а также метаданных об указанных компонентах (наименование, описание назначения, номер версии, разработчик, сведения о классификации и категоризации компоненты, перечни зависимых компонент и др.).

Объекту оценки может обеспечивать ограничение доступа к репозиторию, например, может использоваться отдельный репозиторий для организации тестирования новых версий общесистемных и прикладных компонент национальной программной платформы, доступ к которому будет предоставлен ограниченному кругу лиц.

Объект оценки может быть размещен на специализированном сервере, доступ к которым осуществляется через сети общего доступа, на сервере в ЛВС объекта. Репозиторий может размещаться на отдельном сервере, а также на съемном носителе информации. В целях обеспечения доступности общесистемных и прикладных компонент национальной программной платформы, хранящихся в репозитории, копии репозитория могут размещаться на дополнительных (дублирующих, зеркальных) серверах.

В 2.2 Основные функциональные возможности ОО

В ОО должен быть реализован ряд функциональных возможностей и средств, позволяющих обеспечить безопасность ИТ, надежность ОО, а также упрощающих администрирование ОО и управление ОО. В данном подразделе представлено краткое описание предполагаемых функциональных возможностей и средств.

Объект оценки должен содержать следующие компоненты:

- Web-сервер публичного доступа;
- средство интеграции с операционной системой;
- средство интеграции с эталонной средой разработки, сборки обновления операционной системы;
- средство работы со статистикой загрузки решений пользователями;
- средство обеспечения масштабирования системы;
- средство создания репозитория ограниченного доступа;
- средства идентификации, аутентификации и авторизации пользователей репозитория ограниченного доступа.

В 2.2.1 Основные функциональные возможности

В ОО должны быть включены средства, позволяющие защитить выбранные файлы, приложения и ресурсы. В число таких средств входят списки управления доступом, группы безопасности и механизмы централизованного управления параметрами безопасности, а также инструменты, позволяющие настраивать эти средства и управлять ими.

Доступ к функциям добавления, модификации и удаления компонент хранящихся в репозитории должен предоставляться только ограниченному кругу лиц, в том числе с использованием усиленных мер по защите информации: запрет удаленного доступа для выполнения функций, использование надежных средств идентификации и аутентификации и др.

ОО должен поддерживать следующий функционал:

- обеспечивать web-доступ пользователей к каталогу общесистемных и прикладных решений;

- обеспечивать классификацию и категоризацию общесистемных и прикладных решений;
- обеспечивать простой интуитивно-понятный способ установки требуемого решения на компьютер пользователя;
- обеспечивать подсчет статистики установки решений на компьютеры пользователей;
- обеспечивать информирование пользователя о наличии обновлений к используемым им решениям и степени их критичности для установки;
- обеспечивать возможность как ручного обновления отдельных программ, так и автоматического обновления операционной системы и всех установленных на ней программ с автоматическим разрешением зависимостей обновлений;
- обеспечивать возможность создания как публичных репозиториев программного обеспечения, так и репозиториев ограниченного доступа;
- обеспечивать возможность идентификации, аутентификации и авторизации пользователей репозиториев ограниченного доступа;
- иметь возможность горизонтального масштабирования путем увеличения числа функционирующих серверов;
- обеспечивать авторизацию пользователей посредством протокола OpenID 2.0.

В 2.2.2 Аудит событий безопасности

Объект оценки должен обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в вычислительной среде. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к ОО или доступа к защищаемым активам. В частности, определяя политику аудита, уполномоченный администратор ОО должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как создание и удаление пользователей ОО или неудачные попытки подключения

пользователей к ОО. Запись результатов аудита событий безопасности должна осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору ОО. Просмотр журналов регистрации событий аудита должен выполняться с использованием средств ОО (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

В 2.2.3 Дискреционное управление доступом

В ОО доступ к защищаемым активам должен быть разрешен только уполномоченным на это пользователям ОО. Модель защиты ОО должна включать компоненты, которые реализуют контроль субъектов доступа и действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый пользователь, осуществляющий взаимодействие с ОО, должен быть представлен в нем регистрационной записью, определяющей сущностей, имеющих право доступа к ОО, так и его объектам. Для ОО должна поддерживаться таблица (список дискреционного управления доступом), в которой определены права доступа к объектам ОО. Список дискреционного управления доступом должен включать перечень пользователей (ролей), которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

В 2.2.4 Управление ролями

Использование ролей упрощает управление доступом к защищаемым активам, позволяя назначать разрешения и права группе пользователей, а не отдельной учетной записи. Таким образом, исходя из потребностей в доступе к новым активам, пользователь ОО может быть включен в состав участников определенной роли или исключен из участия в указанной роли.

Объект оценки должен поддерживать ряд предопределенных ролей, создаваемых в момент установки ОО. Членство в данных ролях должно

предоставлять право выполнять ряд административных и системных задач, таких как управление файлами и устройствами резервного копирования, установка и изменение параметров конфигурации ОО. Помимо predetermined ролей в ОО должна быть предусмотрена возможность создания и дальнейшего использования ролей, определяемых пользователями ОО, которые позволяют устанавливать специфичные для конкретной группы пользователей ОО права доступа при работе с ОО.

В 2.2.5 Основные функциональные возможности повышения надежности

Объект оценки должен обеспечивать надежную защиту данных от непредвиденных сбоев отказов системы, подмены и несанкционированному внесению изменений в элементы ОО, обеспечивая возможности по повышению надежности.

В 2.2.6 Средства администрирования, управления и поддержки

В состав ОО должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг) ОО.

В 3 СРЕДА БЕЗОПАСНОСТИ ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

- предположений относительно predetermined использования ОО и аспектов безопасности среды ОО;
- угроз безопасности, которым нужно противостоять средствами ОО;
- политики безопасности объекта эксплуатации, которой должен следовать ОО.

В 3.1 Предположения безопасности

В 3.1.1 Предположения относительно predetermined использования ОО

Предположение-1

Должно быть обеспечено отсутствие на сервере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Предположение-2

Должны быть обеспечены эксплуатация, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Предположение-3

Эксплуатация ОО должна проходить в защищённой среде, предотвращающей несанкционированные действия в отношении ОО и использование инструментальных средств, позволяющих осуществить доступ к защищаемым активам ОО в обход механизмов защиты.

В 3.1.2 Предположения относительно среды функционирования ОО

Предположение, связанное с физической защитой ОО

Предположение-4

Для предотвращения несанкционированного физического доступа ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположения, имеющие отношение к субъектам доступа

Предположение-5

Персонал, ответственный за администрирование ОО, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

Предположение-6

Уполномоченные на доступ к ОО пользователи должны руководствоваться эксплуатационной документацией на ОО, а их действия должны быть направлены исключительно на выполнение штатных функций ОО.

В 3.2 Угрозы

В настоящем ПЗ определены следующие угрозы, которым противостоит ОО.

Угроза-1

1. Аннотация угрозы – осуществление доступа к данным, хранящимся в репозитариях, неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к данным, хранящимся в репозитариях, удаленно, в том числе, с использованием средств поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к данным, связанные с возможностью предоставления доступа к пользовательским данным неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – данные, хранящиеся в репозиториях.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, достоверность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными, хранящиеся в репозиториях, несанкционированная модификация (в том числе подмена) данных; несанкционированное удаление данных.

Угроза-2

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся на объектах ОО (файлах, папках, и т.п.).

2. Источники угрозы – сторонние субъекты (пользователи сторонних по отношению к ОО систем).

3. Способ реализации угрозы – осуществление удаленного доступа к ОО с использованием средств, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; данные, хранящиеся в репозиториях.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемыми данными ФБО и данные, хранящиеся в репозиториях.

Угроза-3

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; данные, хранящиеся в репозитариях.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемыми данными ФБО и данными, хранящимися в репозитариях; невозможность однозначного сопоставления совершенных в ОО действий с пользователем, совершившим данные действия.

Угроза-4

1. Аннотация угрозы – осуществление доступа к данным аудита ОО пользователями ОО и неуполномоченными на это администраторами ОО и возможность несанкционированного удаления и модификации данных аудита ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способы реализации угрозы – осуществление доступа к данным аудита ОО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к данным аудита, связанные с возможностью осуществления доступа к данным аудита пользователями ОО и неуполномоченными на это администраторами ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – подконтрольность, целостность, конфиденциальность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля действий пользователей ОО и администраторов ОО, а также контроля процесса функционирования ОО в целом; навязывание администраторам ОО, ответственным за контроль данных аудита ОО, ложных (модифицированных) данных аудита; несанкционированное ознакомление о произошедших в ОО событиях.

Угроза-5

1. Аннотация угрозы – потеря данных аудита ОО вследствие переполнения выделенного для задач аудита хранилища информации.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – переполнение выделенного для задач аудита хранилища информации.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за переполнения хранилища данных аудита ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

Угроза-6

1. Аннотация угрозы – осуществление доступа к данным ФБО

неуполномоченными на это пользователями ОО и администраторами ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к данным ФБО локально с использованием средств ОО, а также удаленно, в том числе, с использованием средств поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

5. Вид активов, потенциально подверженных угрозе – данные ФБО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, доступность, достоверность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными ФБО (конфигурационные файлы, служебная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

Угроза-7

1. Аннотация угрозы – нарушение режимов функционирования ОО, а также потеря или искажение данных ФБО и пользовательских данных вследствие сбоев и отказов программного обеспечения и оборудования ОО.

2. Источники угрозы – программное обеспечение и оборудование ОО.

3. Способ реализации угрозы – сбои и отказы программного обеспечения и оборудования ОО.

4. Используемые уязвимости – недостатки механизмов защиты ОО от сбоев и отказов программного обеспечения и оборудования ОО; недостатки механизмов безопасного восстановления ОО после сбоев и отказов программного обеспечения и оборудования ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; данные, хранящиеся в репозиториях; программное обеспечение ОО.

6. Нарушаемое свойство безопасности активов – целостность, доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; потеря и искажение данных ФБО и данных, хранящиеся в репозитариях.

В 3.3 Политика безопасности объекта эксплуатации

Объект оценки должен следовать приведенным ниже правилам политики безопасности объекта эксплуатации.

Политика безопасности-1

Должно быть обеспечено наличие надлежащих корректно функционирующих средств администрирования ОО, доступных только уполномоченным администраторам ОО. Уполномоченным пользователям ОО должна быть предоставлена возможность модификации собственных аутентификационных данных.

Политика безопасности-2

Должны быть обеспечены надлежащая регистрация и предупреждение администратора ОО о любых событиях, относящихся к безопасности ОО. Должна быть обеспечена возможность для администратора ОО выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

Политика безопасности-3

Должна быть обеспечена возможность для уполномоченных на это администраторов ОО ограничивать права доступа к защищаемым активам для других пользователей ОО и администраторов ОО.

Политика безопасности-4

Должна быть обеспечена невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

Политика безопасности-5

Должна быть обеспечена возможность периодического контроля целостности ФБО и его данных, а также возможность регламентного тестирования ОО и среды функционирования ОО на предмет корректности функционирования.

Политика безопасности-6

Должен быть предоставлен механизм аутентификации.

В 4 ЦЕЛИ БЕЗОПАСНОСТИ

В 4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Разграничение доступа к защищаемым активам

ОО должен обеспечивать доступ к защищаемым активам только уполномоченным на это пользователям ОО и администраторам ОО. ОО должен обеспечивать возможность уполномоченным на это администраторам ОО ограничивать права доступа к защищаемым активам для других пользователей ОО и администраторов ОО других категорий.

Цель безопасности-2

Разграничение доступа к ОО

ОО должен обеспечивать доступ к ОО только уполномоченным на это пользователям ОО и администраторам ОО. Должны быть предусмотрены механизмы блокирования сеанса пользователя ОО и администратора ОО, осуществляемого по их инициативе, а также иницилируемого ФБО и основанного на интервале времени бездействия пользователя ОО или администратора ОО, либо основанного на ином механизме взаимодействия с ОО.

Цель безопасности-3

Аудит событий

ОО должен располагать надлежащими механизмами регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации должны предоставлять уполномоченным администраторам ОО возможность выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

Цель безопасности-4

Защита данных аудита

ОО должен обеспечивать защиту данных аудита от несанкционированного использования, предоставляя доступ к данным аудита только уполномоченным администраторам ОО, и предотвращать потерю данных аудита в случае переполнения их хранилища или по другим причинам.

Цель безопасности-5

Наличие средств администрирования

ОО должен располагать надлежащими корректно функционирующими средствами администрирования ОО, доступными только уполномоченным администраторам ОО. ОО должен предоставить для уполномоченных пользователей ОО возможность модификации собственных аутентификационных данных.

Цель безопасности-6

Защита данных ФБО

ОО должен обеспечивать защиту данных ФБО, поддерживая внутренний каталог пользователей (домен) для функционирования ФБО.

Цель безопасности-7

Доверенная аутентификация

ОО должен обеспечить невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

Цель безопасности-8

Безопасное восстановление

Должна быть обеспечена возможность безопасного восстановления ОО после сбоев и отказов программного обеспечения и оборудования ОО.

Цель безопасности-9

Контроль функционирования

ОО должен предоставлять возможность периодического контроля целостности ФБО и его данных, а также возможность собственного регламентного тестирования и тестирования среды функционирования ОО на предмет корректности функционирования.

Цель безопасности-10

Функция безопасности

ОО должен предоставлять механизм аутентификации.

В 4.2 Цели безопасности для среды

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

Цель для среды функционирования ОО-1

Доверительная среда функционирования

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Цель для среды функционирования ОО-2

Эксплуатация ОО

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Цель для среды функционирования ОО-3

Физическая защита ОО

Должна быть исключена возможность несанкционированного физического доступа к компьютеру с установленным ОО.

Цель для среды функционирования ОО-4

Требования к администраторам ОО

Персонал, ответственный за администрирование ОО, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.

Цель для среды функционирования ОО-5

Требования к пользователям ОО

Уполномоченные на доступ к ОО пользователи должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на ОО, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

Цель для среды функционирования ОО-6

Доверенная загрузка

Должна быть обеспечена загрузка ОО в доверенной среде, предотвращающей несанкционированное прерывание процесса загрузки ОО и использование инструментальных средств, позволяющих осуществить доступ к защищаемым активам

В 5 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ

В данном разделе ПЗ представлены требования безопасности ИТ, которым должен удовлетворять ОО. Функциональные требования безопасности, представленные в настоящем ПЗ, основаны на функциональных компонентах из части 2 РД БИТ, а также включают один функциональный компонент, сформулированный в явном виде. Требования доверия основаны на компонентах требований доверия из части 3 РД БИТ и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий». Функция безопасности «Аутентификация» реализуется механизмом паролей.

В 5.1 Требования безопасности для ОО

В 5.1.1 Функциональные требования безопасности ОО

Функциональные компоненты из части 2 РД БИТ, на которых основаны функциональные требования безопасности ОО, а также компонент сформулированных в явном виде расширенных ФТБ приведены в таблице 5.1.

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.4	Предотвращение потери данных аудита

Идентификатор компонента требований	Название компонента требований
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.2	Идентификация до любых действий пользователя
FIA_USB.1 (EXT)	Связывание пользователь-субъект
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_MTD.2	Управление ограничениями данных ФБО
FMT_REV.1	Отмена
FMT_SAE.1	Ограниченная по времени авторизация
FMT_SMR.1	Роли безопасности
FPT_AMT.1	Тестирование абстрактной машины
FPT_RCV.1	Ручное восстановление
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_STM.1	Надежные метки времени
FPT_TST.1	Тестирование ФБО
FTA_SSL.1	Блокирование сеанса, инициированное ФБО
FTA_SSL.2	Блокирование, инициированное пользователем
FTA_TSE.1	Открытие сеанса с ОО
FTP_TRP.1	Доверенный маршрут

В 5.1.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

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

- а) запуск и завершение выполнения функций аудита;
- б) [события, приведенные во втором столбце таблицы 5.2, а также [назначение: *другие специально определенные события, потенциально подвергаемые аудиту*]].

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

- а) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);
- б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ, [информацию, определенную в третьем столбце таблицы 5.2, а также [назначение: *другую относящуюся к аудиту информацию*]].

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_SAR.1	Чтение информации из записей аудита	
FAU_SAR.2	Неуспешные попытки читать информацию из записей аудита	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во время сбора данных аудита	
FAU_STG.3	Формирование предупреждения после превышения порога заполнения журнала аудита	

Компонент	Событие	Детализация
FAU_STG.4	Предотвращение регистрации событий или выполнение останова ОО при переполнении журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на объекте, на который распространяется политика дискреционного управления доступом	Идентификатор объекта
FIA_AFL.1	Достижение определенного уполномоченным администратором числа неуспешных попыток доступа к ОО	
FIA_SOS.1	Отклонение или принятие ФБО любого проверенного пароля	
FIA_UAU.2	Все случаи использования механизма аутентификации	
FIA_UID.2	Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	
FIA_USB.1 (EXT)	Успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта)	
FMT_MOF.1	Все модификации режимов функционирования функций, указанных в компоненте FMT_MOF.1	
FMT_MSA.1	Все модификации значений атрибутов безопасности, перечисленных в элементе FDP_ACF.1.1 компонента FDP_ACF.1	
FMT_MSA.3	Модификации настройки по умолчанию ограничительных правил политики дискреционного управления доступом. Все модификации начальных значений атрибутов безопасности, используемых в	

Компонент	Событие	Детализация
	политике дискреционного управления доступом	
FMT_MTD.1	Все модификации значений данных ФБО	
FMT_MTD.2	Модификация порогового значения количества неуспешных попыток аутентификации	
FMT_REV.1 (1)	Все попытки отменить атрибуты безопасности, ассоциированные с пользователями ОО	
FMT_REV.1 (2)	Все попытки отменить атрибуты безопасности, ассоциированные с объектами	
FMT_SAE.1	Назначение срока действия для аутентификационных данных. Блокирование ассоциированной с пользователем учетной записи	
FMT_SMR.1	Модификация группы пользователей – исполнителей роли пользователя ОО и администратора ОО. Каждое использование прав, предоставляемых ролью пользователя ОО и администратора ОО	Роль
FPT_AMT.1	Выполнение тестирования аппаратной среды и результаты тестирования	
FPT_RCV.1	Сбой и прерывание обслуживания	Тип сбоя и прерывания
FPT_STM.1	Изменения внутреннего представления времени	
FPT_TST.1	Выполнение и результаты самотестирования ФБО	
FTA_SSL.1	Все попытки разблокирования интерактивного сеанса	
FTA_SSL.2	Все попытки разблокирования	

Компонент	Событие	Детализация
	интерактивного сеанса	
FTA_TSE.1	Все попытки открытия сеанса пользователя	
FTP_TRP.1	Попытки аутентификации и разблокирования	

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 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.2 «Идентификация до любых действий пользователя».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченному администратору ОО] возможность читать [всю информацию аудита] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **уполномоченному администратору ОО** 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 **уполномоченных администраторов ОО**, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны **предоставлять** возможность выполнить поиск, сортировку данных аудита, основанные на

- [
следующих атрибутах:
а) идентификатор пользователя;
б) [**назначение:** *другие критерии*]
].

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SEL.1 Избирательный аудит

- FAU_SEL.1.1 ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой совокупности по следующим атрибутам:
а) идентификатор пользователя;
б) [**назначение:** *список дополнительных атрибутов, на которых основана избирательность аудита*].

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FMT_MTD.1 «Управление данными ФБО».

FAU_STG.1 Защищенное хранение журнала аудита

- FAU_STG.1.1 ФБО должны защищать хранимые записи аудита от несанкционированного удаления.
FAU_STG.1.2 ФБО должны быть способны к предотвращению модификации записей 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, направленные на сохранение данных журнала аудита и обеспечивающие непрерывность процесса аудита*], если журнал аудита **превысит** [установленный уполномоченным администратором ОО размер].

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны предотвращать события, подвергающиеся аудиту, исключая предпринимаемые уполномоченным администратором ОО и [назначение: **действия, направленные на невозможность совершения дальнейших событий, связанных с безопасностью ОО**], при переполнении журнала аудита.

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

В 5.1.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] для [

- а) [назначение: *список субъектов ОО*], действующих от имени пользователей;
- б) [назначение: *список именованных объектов ОО*];
- в) [назначение: *список операций между субъектами и объектами*]

].

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 дискреционного управления доступом] к объектам, основываясь на [

следующем:

- а) ассоциированные с субъектом идентификатор учетной записи пользователя, принадлежность к группе (группам);
- б) следующие, ассоциированные с объектами, атрибуты управления доступом: [**назначение:** *список атрибутов управления доступом, которые должны обеспечить возможность:*
 - ♣ *ассоциировать разрешение или запрет на выполнение операций с идентификаторами одного или более пользователей;*
 - ♣ *ассоциировать разрешение или запрет на выполнение операций с идентификаторами одной или более групп;*
 - ♣ *ассоциировать разрешение или запрет на выполнение операций по умолчанию]*

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: [**назначение:** *набор правил, определяющих политику дискреционного управления доступом, в которых:*

- а) *для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда идентификатор субъекта соответствует идентификатору, определенному в атрибутах управления доступом объекта;*
- б) *для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда субъект входит в состав группы, идентификатор которой, определен в атрибутах управления доступом объекта;*
- в) *для каждой операции должно быть определено правило или правила использования атрибутов разрешения по умолчанию в случаях, когда идентификатор субъекта не соответствует определенному в атрибутах управления доступом объекта и*

субъект входит в состав группы, идентификатор которой, не определен в атрибутах управления доступом объекта

].

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».

В 5.1.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [назначение: *определенное уполномоченным администратором ОО число*] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

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

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

Замечание по применению:

Конкретизация данного требования совместно с требованием FIA_SOS.1 в ЗБ должна обеспечивать возможность для механизмов безопасности, реализующих

функции безопасности «Аутентификация», предоставлять адекватную защиту от нарушения безопасности ОО нарушителем с низким потенциалом нападения.

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

[

- а) идентификатор пользователя;
- б) принадлежность к группе;
- в) [**назначение:** *другие атрибуты безопасности пользователя*]

].

Зависимости: отсутствуют.

Замечание по применению:

Под пользователями в настоящем компоненте требований понимаются все идентифицированные в FMT_SMR.1 роли.

FIA_SOS.1 Верификация секретов

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

Зависимости: отсутствуют.

Замечание по применению:

Конкретизация данного требования совместно с требованием FIA_AFL.1 в ЗБ должна обеспечивать возможность для механизмов безопасности, реализующих функции безопасности «Аутентификация», предоставлять адекватную защиту от нарушения безопасности ОО нарушителем с низким потенциалом нападения.

FIA_UAU.2 Аутентификация до любых действий пользователя

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

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

FIA_UAU.7 Аутентификация с защищенной обратной связью

FIA_UAU.7.1 ФБО должны предоставлять **субъекту доступа** [возможность ввода аутентификационной информации в скрытом виде] во время выполнения аутентификации.

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

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый **субъект доступа** был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: отсутствуют.

FIA_USB.1 (EXT) Связывание пользователь-субъект

FIA_USB.1.1 (EXT) ФБО должны ассоциировать следующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя:

- а) идентификатор пользователя, который ассоциируется с возможными для аудита событиями;
- б) идентификатор или идентификаторы пользователя, используемые для осуществления политики дискреционного управления доступом;

в) принадлежность к группе или группам, используемая для осуществления политики дискреционного управления доступом;

г) [назначение: *любые другие атрибуты безопасности пользователя*].

FIA_USB.1.2 (EXT) ФБО должны устанавливать следующие правила начальной ассоциации атрибутов безопасности пользователя с субъектами, действующими от имени пользователя:

а) [назначение: *правила начальной ассоциации*].

FIA_USB.1.3 (EXT) ФБО должны устанавливать следующие правила, определяющие возможность изменения атрибутов безопасности пользователя, ассоциированных с субъектами, действующими от имени пользователя:

а) [назначение: *правила изменения атрибутов*].

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

В 5.1.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность определять режим выполнения, модифицировать режим выполнения функций, **связанных**

с:

[

а) аудитом;

б) [назначение: *другие функции*]

]

только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предоставляющую** возможность модифицировать атрибуты безопасности, [перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1], только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предусматривающую** ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления **политики дискреционного управления доступом**.

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

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 [*выполнения операций, указанных во втором столбце таблицы 5.3, а также* [назначение: *другие операции*]] **над данными**, [указанными в третьем столбце таблицы 5.3, а также [назначение: *список других данных ФБО*]] только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.3 – Управляемые данные ФБО

Компонент	Операция	Данные ФБО
FAU_GEN.1	удаление, очистка, создание	журнал аудита
FAU_STG.3	установление, модификация	размер журнала аудита
FIA_ATD.1	установление, модификация	атрибуты безопасности пользователя
FIA_UAU.2	установление, модификация	аутентификационные данные (пароль)
FIA_UID.2	установление, модификация	идентификатор пользователя
FIA_USB.1 (EXT)	переопределение	заданные по умолчанию атрибуты безопасности пользователя
FPT_STM.1	модификация	представление времени

FMT_MTD.2 Управление ограничениями данных ФБО

FMT_MTD.2.1 ФБО должны предоставлять определение ограничений для [порогового значения количества неуспешных попыток аутентификации] только [назначение: *уполномоченные идентифицированные роли*].

FMT_MTD.2.2 ФБО должны предпринять следующие действия при достижении или превышении данными ФБО установленных выше ограничений: [назначение: *список действий, направленных на предотвращение попыток аутентификации*].

Зависимости: FMT_MTD.1 «Управление данными ФБО»,
FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО, администраторами ОО и объектами, в пределах ОДФ только [уполномоченному администратору ОО].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

- а) отмена полномочий у пользователей ОО и администраторов ОО на доступ к объектам должна вступать в силу при следующем сеансе работы пользователя ОО и администратора ОО;
- б) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;
- в) **[назначение: другие правила отмены]**

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с объектами, в пределах ОДФ только **[назначение: пользователи, уполномоченные на изменение атрибутов безопасности в соответствии с политикой дискреционного управления доступом]**.

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

- а) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;
- б) **[назначение: другие правила отмены]**

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_SAE.1 Ограниченная по времени авторизация

FMT_SAE.1.1 ФБО должны **предоставлять** возможность назначать срок действия для [аутентификационных данных] только [назначение: *уполномоченные идентифицированные роли*].

FMT_SAE.1.2 Для каждого из этих атрибутов безопасности ФБО должны быть способны к [блокированию ассоциированной с пользователем учетной записи] по истечении ее срока действия.

Зависимости: FMT_SMR.1 «Роли безопасности»,
FPT_STM.1 «Надежные метки времени».

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

- [
- а) администратор ОО;
 - б) пользователь ОО;
 - в) [назначение: *другие уполномоченные идентифицированные роли*]
-].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать **субъектов доступа** с ролями.

Зависимости: FIA_UID.2 «Выбор момента идентификации».

В 5.1.1.5 Защита ФБО (FPT)

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ при первоначальном запуске, периодически во время нормального функционирования, по запросу уполномоченного администратора ОО для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая **является базовой для ФБО**.

Зависимости: отсутствуют.

FPT_RCV.1 Ручное восстановление

FPT_RCV.1.1 После сбоя или прерывания обслуживания ФБО должны перейти в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию.

Зависимости: FPT_TST.1 «Тестирование ФБО»,
AGD_ADM.1 «Руководство администратора».

FPT_RVM.1 Невозможность обхода ПБО

FPT_RVM.1.1 ФБО должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 Отделение домена ФБО

FPT_SEP.1.1 ФБО должны поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 ФБО должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 ФБО должны быть способны предоставлять надежные метки времени для собственного использования.

Зависимости: отсутствуют.

FPT_TST.1 Тестирование ФБО

FPT_TST.1.1 ФБО должны выполнять пакет программ самотестирования при запуске и периодически в процессе нормального функционирования для демонстрации правильного выполнения ФБО.

FPT_TST.1.2 ФБО должны предоставить уполномоченным пользователям возможность верифицировать целостность данных ФБО.

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

Зависимости: FPT_AMT.1 «Тестирование абстрактной машины».

В 5.1.1.6 Доступ к ОО (FTA)

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

FTA_SSL.1.1 ФБО должны блокировать интерактивный сеанс после [истечения интервала времени бездействия пользователя ОО или администратора ОО], для чего предпринимаются следующие действия:

- а) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;
- б) блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса.

FTA_SSL.1.2 ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [повторная аутентификация пользователя ОО или администратора ОО].

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

FTA_SSL.2 Блокирование, инициированное пользователем

FTA_SSL.2.1 ФБО должны допускать инициированное пользователем **ОО или администратором ОО** блокирование своего собственного интерактивного сеанса, для чего предпринимаются следующие действия:

- а) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;

- б) блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса.

FTA_SSL.2.2 ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [повторная аутентификация пользователя ОО или администратора ОО].

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

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса, основываясь на **следующем**:

- [
а) идентификатор пользователя;
б) *[назначение: другие атрибуты]*
].

Зависимости: отсутствуют.

В 5.1.1.7 Доверенный маршрут/канал (FTP)

FTP_TRP.1 Доверенный маршрут

FTP_TRP.1.1 ФБО должны предоставлять маршрут связи между собой и локальным пользователем **ОО** или **администратором ОО**, который логически отличим от других маршрутов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту передаваемых данных от модификации или раскрытия.

FTP_TRP.1.2 ФБО должны позволить локальным пользователям ОО или администраторам ОО инициировать связь через доверенный маршрут.

FTP_TRP.1.3 ФБО должны требовать использования доверенного маршрута для начальной аутентификации пользователя ОО или администратора ОО *[и разблокирования сеанса]*.

Зависимости: отсутствуют.

В 5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 РД БИТ и образуют ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий» (см. таблицу 5.5).

Таблица 5.5 – Требования доверия к безопасности ОО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Управление конфигурацией	ACM_AUT.1	Частичная автоматизация УК
	ACM_CAP.4	Поддержка генерации, процедуры приемки
	ACM_SCP. 2	Охват УК отслеживания проблем
Поставка и эксплуатация	ADO_DEL.2	Обнаружение модификации
	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP. 2	Полностью определенные внешние интерфейсы
	ADV_HLD. 2	Детализация вопросов безопасности в проекте верхнего уровня
	ADV_IMP.1	Подмножество реализации ФБО
	ADV_LLD.1	Описательный проект нижнего уровня
	ADV_RCR. 1	Неформальная демонстрация соответствия
	ADV_SPM. 1	Неформальная модель политики безопасности ОО
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Поддержка жизненного цикла	ALC_DVS.1	Идентификация мер безопасности
	ALC_FLR. 1	Базовое устранение недостатков
	ALC_LCD. 1	Определение модели жизненного цикла разработчиком
	ALC_TAT. 1	Полностью определенные инструментальные средства разработки
Тестирование	ATE_COV.2	Анализ покрытия

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
	ATE_DPT.1	Тестирование: проект верхнего уровня
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_MSU.2	Подтверждение правильности анализа
	AVA_SOF.1	Оценка стойкости функции безопасности ОО
	AVA_VLA. 3	Умеренно стойкий

В 5.1.3 Управление конфигурацией (АСМ)

АСМ_AUT.1 Частичная автоматизация УК

Элементы действий разработчика

АСМ_AUT.1.1D Разработчик должен использовать систему УК.

АСМ_AUT.1.2D Разработчик должен представить план УК.

Элементы содержания и представления свидетельств

АСМ_AUT.1.1C Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО производятся только санкционированные изменения.

АСМ_AUT.1.2C Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.

АСМ_AUT.1.3C План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.

АСМ_AUT.1.4C План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.

Элементы действий оценщика

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

АСМ_САР.4 Поддержка генерации, процедуры приемки

Элементы действий разработчика

АСМ_САР.4.1D Разработчик должен предоставить маркировку для ОО.

АСМ_САР.4.2D Разработчик должен использовать систему УК.

АСМ_САР.4.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

АСМ_САР.4.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

АСМ_САР.4.2C ОО должен быть помечен маркировкой.

АСМ_САР.4.3C Документация УК должна включать в себя список конфигурации, план УК и план приемки.

АСМ_САР.4.4C Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

АСМ_САР.4.5C Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

АСМ_САР.4.6C Система УК должна уникально идентифицировать все элементы конфигурации.

АСМ_САР.4.7C План УК должен содержать описание, как используется система УК.

АСМ_САР.4.8C Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

АСМ_САР.4.9C Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

АСМ_САР.4.10C Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

АСМ_САР.4.11C Система УК должна поддерживать генерацию ОО.

АСМ_САР.4.12С План приемки должен содержать описание процедур, используемых для приемки модифицированного или вновь созданного элемента конфигурации как части ОО.

Элементы действий оценщика

АСМ_САР.4.1Е Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АСМ_SCP.2 Охват УК отслеживания проблем

Элементы действий разработчика

АСМ_SCP.3.1D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

АСМ_SCP.2.1С Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора, документацию УК **и недостатки безопасности.**

АСМ_SCP.2.2С Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.

Элементы действий оценщика

АСМ_SCP.2.1Е Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

В 5.1.4 Поставка и эксплуатация (ADO)

ADO_DEL.2 Обнаружение модификации

Элементы действий разработчика

ADO_DEL.2.1D Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

ADO_DEL.2.2 Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ADO_DEL.2.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий к местам использования.

ADO_DEL.2.2C Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.

ADO_DEL.2.3C Документация поставки должна содержать описание, как различные процедуры позволяют обнаружить попытку подмены от имени разработчика, даже в тех случаях, когда разработчик ничего не отсылал к месту использования.

Элементы действий оценщика

ADO_DEL.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

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

В 5.1.5 Разработка (ADV)

ADV_FSP.2 Полностью определенные внешние интерфейсы

Элементы действий разработчика

ADV_FSP.2.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.2.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.2.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.2.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая **полную** детализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.2.4C Функциональная спецификация должна полностью представить ФБО.

ADV_FSP.2.5C Функциональная спецификация должна включать в себя логическое обоснование, что ФБО полностью представлены.

Элементы действий оценщика

ADV_FSP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.2.2E Оценщик должен сделать независимое заключение, что функциональная спецификация - точное и полное отображение функциональных требований безопасности ОО.

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

Элементы действий разработчика

ADV_HLD.3.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.2.1C Представление проекта верхнего уровня должно быть неформальным.

ADV_HLD.2.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.2.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.2.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.2.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.2.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.2.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.2.8C Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_HLD.2.9C Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

Элементы действий оценщика

ADV_HLD.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.2.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня - точное и полное отображение функциональных требований безопасности ОО.

ADV_IMP.1 Подмножество реализации ФБО

Элементы действий разработчика

ADV_IMP.1.1D Разработчик должен обеспечить представление реализации для выбранного подмножества ФБО.

Элементы содержания и представления свидетельств

ADV_IMP.1.1C Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.

ADV_IMP.1.2C Представление реализации должно быть внутренне непротиворечивым.

Элементы действий оценщика

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

ADV_IMP.1.2E Оценщик должен сделать независимое заключение, что наименее абстрактное представление ФБО – точное и полное отображение функциональных требований безопасности ОО.

ADV_LLD.1 Описательный проект нижнего уровня

Элементы действий разработчика

ADV_LLD.1.1D Разработчик должен представить проект нижнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_LLD.1.1C Представление проекта нижнего уровня должно быть неформальным.

ADV_LLD.1.2C Проект нижнего уровня должен быть внутренне непротиворечивым.

ADV_LLD.1.3C Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

ADV_LLD.1.4C Проект нижнего уровня должен содержать описание назначения каждого модуля.

ADV_LLD.1.5C Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

ADV_LLD.1.6C Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.

ADV_LLD.1.7C Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

ADV_LLD.1.8C Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

ADV_LLD.1.9C Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя, при необходимости, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_LLD.1.10C Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

Элементы действий оценщика

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

ADV_LLD.1.2E Оценщик должен сделать независимое заключение, что проект нижнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

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

ADV_SPM.1 Неформальная модель политики безопасности ОО

Элементы действий разработчика

ADV_SPM.1.1D Разработчик должен представить модель ПБО.

ADV_SPM.1.2D Разработчик должен демонстрировать или доказать, где это требуется, соответствие между функциональной спецификацией и моделью ПБО.

Элементы содержания и представления свидетельств

ADV_SPM.1.1C Модель ПБО должна быть неформальной.

ADV_SPM.1.2C Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.1.3C Модель ПБО должна включать в себя логическое обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.1.4C Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.

Элементы действий оценщика

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

В 5.1.6 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

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

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

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

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

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

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

Элементы действий оценщика

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

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

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

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

AGD_USR.1.3C Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий,

которые следует контролировать в безопасной среде обработки информации.

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

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

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

Элементы действий оценщика

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

В 5.1.7 Поддержка жизненного цикла (ALC)

ALC_DVS.1 Идентификация мер безопасности

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

ALC_DVS.1.2C Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.

Элементы действий оценщика

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

ALC_DVS.1.2E Оценщик должен подтвердить применение мер безопасности.

ALC_FLR.1 Базовое устранение недостатков

Элементы действий разработчика

ALC_FLR.1.1D Разработчик должен задокументировать процедуры устранения недостатков.

Элементы содержания и представления свидетельств

ALC_FLR.1.1C Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждой редакции ОО.

ALC_FLR.1.2C Процедуры устранения недостатков должны содержать требование представления описания природы и проявлений каждого недостатка безопасности, а также статуса завершения исправления этого недостатка.

ALC_FLR.1.3C Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

ALC_FLR.1.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

Элементы действий оценщика

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

ALC_LCD.1 Определение модели жизненного цикла разработчиком

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 свидетельств

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

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

Элементы действий оценщика

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

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Элементы действий разработчика

ALC_TAT.1.1D Разработчик должен идентифицировать инструментальные средства разработки ОО.

ALC_TAT.1.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.

Элементы содержания и представления свидетельств

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

ALC_TAT.1.2C Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

ALC_TAT.1.3C Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.

Элементы действий оценщика

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

В 5.1.8 Тестирование (ATE)

ATE_COV.2 Анализ покрытия

Элементы действий разработчика

ATE_COV.2.1D Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

ATE_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

ATE_COV.2.2C Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.

Элементы действий оценщика

ATE_COV.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_DPT.1 Тестирование: проект верхнего уровня

Элементы действий разработчика

ATE_DPT.1.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE_DPT.1.1C Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня.

Элементы действий оценщика

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

ATE_FUN.1 Функциональное тестирование

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 свидетельств

ATE_FUN.1.1C Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.

ATE_FUN.1.2C Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей тестирования.

ATE_FUN.1.3C Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии

для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.

ATE_FUN.1.4C Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.

ATE_FUN.1.5C Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.

Элементы действий оценщика

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

ATE_IND.2 Выборочное независимое тестирование

Элементы действий разработчика

ATE_IND.2.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

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 представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.2.2E Оценщик должен протестировать подмножество ФБО, **как необходимо**, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

ATE_IND.2.3E Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

В 5.1.9 Оценка уязвимостей (AVA)

AVA_MSU.2 Подтверждение правильности анализа

Элементы действий разработчика

AVA_MSU.2.1D Разработчик должен представить руководства по применению ОО.

AVA_MSU.2.2D Разработчик должен задокументировать анализ руководств.

Элементы содержания и представления свидетельств

AVA_MSU.2.1C Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.2.2C Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

AVA_MSU.2.3C Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.2.4C Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

AVA_MSU.2.5C Документация анализа должна демонстрировать, что руководства полны.

Элементы действий оценщика

AVA_MSU.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_MSU.2.2E Оценщик должен повторить все процедуры конфигурирования и установки и выборочно другие процедуры для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

AVA_MSU.2.3E Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

AVA_MSU.2.4E Оценщик должен подтвердить, что документация анализа показывает обеспечение руководствами безопасного функционирования во всех режимах эксплуатации ОО.

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

Элементы действий оценщика

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

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

AVA_VLA.3 Умеренно стойкий

Элементы действий разработчика

AVA_VLA.3.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску путей, которыми пользователь может нарушить ПБО.

AVA_VLA.3.2D Разработчик должен задокументировать местоположение идентифицированных уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.3.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.3.2C Документация должна содержать строгое обоснование, что ОО с идентифицированными уязвимостями является стойким к явным нападениям проникновения.

AVA_VLA.3.3C Свидетельство должно показать, что поиск уязвимостей является систематическим.

Элементы действий оценщика

AVA_VLA.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_VLA.3.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.

AVA_VLA.3.3E Оценщик должен выполнить независимый анализ уязвимостей.

AVA_VLA.3.4E Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.

AVA_VLA.3.5E Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим **умеренным** потенциалом нападения.

В 6 ОБОСНОВАНИЕ

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

В 6.1 Обоснование целей безопасности

В 6.1.1 Обоснование целей безопасности для ОО

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

Таблица 6.1 – Отображение целей безопасности на угрозы и политику безопасности объекта эксплуатации

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10
Угроза-1	X									
Угроза-2		X								
Угроза-3		X								
Угроза-4				X						
Угроза-5				X						
Угроза-6						X				
Угроза-7								X		
Политика безопасности-1					X					
Политика безопасности-2			X							
Политика безопасности-3	X									
Политика безопасности-4							X			

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10
Политика безопасности-5									X	
Политика безопасности-6										X

Цель безопасности-1

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-1** и реализацией политики безопасности организации **Политика безопасности-3**, так как обеспечивает доступ к защищаемым активам только уполномоченным на это пользователям ОО и администраторам ОО, а также обеспечивает возможность уполномоченным пользователям ОО ограничивать права доступа к защищаемым активам для других пользователей ОО и администраторов ОО.

Цель безопасности-2

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-2** и **Угроза-3**, так как обеспечивает доступ к ОО только уполномоченным на это пользователям ОО и администраторам ОО, а также блокирование сеанса пользователя ОО и администратора ОО, осуществляемое по их инициативе, а также инициируемое ФБО и основанное на интервале времени бездействия пользователя ОО или администратора ОО.

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-2**, так как обеспечивает наличие надлежащих механизмов регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО.

Механизмы регистрации предоставляют администраторам ОО возможность выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-4** и **Угроза-5**, так как обеспечивает доступ к данным аудита только уполномоченным администраторам ОО и предотвращает потерю данных аудита в случае переполнения их хранилища.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-1**, так как обеспечивает наличие надлежащих корректно функционирующих средств администрирования ОО, доступных только уполномоченным администраторам ОО, а также возможность модификации собственных аутентификационных данных уполномоченными пользователями ОО.

Цель безопасности-6

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-6**, так как обеспечивает защиту данных ФБО, поддерживая домен для функционирования ФБО.

Цель безопасности-7

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-4**, так как обеспечивает невозможность подмены сервисов доступа на этапе аутентификации администраторов ОО и пользователей ОО.

Цель безопасности-8

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-7**, так как обеспечивает возможность безопасного восстановления ОО после сбоя и отказов программного обеспечения и оборудования ОО.

Цель безопасности-9

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-5**, так как обеспечивает возможность периодического контроля целостности ФБО и его данных, а также возможность собственного регламентного тестирования и тестирования среды функционирования ОО на предмет корректности функционирования.

Цель безопасности-10

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-6**, так как обеспечивает наличие механизма аутентификации, обеспечивающего адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения

В 6.1.2 Обоснование целей безопасности для среды

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

Таблица 6.2 – Отображение целей безопасности для среды на предположения безопасности

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-6
Предположение-1	X					
Предположение-2		X				
Предположение-3						X
Предположение-4			X			
Предположение-5				X		
Предположение-6					X	

Цель для среды функционирования ОО-1

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-1**, так как обеспечивает отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Цель для среды функционирования ОО-2

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-2**, так как обеспечивает установку конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Цель для среды функционирования ОО-3

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-4**, так как обеспечивает исключение возможности несанкционированного физического доступа к компьютеру с установленным ОО.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-5**, так как обеспечивает, что персонал, ответственный за администрирование ОО, является благонадежным и компетентным, и руководствуется в своей деятельности соответствующей документацией.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-6** иной документацией на ОО, а их совместные действия направлены исключительно на выполнение своих функциональных обязанностей.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-3**, так как обеспечивает выполнение загрузки ОО в доверенной среде, предотвращающей несанкционированное прерывание процесса загрузки ОО и использование инструментальных средств, позволяющих осуществить доступ к защищаемым активам ОО в обход механизмов защиты.

В 6.2 Обоснование требований безопасности

В 6.2.1 Обоснование требований безопасности для ОО

В 6.2.1.1 Обоснование функциональных требований безопасности ОО

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

Таблица 6.3 – Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10
FAU_GEN.1			X							
FAU_GEN.2			X							
FAU_SAR.1			X							
FAU_SAR.2			X							
FAU_SAR.3			X							
FAU_SEL.1			X							
FAU_STG.1				X						
FAU_STG.3				X						
FAU_STG.4				X						
FDP_ACC.1	X									
FDP_ACF.1	X									
FIA_AFL.1		X								X
FIA_ATD.1	X	X	X		X					
FIA_SOS.1										X
FIA_UAU.2	X	X								
FIA_UAU.7		X								

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6	Цель безопасности-7	Цель безопасности-8	Цель безопасности-9	Цель безопасности-10
FIA_UID.2	X	X								
FIA_USB.1 (EXT)	X	X	X							
FMT_MOF.1					X					
FMT_MSA.1	X				X					
FMT_MSA.3	X				X					
FMT_MTD.1					X					
FMT_MTD.2					X					
FMT_REV.1 (1)					X					
FMT_REV.1 (2)	X									
FMT_SAE.1					X					
FMT_SMR.1	X			X	X	X				
FPT_AMT.1									X	
FPT_RCV.1								X		
FPT_RVM.1						X				
FPT_SEP.1						X				
FPT_STM.1			X		X					
FPT_TST.1									X	
FTA_SSL.1		X								
FTA_SSL.2		X								
FTA_TSE.1		X								
FTP_TRP.1							X			

FAU_GEN.1

Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО.

Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_GEN.2 Ассоциация идентификатора пользователя

Выполнение требований данного компонента обеспечивает возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором учетной записи пользователя или идентификатором регистрационной записи пользователя, который был инициатором этого события. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления уполномоченному администратору ОО всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает запрет всем пользователям доступ к чтению записей аудита, за исключением уполномоченных администраторов ОО, которым явно предоставлен доступ для чтения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает выполнение поиска и сортировки данных аудита, основанных на определенных критериях (идентификатор пользователя). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SEL.1

Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, уполномоченным администратором ОО по определенным атрибутам (идентификатор пользователя). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_STG.1

Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает защиту хранимых записей аудита от несанкционированного удаления и предотвращает модификацию записей аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_STG.3

Действия в случае возможной потери данных аудита

Выполнение требований данного компонента обеспечивает выполнение действий, направленных на сохранение данных журнала аудита и обеспечивающих непрерывность процесса аудита, если журнал аудита превысит определенный уполномоченным администратором ОО размер. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_STG.4

Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает предотвращение событий, подвергающихся аудиту, и выполнение других действий, направленных на невозможность совершения дальнейших событий, связанных с безопасностью ОО, при переполнении журнала аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FDP_ACC.1

Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает реализацию политики дискреционного доступа для субъектов, именованных объектов и всех операций между субъектами и объектами. 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 осуществление политики дискреционного доступа, основываясь на атрибутах безопасности, определении правил доступа субъектов к объектам. 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 ОО. При достижении определенного администратором ОО числа неуспешных попыток аутентификации некоторого лица, ОО предпринимаются действия, направленные на дальнейшее предотвращение попыток доступа со стороны данного лица, ограниченное временным интервалом. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-2, Цель безопасности-10** и способствует их достижению.

FIA_ATD.1

Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя (пользователя ОО и администратора ОО) ряда атрибутов безопасности (идентификатора пользователя, принадлежность к группе). Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3, Цель безопасности-5** и способствует их 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-10** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2** и способствует их достижению.

FIA_UAU.7 Аутентификация с защищенной обратной связью

Выполнение требований данного компонента обеспечивает, что во время выполнения аутентификации вводимый пользователем пароль отображается в скрытом виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение идентификации субъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1, Цель безопасности-2** и способствует их достижению.

FIA_USB.1 (EXT) Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами,

действующими от имени этого субъекта доступа. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3** и способствует их достижению.

FMT_MOF.1 Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает определенные действия над функциями из числа ФБО только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только уполномоченным ролям. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-5** и способствует их достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом, и возможность для уполномоченных ролей определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-5** и способствует их достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность осуществлять определенные операции над данными ФБО только уполномоченным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует их достижению.

FMT_MTD.2

Управление ограничениями данных ФБО

Выполнение требований данного компонента предоставляет возможность определения ограничений для порогового значения количества неуспешных попыток аутентификации только уполномоченной роли. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует их достижению.

FMT_REV.1 (1) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО, в пределах ОДФ только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_REV.1 (2) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с объектами, в пределах ОДФ только пользователю ОО, уполномоченному согласно политике дискреционного управления доступом модифицировать атрибуты безопасности объекта. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FMT_SAE.1

Ограниченная по времени авторизация

Выполнение требований данного компонента предоставляет возможность назначать срок действия для аутентификационных данных только уполномоченным ролям. По истечении срока действия аутентификационных данных ФБО осуществляют блокирование ассоциированной с пользователем учетной записи. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_SMR.1

Роли безопасности

Данный компонент включен в ПЗ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту ролей администратора ОО и пользователя ОО, а также других возможных ролей. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-4, Цель безопасности-5, Цель безопасности-6** и способствует их достижению.

FPT_AMT.1

Тестирование абстрактной машины

Данный компонент включен в ПЗ, для того, чтобы учесть зависимости выполнения требований компонента FPT_TST.1. Выполнение требований данного компонента обеспечивает тестирование правильности выполнения предположений безопасности, представленных базовой абстрактной машиной, при первоначальном запуске, периодически и по запросу уполномоченного администратора ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-9** и способствует ее достижению.

FPT_RCV.1

Ручное восстановление

Выполнение требований данного компонента обеспечивает переход ФБО в режим аварийной поддержки для последующего возврата ОО в безопасное состояние после сбоя или прерывания обслуживания. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-8** и способствует ее достижению.

FPT_RVM.1

Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FPT_SEP.1 Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ПЗ, для того, чтобы учесть зависимости выполнения требований компонента FAU_GEN.1 от наличия в записях аудита точного указания даты и времени и для учета зависимости выполнения требований компонента FMT_SAE.1 от наличия времени для определения срока действия аутентификационных данных. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-3, Цель безопасности-5** и способствует их достижению.

FPT_TST.1 Тестирование ФБО

Выполнение требований данного компонента обеспечивает целостность выполнения ФБО и предоставляет администратору ОО средства верификации целостности кода и данных ФБО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-9** и способствует ее достижению.

FTA_SSL.1 Блокирование сеанса, инициированное ФБО

Выполнение требований данного компонента обеспечивает блокирование сеанса пользователя ОО или администратора ОО после истечения интервала времени бездействия. Определяются действия, необходимые для разблокирования. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FTA_SSL.2 Блокирование, инициированное пользователем

Выполнение требований данного компонента обеспечивает блокирование сеанса, инициированное пользователем ОО или администратором ОО. Определяются действия, необходимые для разблокирования. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FTA_TSE.1 Открытие сеанса с ОО

Выполнение требований данного компонента обеспечивает способность отказа ОО в открытии сеанса доступа к ОО, основываясь на идентификаторе пользователя, а также других атрибутах. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

FTP_TRP.1 Доверенный маршрут

Выполнение требований данного компонента обеспечивает установление доверенной связи между ФБО и локальным пользователем ОО или администратором ОО для целей начальной аутентификации и разблокирования сеанса. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-7** и способствует ее достижению.

В 6.2.1.2 Обоснование требований доверия к безопасности ОО

Включение в настоящий ПЗ ОУД4, усиленный компонентом ALC_FLR.1 «Базовое устранение недостатков» AVA_VLA.3 «Умеренно стойкий», является достаточным при определении допустимости использования ОО в информационных системах, в которых обрабатывается информация ограниченного доступа.

В 6.2.2 Обоснование зависимостей требований

В таблице 6.4 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворены

в настоящем ПЗ либо включением компонентов, определенных в части 2 РД БИТ под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в части 2 РД БИТ под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 6.4 является справочным и содержит компоненты, определенные в части 2 РД БИТ в описании компонентов требований, приведенных в столбце 1 таблицы 6.4, под рубрикой «Зависимости».

Столбец 3 таблицы 6.4 показывает, какие компоненты требований были реально включены в настоящий ПЗ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 6.4. Компоненты требований в столбце 3 таблицы 6.4 либо совпадают с компонентами в столбце 2 таблицы 6.4, либо иерархичны по отношению к ним.

Таблица 6.4 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по РД БИТ	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.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.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
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2

Функциональные компоненты	Зависимости по РД БИТ	Удовлетворение зависимостей
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_USB.1 (EXT)	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1 (1)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_MTD.2	FMT_MTD.1, FMT_SMR.1	FMT_MTD.1, FMT_SMR.1
FMT_REV.1 (1)	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_SAE.1	FMT_SMR.1, FPT_STM.1	FMT_SMR.1, FPT_STM.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RCV.1	FPT_TST.1, AGD_ADM.1, ADV_SPM.1	FPT_TST.1, AGD_ADM.1, <i>обосновано не включение ADV_SPM.1</i>
FPT_TST.1	FPT_AMT.1	FPT_AMT.1
FTA_SSL.1	FIA_UAU.1	FIA_UAU.2
FTA_SSL.2	FIA_UAU.1	FIA_UAU.2

ПРИЛОЖЕНИЕ Г

(обязательное)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИЗДЕЛИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ЭТАЛОННАЯ СРЕДА РАЗРАБОТКИ, СБОРКИ И ОБНОВЛЕНИЯ ОПЕРАЦИОННОЙ СИСТЕМЫ И ПРИКЛАДНЫХ ПРИЛОЖЕНИЙ

**Профиль защиты
ИЗД_ИТ.ЭСР.ОУД4.ПЗ**

Версия 1.0

СОДЕРЖАНИЕ

Г 1	Введение ПЗ	216
Г 1.1	Идентификация ПЗ.....	216
Г 1.2	Аннотация ПЗ	217
Г 1.3	Соглашения.....	218
Г 1.4	Термины и определения.....	219
Г 1.5	Организация ПЗ.....	221
Г 2	Описание ОО	222
Г 2.1	Тип изделия ИТ	222
Г 2.2	Основные функциональные возможности ОО	222
Г 3	Среда безопасности ОО	228
Г 3.1	Предположения безопасности	228
Г 3.2	Угрозы.....	230
Г 3.3	Политика безопасности объекта эксплуатации	237
Г 4	Цели безопасности	239
Г 4.1	Цели безопасности для ОО	239
Г 4.2	Цели безопасности для среды.....	240
Г 5	Требования безопасности ИТ	243
Г 5.1	Требования безопасности для ОО	243
Г 5.2	Требования безопасности для среды ИТ.....	278
Г 6	Обоснование	282
Г 6.1	Обоснование целей безопасности	282
Г 6.2	Обоснование требований безопасности	288

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БИТ	– безопасность информационных технологий
ЗБ	– задание по безопасности
ИС	– информационная система
ИТ	– информационная технология
НСД	– несанкционированный доступ
ОДФ	– область действия функции безопасности объекта оценки
ОО	– объект оценки
ОС	– операционная система
ОУД	– оценочный уровень доверия
ПБО	– политика безопасности объекта оценки
ПЗ	– профиль защиты
ПФБ	– политика функции безопасности
УК	– управление конфигурацией
ФБО	– функции безопасности объекта оценки
ФТБ	– функциональные требования безопасности

Г 1 ВВЕДЕНИЕ ПЗ

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

Г 1.1 Идентификация ПЗ

Название ПЗ:	Безопасность информационных технологий. Изделия информационных технологий. Эталонная среда разработки. Профиль защиты.
Семейство ПЗ:	Изделия ИТ.
Функциональная группа:	Среды разработки.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИЗД_ИТ.ЭСР.ОУД4.ПЗ.
Идентификация ОО:	Эталонная среда разработки.
Уровень доверия:	ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий».

***Идентификация РД
БИТ:***

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 1: Введение и общая модель, ФСТЭК (Гостехкомиссия) России, 2002.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 2: Функциональные требования безопасности, ФСТЭК (Гостехкомиссия) России, 2002.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 3: Требования доверия к безопасности, ФСТЭК (Гостехкомиссия) России, 2002.

Ключевые слова:

Эталонная среда разработки, средство защиты информации, профиль защиты, ОУД4.

Г 1.2 Аннотация ПЗ

Настоящий ПЗ определяет требования безопасности для Эталонной среды разработки (далее – объект оценки).

Объект оценки представляет собой полнофункциональную среду разработки, сборки и обновления операционной системы и прикладных приложений на основе свободного программного обеспечения, обеспечивающую надежную инфраструктурную платформу высокой производительности для создания, развертывания и поддержки производственных программных продуктов.

Среды разработки, соответствующие настоящему профилю защиты, могут использоваться в информационных системах, обрабатывающих конфиденциальную информацию.

Г 1.3 Соглашения

Руководящий документ ФСТЭК (Гостехкомиссии) России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (далее – РД БИТ) допускает выполнение определенных в части 2 РД БИТ операций над функциональными требованиями. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор», «назначение» и «итерация».

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

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

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

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

В настоящем ПЗ используются компоненты функциональных требований безопасности, включающие незавершенные операции **«назначение»** в которых область предполагаемых значений уточнена по отношению к исходному компоненту из части 2 РД БИТ. В данных компонентах операции **«назначения»** с

уточненной областью предполагаемых значений обозначаются как [назначение: *уточненная область предполагаемых значений*].

Операция «**итерация**» используется для более чем однократного использования компонента функциональных требований безопасности ИТ при различном выполнении разрешенных операций (уточнение, выбор, назначение). Выполнение «итерации» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

Замечания по применению предназначены либо для разъяснения назначения некоторого требования, идентификации вариантов реализации, либо для определения условий выполнения требования. В случае использования, замечания по применению следуют за компонентом требования.

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

Г 1.4 Термины и определения

В настоящем ПЗ применяются следующие термины с соответствующими определениями.

Активы: Информация и ресурсы, подлежащие защите.

Аутентификационные данные: информация, используемая для верификации предъявленного идентификатора.

Аутентификация: Процесс установления подлинности информации, предъявленной администратором безопасности и пользователем ИС при регистрации.

Данные ФБО: Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО.

Доступность: Состояние безопасности активов (информации), характеризующее их готовностью к использованию по запросу

уполномоченных лиц, объектов или субъектов, а также возможностью их восстановления в случае сбоя (отказа).

Задание по безопасности: Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного изделия ИТ.

Конфиденциальность: Состояние безопасности активов (информации), характеризующее их защищенностью от несанкционированного доступа и/или раскрытия их содержания неуполномоченным лицам, объектам или процессам.

Область действия ФБО: Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО.

Объект оценки: подлежащее оценке изделие ИТ с документацией.

Политика безопасности объекта эксплуатации: Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

Политика безопасности ОО: Совокупность правил, определяющих режим обеспечения безопасности ОО и представляемых в виде набора функциональных требований безопасности.

Политика функции безопасности: Политика безопасности, осуществляемая ФБ.

Пользователь: Любая сущность (человек-пользователь или внешний объект изделия ИТ) вне ОО, которая взаимодействует с ОО.

Изделие ИТ: Программное, программно-аппаратное или аппаратное обеспечение изделий ИТ, специально разработанное для использования в составе ИС

Профиль защиты: Совокупность требований безопасности для некоторого типа изделий ИТ.

Уполномоченный администратор: Уполномоченный пользователь, ответственный за эксплуатацию ОО.

Функция безопасности: Функциональные возможности части или частей изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных функциональных требований безопасности.

Целостность: Состояние безопасности активов (информации), характеризующее их полнотой и защищенностью от несанкционированного изменения (модификации).

Г 1.5 Организация ПЗ

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

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

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

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

В разделе 5 «Требования безопасности ИТ» на основе частей 2 и 3 РД БИТ определены, соответственно, функциональные требования безопасности ИТ и требования доверия к безопасности ОО.

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

Г 2 ОПИСАНИЕ ОО

Объектом оценки в настоящем ПЗ является эталонная среда разработки, сборки и обновления операционной системы и прикладных приложений.

Г 2.1 Тип изделия ИТ

Эталонная среда разработки, сборки и обновления операционной системы и прикладных приложений на основе свободного программного обеспечения является интегрированной средой разработки.

Интегрированная среда разработки - это совокупность программных средств, поддерживающая все этапы разработки программного обеспечения от написания исходного текста программы до ее компиляции и отладки, и обеспечивающая простое и быстрое взаимодействие с другими инструментальными средствами.

Цель использования интегрированной среды разработки заключается в том, чтобы объединить утилиты командной строки в одном средстве, которое позволит повысить производительность при разработке программного обеспечения. С помощью интегрированной среды разработки программист может редактировать, компилировать и запускать программы, не покидая интегрированной среды разработки.

Использование интегрированной среды разработки для разработки программного обеспечения является прямой противоположностью способа, в котором используются отдельные несвязанные инструменты, такие как текстовый редактор, компилятор и другие, взаимодействие между которыми осуществляется пользователем вручную через интерфейс командной строки, что существенно повышает вероятность ошибки и трудоемкость разработки.

Г 2.2 Основные функциональные возможности ОО

В ОО должен быть реализован ряд функциональных возможностей и средств, позволяющих обеспечить безопасность ИТ, надежность ОО, а также упрощающих

администрирование ОО и управление ОО. В данном подразделе представлено краткое описание предполагаемых функциональных возможностей и средств.

ОО должен содержать следующие основные программные компоненты:

- распределённая система управления версиями исходного кода;
- средство обеспечения хранения исходных и бинарных пакетов программ;
- средство автоматической сборки пакетов из системы контроля версий в хранилище;
- средство управления очередью заданий на сборку;
- средство автоматического тестирования неухудшения характеристик хранилища (замкнутость по зависимостям в том числе — бинарных пакетов по всем предоставляемыми используемым символам)
- средство автоматического формирования пакетов с отладочной информацией с поддержкой зависимостей между ними;
- средство работы с персональными дополнениями к хранилищу;
- средство проведения масштабных экспериментов над хранилищем;
- средство проведение автоматического интеграционного тестирования на основе виртуальных машин:
- Web-интерфейс сборочной системы;
- средства интеграции со внешними системами управления версий программного обеспечения на базе cvs, svn, git;
- средства горизонтального масштабирования системы;
- средства управления сборкой для различных версий дистрибутивов и аппаратных платформ;
- XML-RPC API для интеграции с внешними системами;
- средства идентификации, аутентификации и авторизации пользователей, разграничение доступа пользователей, назначение различных полномочий пользователей на выполнение операций вплоть до уровня отдельных пакетов;
- средства ведения журнала операций с возможностью полного аудита событий в системе.

Г 2.2.1 Основные функциональные возможности

В ОО должны быть включены средства, позволяющие защитить выбранные файлы, приложения и ресурсы. В число таких средств входят списки управления доступом, группы безопасности и механизмы централизованного управления параметрами безопасности, а также инструменты, позволяющие настраивать эти средства и управлять ими. Вместе они обеспечивают мощную и гибкую инфраструктуру управления доступом.

ОО должен поддерживать следующий функционал:

- сборка пакетов хранилища из распределённой системы управления версиями программного обеспечения;
- интеграция со внешними системами управления версий программного обеспечения на базе cvs, svn, git;
- контроль наследования сборок пакетов хранилища в распределённой системе управления версиями программного обеспечения;
- автоматическая сборка (роботы) для нескольких различных классов пакетов программ;
- поддержка одновременной работы с несколькими версиями дистрибутива, возможность параллельной сборки отдельных пакетов как для всех версий, так и для определенного подмножества;
- поддержка одновременной работы с сборочными системами разных аппаратных архитектур, возможность параллельной сборки пакетов как для всех архитектур, так и для определенного подмножества;
- простое масштабирование среды сборки за счет подключения дополнительных серверов для выполнения сборки без переконфигурирования остальной части системы;
- среда автоматического интеграционного тестирования на базе виртуальных машин;
- полное замыкание бинарных архитектурно-зависимых пакетов по предоставляемым и используемым символам;

- возможность создания пакетов с отладочной информацией и с поддержкой зависимостей между такими пакетами;
- контроль неухудшения характеристик хранилища по критерию пересобираемости пакетов;
- поддержка клонирования хранилища для проведения масштабного эксперимента над значительной частью пакетов хранилища;
- поддержка персональных дополнений к хранилищу (пакеты, не опубликованные в хранилище, но совместимые с ним);
- Web-интерфейс сборочной системы (мониторинг состояния сборочной очереди, отправка заданий на сборку);
- наличие XML-RPC API для интеграции с внешними системами;
- наличие средств идентификации, аутентификации и авторизации пользователей, разграничение доступа пользователей, назначение различных полномочий пользователей на выполнение операций вплоть до уровня отдельных пакетов;
- ведение журнала операций и возможность полного аудита событий в системе.

Г 2.2.2 Аудит событий безопасности

Объект оценки должен обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в вычислительной среде. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к ОО или доступа к защищаемым активам. В частности, определяя политику аудита, уполномоченный администратор ОО должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как создание и удаление пользователей ОО или неудачные попытки подключения пользователей к ОО. Запись результатов аудита событий безопасности должна

осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору ОО. Просмотр журналов регистрации событий аудита должен выполняться с использованием средств ОО (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

Г 2.2.3 Дискреционное управление доступом

В ОО доступ к защищаемым активам должен быть разрешен только уполномоченным на это пользователям ОО. Модель защиты ОО должна включать компоненты, которые реализуют контроль субъектов доступа и действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый пользователь, осуществляющий взаимодействие с ОО, должен быть представлен в нем регистрационной записью, определяющей сущностей, имеющих право доступа к ОО, так и его объектам. Для ОО должна поддерживаться таблица (список дискреционного управления доступом), в которой определены права доступа к объектам ОО. Список дискреционного управления доступом должен включать перечень пользователей (ролей), которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

Г 2.2.4 Управление ролями

Использование ролей упрощает управление доступом к защищаемым активам, позволяя назначать разрешения и права группе пользователей, а не отдельной учетной записи. Таким образом, исходя из потребностей в доступе к новым активам, пользователь ОО может быть включен в состав участников определенной роли или исключен из участия в указанной роли.

Объект оценки должен поддерживать ряд предопределенных ролей, создаваемых в момент установки ОО. Членство в данных ролях должно предоставлять право выполнять ряд административных и системных задач, таких как управление файлами и устройствами резервного копирования, установка и изменение параметров конфигурации ОО. Помимо предопределенных ролей в ОО должна быть предусмотрена возможность создания и дальнейшего использования ролей, определяемых пользователями ОО, которые позволяют устанавливать специфичные для конкретной группы пользователей ОО права доступа при работе с ОО.

Г 2.2.5 Основные функциональные возможности повышения надежности

Объект оценки должен обеспечивать надежную защиту данных от непредвиденных сбоев отказов системы, подмены и несанкционированному внесению изменений в элементы ОО, обеспечивая возможности по повышению надежности.

Г 2.2.6 Средства администрирования, управления и поддержки

В состав ОО должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг) ОО.

Г 3 СРЕДА БЕЗОПАСНОСТИ ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

- предположений относительно предопределенного использования ОО и аспектов безопасности среды ОО;
- угроз безопасности, которым нужно противостоять средствами ОО;
- политики безопасности объекта эксплуатации, которой должен следовать ОО.

Г 3.1 Предположения безопасности

Г 3.1.1 Предположения относительно предопределенного использования ОО

Предположение-1

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Предположение-2

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположение-3

Должно быть обеспечено взаимодействие ОО только с доверенными изделиями (системами) ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

Предположение-4

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Предположение-5

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

Предположение-6

Функционирование ОО должно осуществляться в среде функционирования, предоставляющей механизм аутентификации.

Предположение-7

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

Г 3.1.2 Предположения относительно среды функционирования ОО

Предположение, связанное с физической защитой ОО

Предположение-8

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположения, имеющие отношение к персоналу

Предположение-9

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

Предположение-10

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

Г 3.2 Угрозы

Г 3.2.1 Угрозы, которым противостоит ОО

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

Угроза-1

1. Аннотация угрозы – осуществление доступа к информации, размещаемой на объектах ОО, неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к информации, размещаемой на объектах ОО, с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к объектам ОО, связанные с возможностью предоставления доступа к информации, размещаемой на объектах ОО, неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – информация, размещаемая на объектах ОО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, достоверность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, размещаемой на объектах ОО; несанкционированная модификация информации (в том числе подмена), размещаемой на объектах ОО; несанкционированное удаление информации, размещаемой на объектах ОО.

Угроза-2

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией ОО.

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем).

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация ОО.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией, ОО.

Угроза-3

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к ОО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация ОО.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией ОО; невозможность однозначного сопоставления совершенных в ОО действий с субъектом, совершившим данные действия.

Угроза-4

1. Аннотация угрозы – осуществление доступа к данным аудита ОО пользователями ОО и неуполномоченными на это администраторами ОО и возможность несанкционированного удаления и модификации данных аудита ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способы реализации угрозы – осуществление доступа к данным аудита ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным аудита с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к данным аудита, связанные с возможностью осуществления доступа к данным аудита пользователями ОО и неуполномоченными на это администраторами ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – подконтрольность, целостность, конфиденциальность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля действий пользователей ОО и администраторов ОО, а также контроля процесса функционирования ОО в целом; навязывание администраторам ОО, ответственным за контроль данных аудита ОО, ложных (модифицированных) данных аудита; несанкционированное ознакомление о произошедших в ОО событиях.

Угроза-5

1. Аннотация угрозы – потеря данных аудита ОО вследствие переполнения выделенного для задач аудита хранилища информации.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – переполнение выделенного для задач аудита хранилища информации.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за переполнения хранилища данных аудита ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

Угроза-6

1. Аннотация угрозы – потеря данных аудита ОО вследствие исчерпания свободного дискового пространства.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – исчерпание свободного дискового пространства.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за исчерпания свободного дискового пространства.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

Угроза-7

1. Аннотация угрозы – осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к данным ФБО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным ФБО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

5. Вид активов, потенциально подверженных угрозе – данные ФБО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, доступность, достоверность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными ФБО (конфигурационные файлы, конфиденциальная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

Угроза-8

1. Аннотация угрозы – использование ресурсов ОО неуполномоченными на это субъектами.

2. Источники угрозы – субъекты, действующие от имени пользователей ОО и администраторов ОО.

3. Способ реализации угрозы – неограниченное использование свободных ресурсов ОО субъектами, действующими от имени пользователей ОО и администраторов ОО.

4. Используемые уязвимости – недостатки механизмов защиты ресурсов ОО, связанные с возможностью несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – ресурсы ОО.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

Г 3.2.2 Угрозы, которым противостоит среда

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

Угроза-9

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией ОО.

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем).

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в ОО.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией.

Угроза-10

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к ОО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация ОО.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией; невозможность однозначного сопоставления совершенных в ОО действий с субъектом, совершившим данные действия.

Угроза-11

1. Аннотация угрозы – использование ресурсов ОО неуполномоченными на использование субъектами в нарушение политики безопасности.

2. Источники угрозы – субъекты, действующие от имени пользователей ОО и администраторов ОО.

3. Способ реализации угрозы – неограниченное использование свободных ресурсов ОО субъектами, действующими от имени пользователей ОО и администраторов ОО.

4. Используемые уязвимости – недостатки механизмов защиты ресурсов ОО, связанные с возможностью несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – ресурсы ОО.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

Г 3.3 Политика безопасности объекта эксплуатации

Объект оценки должен следовать приведенным ниже правилам политики безопасности объекта эксплуатации.

Политика безопасности-1

Должны быть в наличии надлежащие корректно функционирующие средства администрирования, доступные только уполномоченным администраторам ОО.

Политика безопасности-2

Должны быть обеспечены надлежащая регистрация и предупреждение администратора ОО о любых событиях, относящихся к безопасности ОО. Должна быть обеспечена возможность для администратора ОО выборочного ознакомления с информацией о произошедших в ОО событиях.

Политика безопасности-3

Должна быть обеспечена возможность для уполномоченных администраторов ОО определять доступность объектов ОО для других пользователей ОО.

Политика безопасности-4

Должна быть обеспечена привязка по времени событий, подвергаемых аудиту.

Г 4 ЦЕЛИ БЕЗОПАСНОСТИ

Г 4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Разграничение доступа к объектам ОО

ОО должен обеспечивать доступ к объектам ОО только уполномоченным на это пользователям ОО. ОО должен обеспечивать возможность уполномоченным на это администраторам ОО определять доступность объектов ОО для других пользователей ОО.

Цель безопасности-2

Разграничение доступа к ОО

ОО должен обеспечивать доступ к ОО только уполномоченным на это пользователям.

Цель безопасности-3

Аудит событий

ОО должен располагать надлежащими механизмами регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации должны предоставлять администраторам ОО возможность выборочного ознакомления с информацией о произошедших в ОО событиях.

Цель безопасности-4

Защита данных аудита

ОО должен обеспечивать доступ к данным аудита только уполномоченным администраторам ОО и предотвращать потерю данных аудита в случае

переполнения их хранилища, а также в случае невозможности дальнейшего ведения аудита вследствие исчерпания свободного дискового пространства.

Цель безопасности-5

Наличие средств администрирования

ОО должен располагать надлежащими корректно функционирующими средствами администрирования, доступными только уполномоченным администраторам ОО.

Цель безопасности-6

Защита данных ФБО и ресурсов ОО

ОО должен обеспечивать защиту данных ФБО и ресурсов ОО, поддерживая домен для функционирования ФБО.

Г 4.2 Цели безопасности для среды

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

Цель для среды функционирования ОО-1

Доверительная среда функционирования

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Цель для среды функционирования ОО-2

Контролируемые точки доступа

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, т.е. охраняемой территории и помещении, оборудованной средствами и системами физической защиты и охраны

(контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-3

Взаимодействие с доверенными системами

Должно быть обеспечено взаимодействие ОО только с доверенными изделиями (системами) ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

Цель для среды функционирования ОО-4

Эксплуатация ОО

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Цель для среды функционирования ОО-5

Аутентификация с использованием механизмов ОС

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

Цель для среды функционирования ОО-6

Функция безопасности

Функционирование ОО должно осуществляться в среде функционирования, предоставляющей механизм аутентификации.

Цель для среды функционирования ОО-7

Физическая защита ОО

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-8

Требования к администраторам ОО

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

Цель для среды функционирования ОО-9

Требования к пользователям ОО

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

Цель для среды функционирования ОО-10

Защита данных ФБО и ресурсов ОО

Должна быть обеспечена защита данных ФБО и ресурсов ОО, а также поддержка домена для функционирования ФБО.

Цель для среды функционирования ОО-11

Поддержка аудита

Должна быть обеспечена поддержка средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

Цель для среды функционирования ОО-12

Восстановление ОО

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

Г 5 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ

В данном разделе ПЗ представлены требования безопасности ИТ, которым должен удовлетворять ОО и его среда. Функциональные требования, представленные в настоящем ПЗ, основаны на функциональных компонентах из части 2 РД БИТ. Требования доверия основаны на компонентах требований доверия из части 3 РД БИТ и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий».

Г 5.1 Требования безопасности для ОО

Г 5.1.1 Функциональные требования безопасности ОО

Функциональные компоненты из части 2 РД БИТ, на которых основаны функциональные требования безопасности ОО, приведены в таблице 5.1.

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.4	Предотвращение потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах

Идентификатор компонента требований	Название компонента требований
	безопасности
FIA_ATD.1	Определение атрибутов пользователя
FIA_UID.2	Идентификация до любых действий пользователя
FIA_USB.1	Связывание пользователь-субъект
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_REV.1	Отмена
FMT_SMR.1	Роли безопасности
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FTA_TSE.1	Открытие сеанса с ОО

Г 5.1.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

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

- а) запуск и завершение выполнения функций аудита;
- б) все события, потенциально подвергаемые аудиту, на неопределенном уровне аудита;
- в) [события, приведенные во втором столбце таблицы 5.2, а также [назначение: *другие специально определенные события, потенциально подвергаемые аудиту*]].

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

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

- б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ, [информацию, определенную в третьем столбце таблицы 5.2, а также **[назначение: другую относящуюся к аудиту информацию]]**].

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во время сбора данных аудита	
FAU_STG.3	Предпринимаемые действия после превышения порога заполнения журнала аудита	
FAU_STG.4	Факт останова ОО при отсутствии свободного дискового пространства для создания журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на именованном объекте, на который распространяется политика дискреционного управления доступом	Идентификатор объекта
FIA_UID.2	Все случаи использования механизма идентификации субъектов доступа	
FIA_USB.1	Факт создания пользователя	
FMT_MOF.1	Все модификации режима выполнения аудита	
FMT_MSA.1	Все модификации значений атрибутов безопасности, используемых в политике дискреционного управления доступом	
FMT_MSA.3	Модификации настройки по умолчанию	

Компонент	Событие	Детализация
	ограничительных правил, все модификации начальных значений атрибутов безопасности, которые используются для политики дискреционного управления доступом	
FMT_MTD.1	Все модификации значений данных ФБО	
FMT_REV.1 (1)	Все попытки отмены полномочий у пользователей ОО на доступ к объектам, отмены прав доступа к объекту (модификация списка дискреционного доступа)	
FMT_REV.1 (2)	Все попытки отмены прав доступа к объекту (модификация списка дискреционного доступа)	
FMT_SMR.1	Модификация множества администраторов ОО и пользователей ОО и других определенных ролей	
FTA_TSE.1	Все попытки открытия сеанса доступа к ОО со стороны субъектов	

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 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.2 «Идентификация до любых действий пользователя».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченному администратору ОО] возможность читать [всю информацию аудита] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **уполномоченному администратору ОО** 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 **уполномоченных администраторов ОО**, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны **предоставить** возможность выполнить поиск данных аудита, основанный на
[
 следующих критериях:
 а) тип события;
 б) [**назначение: другие критерии**]
].

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SEL.1 Избирательный аудит

FAU_SEL.1.1 ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой совокупности по следующим атрибутам:
а) тип события;
б) [**назначение: список дополнительных атрибутов, на которых основана избирательность аудита**].

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FMT_MTD.1 «Управление данными ФБО».

FAU_STG.1 Защищенное хранение журнала аудита

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

FAU_STG.1.2 ФБО должны быть способны предотвращать модификации записей 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, направленные на сохранение данных журнала аудита и обеспечивающие непрерывность процесса аудита*], если журнал аудита **превысит** [установленный уполномоченным администратором ОО размер].

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны игнорировать события, подвергающиеся аудиту и [назначение: *действия, направленные на невозможность совершения дальнейших событий, связанных с безопасностью ОО*] при **отсутствии свободного дискового пространства для создания журнала аудита.**

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

Замечание по применению:

Разработчиком ЗБ должны быть специфицированы действия, обеспечивающие, в случае отсутствия свободного дискового пространства для создания и ведения журнала аудита, невозможность совершения любых событий, связанных с безопасностью ОО. Примерами таких действий может служить временная приостановка функционирования ОО, полный останов ОО и т.п.

Г 5.1.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику информационного управления доступом] для
[
а) [назначение: список субъектов ОО], действующих от имени пользователей;
б) [назначение: список именованных объектов ОО];
в) всех операций между субъектами и объектами
].

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 дискреционного управления доступом] к объектам, основываясь на
[
следующем:
а) ассоциированные с субъектом идентификатор учетной записи пользователя, принадлежность к роли (ролям);
б) следующие, ассоциированные с объектами, атрибуты управления доступом: [назначение: список атрибутов управления доступом, которые должны обеспечить возможность:
 ♣ ассоциировать разрешение или запрет на выполнение операций с идентификаторами одного или более пользователей;
 ♣ ассоциировать разрешение или запрет на выполнение операций с идентификаторами одной или более ролей;
 ♣ ассоциировать разрешение или запрет на выполнение операций по умолчанию]

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[назначение: набор правил, определяющих политику дискреционного доступа, в которых:

- а) для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда идентификатор субъекта соответствует идентификатору, определенному в атрибутах контроля доступа объекта;*
- б) для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда субъект является участником роли, идентификатор которой, определен в атрибутах контроля доступа объекта;*
- в) для каждой операции должно быть определено правило или правила использования атрибутов разрешения по умолчанию в случаях, когда идентификатор субъекта не соответствует определенному в атрибутах контроля доступа объекта и субъект является участником роли, идентификатор которой, не определен в атрибутах контроля доступа объекта*

].

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».

Г 5.1.1.3 Идентификация и аутентификация (FIA)

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

- [
- а) идентификатор пользователя;
 - б) идентификатор роли, участником которой является пользователь;
 - в) [**назначение:** *другие атрибуты безопасности пользователя*]
-].

Зависимости: отсутствуют.

Замечание по применению:

Под пользователями в настоящем компоненте требований понимаются все идентифицированные в FMT_SMR.1 роли.

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый **субъект доступа** был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: отсутствуют.

FIA_USB.1 Связывание пользователь-субъект

FIA_USB.1.1 ФБО должны ассоциировать соответствующие атрибуты безопасности **субъекта доступа** с субъектами, действующими от имени этого **субъекта доступа**.

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

Г 5.1.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность определять режим выполнения, модифицировать режим выполнения функций, **связанных с:**

[

а) аудитом;

б) [назначение: *другие функции*]

]

только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предоставляющую** возможность модифицировать атрибуты безопасности, [перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1], только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предусматривающую** ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления **политики дискреционного управления доступом.**

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

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 [*выполнения операций, указанных во втором столбце таблицы 5.3, а также [назначение: другие операции]*] **над данными**, [указанными в третьем столбце таблицы 5.3, а также [назначение: *список других данных ФБО*]] только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.3 – Управляемые данные ФБО

Компонент	Операция	Данные ФБО
FAU_SAR.1	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих чтение записей аудита
FAU_STG.3	установление, модификация	размер журнала аудита
FIA_UID.2	создание, модификация, удаление	идентификационная информация пользователя
FMT_MOF.1	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих доступ к управлению режимами аудита
FMT_MSA.1	удаление, модификация, добавление	состав уполномоченных пользователей, являющихся участниками ролей, предусматривающих модификацию

Компонент	Операция	Данные ФБО
		атрибутов безопасности
FMT_MSA.3	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих модификацию начальных значений атрибутов безопасности
FMT_MTD.1	удаление, модификация, добавление	состав уполномоченных пользователей, являющихся участниками ролей, предусматривающих модификацию данных ФБО, определенных в настоящей таблице
FMT_REV.1 (1)	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих возможность отмены атрибутов безопасности, ассоциированных с пользователями и объектами
FMT_SMR.1	удаление, модификация, добавление	состав пользователей ОО, являющихся участниками ролей администратор ОО и пользователь ОО
FTA_TSE.1	установление, модификация	значение параметров, запрещающих установление соединения с ОО

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны **предоставлять** возможность отмены атрибутов безопасности, ассоциированных с **пользователями ОО и объектами**, в пределах ОДФ только [уполномоченному администратору ОО].

FMT_REV.1.2 ФБО должны **осуществлять следующие** правила:

[

- а) отмена полномочий у пользователей ОО на доступ к объектам должна вступать в силу при следующем сеансе работы пользователя ОО;
- б) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;
- в) [**назначение:** *другие правила отмены*]

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны **предоставлять** возможность отмены атрибутов безопасности, ассоциированных с **объектами**, в пределах ОДФ только [**назначение:** *пользователи, уполномоченные на изменение атрибутов безопасности в соответствии с политикой дискреционного управления доступом*].

FMT_REV.1.2 ФБО должны **осуществлять следующие** правила:

[

- а) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;
- б) [**назначение:** *другие правила отмены*]

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

[

а) администратор ОО;

б) пользователь ОО;

в) [**назначение:** *другие уполномоченные идентифицированные роли*]

].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать **субъектов доступа** с ролями.

Зависимости: FIA_UID.2 «Выбор момента идентификации».

Г 5.1.1.5 Защита ФБО (FPT)

FPT_RVM.1 (1) Невозможность обхода ПБО

FPT_RVM.1.1 ФБО должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 (1) Отделение домена ФБО

FPT_SEP.1.1 ФБО должны поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 ФБО должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

Г 5.1.1.6 Доступ к ОО (FTA)

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса **доступа к ОО**, основываясь на

[

следующих атрибутах:

а) идентификатор пользователя;

б) [назначение: *другие атрибуты*]

].

Зависимости: отсутствуют.

Г 5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 РД БИТ и образуют ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий» (см. таблицу 5.5).

Таблица 5.5 – Требования доверия к безопасности ОО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Управление конфигурацией	ACM_AUT.1	Частичная автоматизация УК
	ACM_CAP.4	Поддержка генерации, процедуры приемки
	ACM_SCP. 2	Охват УК отслеживания проблем
Поставка и эксплуатация	ADO_DEL.2	Обнаружение модификации
	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP. 2	Полностью определенные внешние интерфейсы
	ADV_HLD. 2	Детализация вопросов безопасности в проекте верхнего уровня
	ADV_IMP.1	Подмножество реализации ФБО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
	ADV_LLD.1	Описательный проект нижнего уровня
	ADV_RCR. 1	Неформальная демонстрация соответствия
	ADV_SPM. 1	Неформальная модель политики безопасности ОО
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Поддержка жизненного цикла	ALC_DVS.1	Идентификация мер безопасности
	ALC_FLR. 1	Базовое устранение недостатков
	ALC_LCD. 1	Определение модели жизненного цикла разработчиком
	ALC_TAT. 1	Полностью определенные инструментальные средства разработки
Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.1	Тестирование: проект верхнего уровня
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_MSU.2	Подтверждение правильности анализа
	AVA_SOF.1	Оценка стойкости функции безопасности ОО
	AVA_VLA. 3	Умеренно стойкий

Г 5.1.3 Управление конфигурацией (АСМ)

АСМ_AUT.1 Частичная автоматизация УК

Элементы действий разработчика

АСМ_AUT.1.1D Разработчик должен использовать систему УК.

АСМ_AUT.1.2D Разработчик должен представить план УК.

Элементы содержания и представления свидетельств

АСМ_AUT.1.1С Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО производятся только санкционированные изменения.

АСМ_AUT.1.2С Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.

АСМ_AUT.1.3С План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.

АСМ_AUT.1.4С План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.

Элементы действий оценщика

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

АСМ_CAP.4 Поддержка генерации, процедуры приемки

Элементы действий разработчика

АСМ_CAP.4.1D Разработчик должен предоставить маркировку для ОО.

АСМ_CAP.4.2D Разработчик должен использовать систему УК.

АСМ_CAP.4.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

АСМ_CAP.4.1С Маркировка ОО должна быть уникальна для каждой версии ОО.

АСМ_CAP.4.2С ОО должен быть помечен маркировкой.

АСМ_CAP.4.3С Документация УК должна включать в себя список конфигурации, план УК и план приемки.

АСМ_CAP.4.4С Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

АСМ_CAP.4.5С Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

АСМ_САР.4.6С Система УК должна уникально идентифицировать все элементы конфигурации.

АСМ_САР.4.7С План УК должен содержать описание, как используется система УК.

АСМ_САР.4.8С Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

АСМ_САР.4.9С Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

АСМ_САР.4.10С Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

АСМ_САР.4.11С Система УК должна поддерживать генерацию ОО.

АСМ_САР.4.12С План приемки должен содержать описание процедур, используемых для приемки модифицированного или вновь созданного элемента конфигурации как части ОО.

Элементы действий оценщика

АСМ_САР.4.1Е Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АСМ_SCP.2 Охват УК отслеживания проблем

Элементы действий разработчика

АСМ_SCP.3.1D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

АСМ_SCP.2.1С Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора, документацию УК и недостатки безопасности.

ACM_SCP.2.2C Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.

Элементы действий оценщика

ACM_SCP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

Г 5.1.4 Поставка и эксплуатация (ADO)

ADO_DEL.2 Обнаружение модификации

Элементы действий разработчика

ADO_DEL.2.1D Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

ADO_DEL.2.2 Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ADO_DEL.2.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий к местам использования.

ADO_DEL.2.2C Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.

ADO_DEL.2.3C Документация поставки должна содержать описание, как различные процедуры позволяют обнаружить попытку подмены от имени разработчика, даже в тех случаях, когда разработчик ничего не отсылал к месту использования.

Элементы действий оценщика

ADO_DEL.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

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

Г 5.1.5 Разработка (ADV)

ADV_FSP.2 Полностью определенные внешние интерфейсы

Элементы действий разработчика

ADV_FSP.2.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.2.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.2.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.2.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая **полную** детализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.2.4C Функциональная спецификация должна полностью представить ФБО.

ADV_FSP.2.5C Функциональная спецификация должна включать в себя логическое обоснование, что ФБО полностью представлены.

Элементы действий оценщика

ADV_FSP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.2.2E Оценщик должен сделать независимое заключение, что функциональная спецификация - точное и полное отображение функциональных требований безопасности ОО.

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

Элементы действий разработчика

ADV_HLD.3.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.2.1C Представление проекта верхнего уровня должно быть неформальным.

ADV_HLD.2.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.2.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.2.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.2.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.2.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.2.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.2.8C Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_HLD.2.9C Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

Элементы действий оценщика

ADV_HLD.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.2.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня - точное и полное отображение функциональных требований безопасности ОО.

ADV_IMP.1 Подмножество реализации ФБО

Элементы действий разработчика

ADV_IMP.1.1D Разработчик должен обеспечить представление реализации для выбранного подмножества ФБО.

Элементы содержания и представления свидетельств

ADV_IMP.1.1C Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.

ADV_IMP.1.2C Представление реализации должно быть внутренне непротиворечивым.

Элементы действий оценщика

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

ADV_IMP.1.2E Оценщик должен сделать независимое заключение, что наименее абстрактное представление ФБО – точное и полное отображение функциональных требований безопасности ОО.

ADV_LLD.1 Описательный проект нижнего уровня

Элементы действий разработчика

ADV_LLD.1.1D Разработчик должен представить проект нижнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_LLD.1.1C Представление проекта нижнего уровня должно быть неформальным.

ADV_LLD.1.2C Проект нижнего уровня должен быть внутренне непротиворечивым.

ADV_LLD.1.3C Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

ADV_LLD.1.4C Проект нижнего уровня должен содержать описание назначения каждого модуля.

ADV_LLD.1.5C Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

ADV_LLD.1.6C Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.

ADV_LLD.1.7C Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

ADV_LLD.1.8C Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

ADV_LLD.1.9C Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя, при необходимости, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_LLD.1.10C Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

Элементы действий оценщика

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

ADV_LLD.1.2E Оценщик должен сделать независимое заключение, что проект нижнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

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

ADV_SPM.1 Неформальная модель политики безопасности ОО

Элементы действий разработчика

ADV_SPM.1.1D Разработчик должен представить модель ПБО.

ADV_SPM.1.2D Разработчик должен демонстрировать или доказать, где это требуется, соответствие между функциональной спецификацией и моделью ПБО.

Элементы содержания и представления свидетельств

ADV_SPM.1.1C Модель ПБО должна быть неформальной.

ADV_SPM.1.2C Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.1.3C Модель ПБО должна включать в себя логическое обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.1.4C Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.

Элементы действий оценщика

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

Г 5.1.6 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

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

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

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

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

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

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

Элементы действий оценщика

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

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

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

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

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

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

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

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

Элементы действий оценщика

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

Г 5.1.7 Поддержка жизненного цикла (ALC)

ALC_DVS.1 Идентификация мер безопасности

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

ALC_DVS.1.2C Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.

Элементы действий оценщика

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

ALC_DVS.1.2E Оценщик должен подтвердить применение мер безопасности.

ALC_FLR.1 Базовое устранение недостатков

Элементы действий разработчика

ALC_FLR.1.1D Разработчик должен задокументировать процедуры устранения недостатков.

Элементы содержания и представления свидетельств

ALC_FLR.1.1C Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждой редакции ОО.

ALC_FLR.1.2C Процедуры устранения недостатков должны содержать требование представления описания природы и проявлений каждого недостатка безопасности, а также статуса завершения исправления этого недостатка.

ALC_FLR.1.3C Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

ALC_FLR.1.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

Элементы действий оценщика

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

ALC_LCD.1 Определение модели жизненного цикла разработчиком

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 свидетельств

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

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

Элементы действий оценщика

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

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Элементы действий разработчика

ALC_TAT.1.1D Разработчик должен идентифицировать инструментальные средства разработки ОО.

ALC_TAT.1.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.

Элементы содержания и представления свидетельств

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

ALC_TAT.1.2C Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

ALC_TAT.1.3C Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.

Элементы действий оценщика

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

Г 5.1.8 Тестирование (АТЕ)

АТЕ_COV.2 Анализ покрытия

Элементы действий разработчика

АТЕ_COV.2.1D Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

АТЕ_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

АТЕ_COV.2.2C Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.

Элементы действий оценщика

АТЕ_COV.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АТЕ_DPT.1 Тестирование: проект верхнего уровня

Элементы действий разработчика

АТЕ_DPT.1.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

АТЕ_DPT.1.1C Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня.

Элементы действий оценщика

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

ATE_FUN.1 Функциональное тестирование

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 свидетельств

ATE_FUN.1.1C Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.

ATE_FUN.1.2C Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей тестирования.

ATE_FUN.1.3C Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.

ATE_FUN.1.4C Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.

ATE_FUN.1.5C Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.

Элементы действий оценщика

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

ATE_IND.2 Выборочное независимое тестирование

Элементы действий разработчика

ATE_IND.2.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

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 представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.2.2E Оценщик должен протестировать подмножество ФБО, **как необходимо**, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

ATE_IND.2.3E Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

Г 5.1.9 Оценка уязвимостей (AVA)

AVA_MSU.2 Подтверждение правильности анализа

Элементы действий разработчика

AVA_MSU.2.1D Разработчик должен представить руководства по применению ОО.

AVA_MSU.2.2D Разработчик должен задокументировать анализ руководств.

Элементы содержания и представления свидетельств

AVA_MSU.2.1C Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.2.2C Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

AVA_MSU.2.3C Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.2.4C Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

AVA_MSU.2.5C Документация анализа должна демонстрировать, что руководства полны.

Элементы действий оценщика

AVA_MSU.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_MSU.2.2E Оценщик должен повторить все процедуры конфигурирования и установки и выборочно другие процедуры для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

AVA_MSU.2.3E Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

AVA_MSU.2.4E Оценщик должен подтвердить, что документация анализа показывает обеспечение руководствами безопасного функционирования во всех режимах эксплуатации ОО.

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

AVA_SOF.1.1C Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее

стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.

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

Элементы действий оценщика

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

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

AVA_VLA.3 Умеренно стойкий

Элементы действий разработчика

AVA_VLA.3.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску путей, которыми пользователь может нарушить ПБО.

AVA_VLA.3.2D Разработчик должен задокументировать местоположение идентифицированных уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.3.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.3.2C Документация должна содержать строгое обоснование, что ОО с идентифицированными уязвимостями является стойким к явным нападениям проникновения.

AVA_VLA.3.3C Свидетельство должно показать, что поиск уязвимостей является систематическим.

Элементы действий оценщика

- AVA_VLA.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
- AVA_VLA.3.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.
- AVA_VLA.3.3E Оценщик должен выполнить независимый анализ уязвимостей.
- AVA_VLA.3.4E Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.
- AVA_VLA.3.5E Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим **умеренным** потенциалом нападения.

Г 5.2 Требования безопасности для среды ИТ

Функцией безопасности, реализуемой средой ИТ в интересах обеспечения безопасности ОО, является функция безопасности «Аутентификация». Данная функция реализуется механизмом паролей среды ИТ. Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости.

Функциональные компоненты из части 2 РД БИТ, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.5.

Таблица 5.6 – Функциональные компоненты, на которых основаны ФТБ среды ИТ

Идентификатор компонента требований	Название компонента требований
FIA_AFL.1	Обработка отказов аутентификации
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FPT_RVM.1 (2)	Невозможность обхода ПБО
FPT_SEP.1 (2)	Отделение домена ФБО
FPT_STM.1	Надежные метки времени

Г 5.2.1 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

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

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

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

Замечание по применению:

Конкретизация данного требования совместно с требованием FIA_SOS.1 в ЗБ должна обеспечивать возможность для механизмов безопасности, реализующих функции безопасности «Аутентификация», предоставлять адекватную защиту от нарушения безопасности ОО нарушителем с низким потенциалом нападения.

FIA_SOS.1 Верификация секретов

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

Зависимости: отсутствуют.

Замечание по применению:

Конкретизация данного требования совместно с требованием FIA_AFL.1 в ЗБ должна обеспечивать возможность для механизмов безопасности, реализующих функции безопасности «Аутентификация», предоставлять адекватную защиту от нарушения безопасности ОО нарушителем с низким потенциалом нападения.

FIA_UAU.2 Аутентификация до любых действий пользователя

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

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

Г 5.2.2 Защита ФБО (FPT)

FPT_RVM.1 (2) Невозможность обхода ПБО

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

Зависимости: отсутствуют.

FPT_SEP.1 (2) Отделение домена ФБО

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

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

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 Функции безопасности среды ИТ должны быть способны предоставить надежные метки времени для **использования ФБО**.

Зависимости: отсутствуют.

Г 6 ОБОСНОВАНИЕ

В данном разделе дано обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ПЗ. В разделе «Обоснование» также демонстрируется справедливость утверждений о СФБ.

Г 6.1 Обоснование целей безопасности

Г 6.1.1 Обоснование целей безопасности для ОО

В таблице 6.1 приведено отображение целей безопасности на угрозы и политику безопасности объекта эксплуатации.

Таблица 6.1 – Отображение целей безопасности на угрозы и политику безопасности объекта эксплуатации

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

Цель безопасности-1

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1**, и реализацией политики безопасности организации **Политика безопасности-3**, так как обеспечивает доступ к объектам ОО только уполномоченным пользователям ОО, а также обеспечивает возможность уполномоченным пользователям ОО определять доступность объектов ОО для других пользователей ОО.

Цель безопасности-2

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-2** и **Угроза-3**, так как обеспечивает доступ к ОО только уполномоченным на это пользователям.

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-2**, так как обеспечивает наличие надлежащих механизмов регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации предоставляют администраторам ОО возможность выборочного ознакомления с информацией о произошедших в ОО событиях.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-4**, **Угроза-5** и **Угроза-6**, так как обеспечивает доступ к данным аудита только уполномоченным администраторам ОО и предотвращает потерю данных аудита в случае переполнения их хранилища, а также в случае невозможности дальнейшего ведения аудита вследствие исчерпания свободного дискового пространства.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-1**, так как обеспечивает наличие надлежащих корректно функционирующих средств администрирования, доступных только уполномоченным администраторам ОО.

Цель безопасности-6

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-7** и **Угроза-8**, так как обеспечивает защиту данных ФБО и ресурсов ОО, поддерживая домен для функционирования ФБО.

Г 6.1.2 Обоснование целей безопасности для среды

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

Таблица 6.2 – Отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности объекта эксплуатации

	Цель для среды функционирования ОО-	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования	Цель для среды функционирования
Предположение-1	X											
Предположение-2		X										
Предположение-3			X									
Предположение-4				X								
Предположение-5	2.1.				X							
Предположение-6						X						
Предположение-7												X
Предположение-8							X					
Предположение-9								X				
Предположение-10									X			
Угроза-9					X							
Угроза-10					X							
Угроза-11										X		
Политика безопасности-4											X	

Цель для среды функционирования ОО-1

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-1**, так как обеспечивает отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Цель для среды функционирования ОО-2

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-2**, так как обеспечивает осуществление доступа к ОО только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-3

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-3**, так как обеспечивает взаимодействие ОО только с доверенными системами ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-4**, так как обеспечивает установку конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-5** и противостояния угрозам **Угроза-9** и **Угроза-10**, так как обеспечивает осуществление аутентификации

субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов ОС, под управлением которой функционирует ОО.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-6**, так как обеспечивает осуществление функционирования ОО в среде функционирования, предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от нарушения безопасности ОО нарушителями с низким потенциалом нападения.

Цель для среды функционирования ОО-7

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-8**, так как обеспечивает, для предотвращения несанкционированного физического доступа, размещение компьютера с установленным ОО в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-8

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-9**, так как обеспечивает прохождение персоналом, ответственным за администрирование ОО, проверок на благонадежность и компетентность, а также деятельность согласно соответствующей документации.

Цель для среды функционирования ОО-9

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-10**, так как обеспечивает прохождение уполномоченными на доступ к ОО пользователями проверок на

благонадежность, а их совместные действия направлены исключительно на выполнение своих функциональных обязанностей.

Цель для среды функционирования ОО-10

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-11**, так как обеспечивает защиту данных ФБО и ресурсов ОО, а также поддержку домена для функционирования ФБО.

Цель для среды функционирования ОО-11

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-4**, так как обеспечивает поддержку средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

Цель для среды функционирования ОО-12

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-7**, так как обеспечивает выполнение мероприятий, направленных на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

Г 6.2 Обоснование требований безопасности

Г 6.2.1 Обоснование требований безопасности для ОО

Г 6.2.1.1 Обоснование функциональных требований безопасности ОО

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

Таблица 6.3 – Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6
FAU_GEN.1			X			
FAU_GEN.2			X			
FAU_SAR.1			X			
FAU_SAR.2				X		
FAU_SAR.3			X			
FAU_SEL.1			X			
FAU_STG.1				X		
FAU_STG.3				X		
FAU_STG.4				X		
FDP_ACC.1	X					
FDP_ACF.1	X					
FIA_ATD.1	X	X	X		X	
FIA_UID.2	X	X				
FIA_USB.1	X	X	X			
FMT_MOF.1					X	
FMT_MSA.1	X				X	
FMT_MSA.3	X				X	
FMT_MTD.1					X	
FMT_REV.1 (1)					X	
FMT_REV.1 (2)	X					
FMT_SMR.1	X			X	X	X
FPT_RVM.1 (1)						X
FPT_SEP.1 (1)						X
FTA_TSE.1		X				

FAU_GEN.1

Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_GEN.2

Ассоциация идентификатора пользователя

Выполнение требований данного компонента обеспечивает возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.1

Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления уполномоченным администраторам ОО всей информации аудита в понятном для него виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.2

Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает запрет всем пользователям доступ к чтению записей аудита, за исключением уполномоченных администраторов ОО, которым явно предоставлен доступ для чтения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_SAR.3

Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает выполнение поиска данных аудита, основанного на определенных критериях (тип события).

Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SEL.1 Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, уполномоченным администратором ОО по таким атрибутам, как тип события. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает защиту хранимых записей аудита от несанкционированного удаления и предотвращает модификацию записей аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_STG.3 Действия в случае возможной потери данных аудита

Выполнение требований данного компонента обеспечивает выполнение действий, направленных на сохранение данных журнала аудита и обеспечивающих непрерывность процесса аудирования, если журнал аудита превысит установленный уполномоченным администратором ОО размер. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает игнорирование событий, подвергающихся аудиту, и выполнение действий, направленных на невозможность совершения дальнейших событий, связанных с безопасностью ОО при отсутствии свободного дискового пространства для создания журнала аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FDP_ACC.1**Ограниченное управление доступом**

Выполнение требований данного компонента обеспечивает реализацию политики дискреционного доступа для субъектов, именованных объектов и всех операций между субъектами и объектами. 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 осуществление политики дискреционного доступа, основываясь на атрибутах безопасности, определении правил доступа субъектов к объектам. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_ATD.1**Определение атрибутов пользователя**

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя (пользователя ОО и администратора ОО) в качестве атрибутов безопасности идентификатора пользователя, идентификатора роли, участником которой является пользователь, а также других атрибутов безопасности. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3, Цель безопасности-5** и способствует их достижению.

FIA_UID.2**Идентификация до любых действий пользователя**

Выполнение требований данного компонента обеспечивает выполнение идентификации субъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2** и способствует их достижению.

FIA_USB.1 Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами, действующими от имени этого субъекта доступа. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3** и способствует их достижению.

FMT_MOF.1 Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает модификацию и определение режимов выполнения функций, связанных с аудитом, только уполномоченному администратору ОО, предусмотрена возможность определения других функций. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-5** и способствует их достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом, и возможность для уполномоченных идентифицированных ролей определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-5** и способствует их достижению.

FMT_MTD.1

Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации определенных данных ФБО только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** по достижению.

FMT_REV.1 (1) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО и объектами, в пределах ОДФ только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_REV.1 (2) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с объектами, в пределах ОДФ только пользователям, уполномоченным на изменение атрибутов безопасности в соответствии с политикой дискреционного управления доступом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_SMR.1

Роли безопасности

Данный компонент включен в ПЗ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту ролей администратора ОО и пользователя ОО, предусмотрена возможность определения других уполномоченных идентифицированных ролей. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-4, Цель безопасности-5, Цель безопасности-6** и способствует их достижению.

FPT_RVM.1 (1) Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FPT_SEP.1 (1) Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FTA_TSE.1 Открытие сеанса с ОО

Выполнение требований данного компонента обеспечивает способность отказа ОО в открытии сеанса доступа к ОО, основываясь на идентификаторе пользователя, предусмотрена возможность определения других атрибутов. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

Г 6.2.1.2 Обоснование требований доверия к безопасности ОО

Включение в настоящий ПЗ ОУД4, усиленный компонентом ALC_FLR.1 «Базовое устранение недостатков» AVA_VLA.3 «Умеренно стойкий», является достаточным при определении допустимости использования ОО в информационных системах, в которых обрабатывается информация ограниченного доступа.

Г 6.2.2 Обоснование требований безопасности для среды ИТ

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

Таблица 6.4 – Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11
FIA_AFL.1	X		
FIA_SOS.1	X		
FIA_UAU.2	X		
FPT_RVM.1 (2)		X	
FPT_SEP.1 (2)		X	
FPT_STM.1			X

FIA_AFL.1 Обработка отказов аутентификации

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

компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает верификацию качества паролей на доступ к ОО. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа к ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FPT_RVM.1 (2) Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-10** и способствует ее достижению.

FPT_SEP.1 (2) Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-10** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ПЗ для удовлетворения зависимости компонента FAU_GEN.1 от наличия в записях аудита точного указания даты и времени. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-11** и способствует ее достижению.

Г 6.2.3 Обоснование зависимостей требований

В таблице 6.5 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворены в настоящем ПЗ либо включением компонентов, определенных в части 2 РД БИТ под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в части 2 РД БИТ под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 6.5 является справочным и содержит компоненты, определенные в части 2 РД БИТ в описании компонентов требований, приведенных в столбце 1 таблицы 6.5, под рубрикой «Зависимости».

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

Таблица 6.5 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по РД БИТ	Удовлетворение зависимостей
Зависимости функциональных требований ОО		
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2

Функциональные компоненты	Зависимости по РД БИТ	Удовлетворение зависимостей
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.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
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (1)	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
Зависимости функциональных требований среды ИТ		
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2

ПРИЛОЖЕНИЕ Д

(обязательное)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ИЗДЕЛИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ – ЧЕТВЕРТЫЙ

Профиль защиты

ИЗД_ИТ.СУБД.ОУД4.ПЗ

Версия 1.0

СОДЕРЖАНИЕ

Д 1	Введение ПЗ	303
Д 1.1	Идентификация ПЗ.....	303
Д 1.2	Аннотация ПЗ	304
Д 1.3	Соглашения.....	305
Д 1.4	Термины и определения.....	306
Д 1.5	Организация ПЗ.....	308
Д 2	Описание ОО	310
Д 2.1	Тип изделия ИТ	310
Д 2.2	Основные функциональные возможности ОО	310
Д 3	Среда безопасности ОО	314
Д 3.1	Предположения безопасности	314
Д 3.2	Угрозы.....	316
Д 3.3	Политика безопасности объекта эксплуатации	324
Д 4	Цели безопасности	325
Д 4.1	Цели безопасности для ОО	325
Д 4.2	Цели безопасности для среды.....	326
Д 5	Требования безопасности ИТ	330
Д 5.1	Требования безопасности для ОО	330
Д 5.2	Требования безопасности для среды ИТ.....	365
Д 6	Обоснование	369
Д 6.1	Обоснование целей безопасности	369
Д 6.2	Обоснование требований безопасности	376

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БИТ	– безопасность информационных технологий
БД	- база данных
ЗБ	– задание по безопасности
ИС	- информационная система
ИТ	– информационная технология
НСД	– несанкционированный доступ
ОДФ	– область действия функции безопасности объекта оценки
ОО	– объект оценки
ОУД	– оценочный уровень доверия
ПБО	– политика безопасности объекта оценки
ПЗ	– профиль защиты
ПФБ	– политика функции безопасности
УК	– управление конфигурацией
ФБО	– функции безопасности объекта оценки
ФТБ	– функциональные требования безопасности

Д 1 ВВЕДЕНИЕ ПЗ

Данный раздел содержит информацию общего характера. Подраздел «Идентификация ПЗ» предоставляет маркировку и описательную информацию, которые необходимы, чтобы идентифицировать, каталогизировать ПЗ и ссылаться на него. Подраздел «Аннотация ПЗ» содержит общую характеристику ПЗ. В подразделе «Соглашения» дается описание операций конкретизации компонентов требований безопасности ИТ. В подразделе «Термины и определения» представлены определения основных терминов, специфичных для настоящего ПЗ. В подразделе «Организация ПЗ» дается пояснение организации документа.

Д 1.1 Идентификация ПЗ

Название ПЗ:	Безопасность информационных технологий. Изделия информационных технологий. Системы управления базами данных. Оценочный уровень доверия – четвертый. Профиль защиты.
Семейство ПЗ:	Изделия ИТ.
Функциональная группа:	Системы управления базами данных.
Версия ПЗ:	Версия 1.0.
Обозначение ПЗ:	ИЗД_ИТ.СУБД.ОУД4.ПЗ.
Идентификация ОО:	Системы управления базами данных.
Уровень доверия:	ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий».

Идентификация РД БИТ:

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 1: Введение и общая модель, ФСТЭК (Гостехкомиссия) России, 2002.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 2: Функциональные требования безопасности, ФСТЭК (Гостехкомиссия) России, 2002.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.

Часть 3: Требования доверия к безопасности, ФСТЭК (Гостехкомиссия) России, 2002.

Ключевые слова:

Система управления базами данных, средство защиты информации, дискреционное управление доступом, ИС, профиль защиты, ОУД4.

Д 1.2 Аннотация ПЗ

Настоящий ПЗ определяет требования безопасности для систем управления базами данных (далее – объект оценки).

Объект оценки представляет собой полнофункциональную реляционную систему управления базами данных, обеспечивающую надежную инфраструктурную платформу высокой производительности для создания, развертывания и поддержки производственных баз данных. Реляционное ядро ОО

обеспечивает достоверность и защиту хранимых в реляционных таблицах данных, отказоустойчивость и динамическую оптимизацию производительности системы. Предполагается функционирование ОО под управлением ОС.

Системы управления базами данных, соответствующие настоящему профилю защиты, могут использоваться в информационных системах, обрабатывающих конфиденциальную информацию.

Д 1.3 Соглашения

Руководящий документ ФСТЭК (Гостехкомиссии) России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (далее – Общие критерии) допускает выполнение определенных в части 2 РД БИТ операций над функциональными требованиями. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор», «назначение» и «итерация».

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

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

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

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

В настоящем ПЗ используются компоненты функциональных требований безопасности, включающие незавершенные операции **«назначение»** в которых область предполагаемых значений уточнена по отношению к исходному компоненту из части 2 РД БИТ. В данных компонентах операции **«назначения»** с уточненной областью предполагаемых значений обозначаются как [назначение: *уточненная область предполагаемых значений*].

Операция **«итерация»** используется для более чем однократного использования компонента функциональных требований безопасности ИТ при различном выполнении разрешенных операций (уточнение, выбор, назначение). Выполнение «итерации» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

Замечания по применению предназначены либо для разъяснения назначения некоторого требования, идентификации вариантов реализации, либо для определения условий выполнения требования. В случае использования, замечания по применению следуют за компонентом требования.

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

Д 1.4 Термины и определения

В настоящем ПЗ применяются следующие термины с соответствующими определениями.

Информационная система: Система, состоящая из персонала и комплекса изделий ИТ, обеспечивающая автоматизацию функционирования определенных структурных элементов.

Активы: Информация или ресурсы ОО, подлежащие защите контрмерами ОО.

Аутентификационные данные: Информация, используемая для

верификации предъявленного идентификатора.

Аутентификация: Процесс установления подлинности информации, предъявленной администратором ОО или пользователем ОО при регистрации.

Данные ФБО: Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО.

Доступность: Состояние безопасности активов (информации), характеризующее их готовностью к использованию по запросу уполномоченных лиц, объектов или субъектов, а также возможностью их восстановления в случае сбоя (отказа).

Задание по безопасности: Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО.

Конфиденциальность: Характеристика безопасности активов, связанная с предотвращением возможности доступа к информации и/или ее раскрытия неуполномоченным лицам, объектам или процессам.

Область действия ФБО: Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО.

Объект оценки: Подлежащие оценке изделие ИТ (в данном случае – СУБД) с руководствами по эксплуатации.

Политика безопасности объекта эксплуатации: Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

Политика безопасности ОО: Совокупность правил, определяющих режим обеспечения безопасности ОО и представляемых в виде набора функциональных требований безопасности.

Политика функции безопасности: Политика безопасности, осуществляемая ФБ.

Пользователь: Любая сущность (человек-пользователь или внешний

объект изделия ИТ) вне ОО, которая взаимодействует с ОО.

Изделие ИТ: Программное, программно-аппаратное или аппаратное обеспечение изделий ИТ, специально разработанное для использования в составе ИС.

Профиль защиты: Совокупность требований безопасности для некоторого типа изделий ИТ.

Уполномоченный администратор: Уполномоченный пользователь, ответственный за эксплуатацию ОО.

Функция безопасности: Функциональные возможности части или частей ИС или изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных функциональных требований безопасности.

Целостность: Состояние безопасности активов (информации), характеризующее их полнотой и защищенностью от несанкционированного изменения (модификации).

Д 1.5 Организация ПЗ

Раздел 1 «Введение ПЗ» содержит информацию управления документооборотом и обзорную информацию, необходимую для идентификации ПЗ и работы с реестром ПЗ.

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

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

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

В разделе 5 «Требования безопасности ИТ» на основе частей 2 и 3 РД БИТ определены, соответственно, функциональные требования безопасности ИТ и требования доверия к безопасности.

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

Д 2 ОПИСАНИЕ ОО

Объектом оценки в настоящем ПЗ является система управления базами данных.

Д 2.1 Тип изделия ИТ

Объект оценки представляет собой систему управления базами данных, обеспечивающую надежную инфраструктурную платформу высокой производительности для создания, развертывания и поддержки баз данных. ОО обеспечивает достоверность и защиту хранимых данных. Предполагается функционирование ОО под управлением ОС.

Д 2.2 Основные функциональные возможности ОО

В ОО должен быть реализован ряд функциональных возможностей и средств, позволяющих обеспечить безопасность ИТ, надежность ОО, а также упрощающих администрирование ОО и управление вычислительной средой ОО. В данном подразделе представлено краткое описание предполагаемых функциональных возможностей и средств.

ОО должен содержать следующие основные программные компоненты:

- сервер системы управления базами данных;
- средство интерактивной работы с системой управления базами данных;
- прикладные библиотеки доступа к системе управления базами данных для различных языков программирования;

Д 2.2.1 Основные функциональные возможности

Объект оценки должен характеризоваться как управляемая, надежная и безопасная система, что должно достигаться за счет таких возможностей

обеспечения безопасности, как использование единых регистрационных данных пользователя при доступе к ОС и к ОО, аудит событий безопасности, управление ролями, дискреционное управление доступом.

ОО должен поддерживать следующий функционал:

- поддержка масштабируемых геоинформационных систем (ГИС), в частности:

- поиск ближайших соседей для различных типов данных;
- поиск и хранения объектов со сферическими атрибутами;
- гибкая система полнотекстового поиска со встроенной поддержкой русского языка с поддержкой поиска фраз;

- поиск похожих строк (поиск с опечатками);
- поиск похожих объектов;
- хранение и поиск слабо-структурированной информации;
- поддержка мандатной политики доступа применительно ко всем объектам СУБД (таблицам, колонкам, записям) и интеграция с системой безопасности операционной системы для обеспечения целостности системы безопасности независимо от системы авторизации СУБД;

- поддержка ролевой системы политики доступа к объектам СУБД;
- поддержка работы по защищенным (шифрованным) соединениям;
- поддержка гибкой системы аутентификации (на основе GSSAPI, SSPI, LDAP, PAM, Kerberos, Ident);

- поддержка шифрования объектов СУБД для защиты информации от несанкционированного использования;

- поддержка разработки новых пользовательских типов данных и запросов с эффективными методами доступа и их использование без остановки сервера НСУБД;

- локализация программного обеспечения - перевод сообщений на русский язык.

Д 2.2.2 Аудит событий безопасности

Объект оценки должен обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в среде разработки. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к ОО или доступа к защищаемым активам. В частности, определяя политику аудита, уполномоченный администратор ОО должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как создание и удаление учётных записей ОО (привязки пользователей к ролям) или неудачные попытки подключения пользователей к ОО. Запись результатов аудита событий безопасности должна осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору ОО. Просмотр журналов регистрации событий аудита должен выполняться с использованием средств ОО (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

Д 2.2.3 Дискреционное управление доступом

В ОО доступ к защищаемым активам должен быть разрешен только уполномоченным на это пользователям ОО. Модель защиты ОО должна включать компоненты, которые реализуют контроль субъектов доступа и действий, предпринимаемых конкретным субъектом по отношению к объекту доступа.

Каждый пользователь, осуществляющий взаимодействие с ОО, должен быть представлен в нем регистрационной записью, определяющей сущностей, имеющих право доступа к ОО и используемой ОО при управлении доступом как к данным ОО, так и его объектам. Для ОО должна поддерживаться таблица (список

дискреционного управления доступом), в которой определены права доступа к объектам ОО. Список дискреционного управления доступом должен включать перечень пользователей (ролей), которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

Д 2.2.4 Управление ролями

Использование ролей упрощает управление доступом к защищаемым активам, позволяя назначать разрешения и права группе пользователей, а не отдельной учетной записи. Таким образом, исходя из потребностей в доступе к новым активам, пользователь ОО может быть включен в состав участников определенной роли или исключен из участия в указанной роли.

Объект оценки должен поддерживать ряд предопределенных ролей. Помимо предопределенных ролей в ОО должна быть предусмотрена возможность создания и дальнейшего использования ролей, определяемых пользователями ОО, которые позволяют устанавливать специфичные для конкретной группы пользователей ОО права доступа при работе с ОО.

Д 2.2.5 Основные функциональные возможности повышения надежности

Объект оценки должен обеспечивать надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

Д 2.2.6 Средства администрирования, управления и поддержки

В состав ОО должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг) как ОО, так и БД, находящимися под управлением ОО.

Д 3 СРЕДА БЕЗОПАСНОСТИ ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

- предположений относительно предопределенного использования ОО и аспектов безопасности среды ОО;
- угроз безопасности, которым нужно противостоять средствами ОО;
- политики безопасности объекта эксплуатации, которой должен следовать ОО.

Д 3.1 Предположения безопасности

Д 3.1.1 Предположения относительно предопределенного использования ОО

Предположение-1

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Предположение-2

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположение-3

Должно быть обеспечено взаимодействие ОО только с доверенными изделиями (системами) ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

Предположение-4

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Предположение-5

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

Предположение-6

Функционирование ОО должно осуществляться в среде функционирования, предоставляющей механизм аутентификации.

Предположение-7

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

Д 3.1.2 Предположения относительно среды функционирования ОО

Предположение, связанное с физической защитой ОО

Предположение-8

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположения, имеющие отношение к персоналу

Предположение-9

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

Предположение-10

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

Д 3.2 Угрозы

Д 3.2.1 Угрозы, которым противостоит ОО

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

Угроза-1

1. Аннотация угрозы – осуществление доступа к информации, размещаемой на объектах ОО, неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к информации, размещаемой на объектах ОО, с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к объектам ОО, связанные с возможностью предоставления доступа к информации, размещаемой на объектах ОО, неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – информация, размещаемая на объектах ОО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, достоверность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, размещаемой на объектах ОО; несанкционированная модификация информации (в том числе подмена), размещаемой на объектах ОО; несанкционированное удаление информации, размещаемой на объектах ОО.

Угроза-2

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся в БД.

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем (в т.ч. СУБД)).

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией, хранящейся в БД.

Угроза-3

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к ОО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией, хранящейся в БД; невозможность однозначного сопоставления совершенных в ОО действий с субъектом, совершившим данные действия.

Угроза-4

1. Аннотация угрозы – осуществление доступа к данным аудита ОО пользователями ОО и неуполномоченными на это администраторами ОО и возможность несанкционированного удаления и модификации данных аудита ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способы реализации угрозы – осуществление доступа к данным аудита ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным аудита с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к данным аудита, связанные с возможностью осуществления доступа к данным аудита пользователями ОО и неуполномоченными на это администраторами ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – подконтрольность, целостность, конфиденциальность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля действий пользователей ОО и администраторов ОО, а

также контроля процесса функционирования ОО в целом; навязывание администраторам ОО, ответственным за контроль данных аудита ОО, ложных (модифицированных) данных аудита; несанкционированное ознакомление о произошедших в ОО событиях.

Угроза-5

1. Аннотация угрозы – потеря данных аудита ОО вследствие переполнения выделенного для задач аудита хранилища информации.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – переполнение выделенного для задач аудита хранилища информации.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за переполнения хранилища данных аудита ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

Угроза-6

1. Аннотация угрозы – потеря данных аудита ОО вследствие исчерпания свободного дискового пространства.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – исчерпание свободного дискового пространства.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за исчерпания свободного дискового пространства.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

Угроза-7

1. Аннотация угрозы – осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к данным ФБО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным ФБО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

5. Вид активов, потенциально подверженных угрозе – данные ФБО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, доступность, достоверность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными ФБО (конфигурационные файлы, конфиденциальная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

Угроза-8

1. Аннотация угрозы – использование ресурсов ОО неуполномоченными на это субъектами.

2. Источники угрозы – субъекты, действующие от имени пользователей ОО и администраторов ОО.

3. Способ реализации угрозы – неограниченное использование свободных ресурсов ОО субъектами, действующими от имени пользователей ОО и администраторов ОО.

4. Используемые уязвимости – недостатки механизмов защиты ресурсов ОО, связанные с возможностью несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – ресурсы ОО.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

Д 3.2.2 Угрозы, которым противостоит среда

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

Угроза-9

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся в БД.

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем (в т.ч. СУБД)).

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией.

Угроза-10

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к ОО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией; невозможность однозначного сопоставления совершенных в ОО действий с субъектом, совершившим данные действия.

Угроза-11

1. Аннотация угрозы – использование ресурсов ОО неуполномоченными на использование субъектами в нарушение политики безопасности.

2. Источники угрозы – субъекты, действующие от имени пользователей ОО и администраторов ОО.

3. Способ реализации угрозы – неограниченное использование свободных ресурсов ОО субъектами, действующими от имени пользователей ОО и администраторов ОО.

4. Используемые уязвимости – недостатки механизмов защиты ресурсов ОО, связанные с возможностью несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – ресурсы ОО.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

Угроза-12

1. Аннотация угрозы – осуществление доступа к информации ОО, хранимой на уровне ОС в файлах файловой системы, неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к информации, хранимой в файлах, с использованием приложений, поддерживающих возможность осуществления доступа к файлам.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к файлам, связанные с возможностью предоставления доступа к информации, размещаемой в файлах, неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – информация, хранимая в файлах.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, достоверность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, хранимой в файлах; несанкционированная модификация информации (в том числе подмена), хранимой в файлах; несанкционированное удаление информации, хранимой в файлах.

Д 3.3 Политика безопасности объекта эксплуатации

Объект оценки должен следовать приведенным ниже правилам политики безопасности объекта эксплуатации.

Политика безопасности-1

Должны быть в наличии надлежащие корректно функционирующие средства администрирования, доступные только уполномоченным администраторам ОО.

Политика безопасности-2

Должны быть обеспечены надлежащая регистрация и предупреждение администратора ОО о любых событиях, относящихся к безопасности ОО. Должна быть обеспечена возможность для администратора ОО выборочного ознакомления с информацией о произошедших в ОО событиях.

Политика безопасности-3

Должна быть обеспечена возможность для уполномоченных пользователей ОО определять доступность объектов ОО для других пользователей ОО.

Политика безопасности-4

Должна быть обеспечена привязка по времени событий, подвергаемых аудиту.

Д 4 ЦЕЛИ БЕЗОПАСНОСТИ

Д 4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

Цель безопасности-1

Разграничение доступа к объектам ОО

ОО должен обеспечивать доступ к объектам ОО только уполномоченным на это пользователям ОО. ОО должен обеспечивать возможность уполномоченным на это пользователям ОО определять доступность объектов ОО для других пользователей ОО.

Цель безопасности-2

Разграничение доступа к ОО

ОО должен обеспечивать доступ к ОО только уполномоченным на это пользователям.

Цель безопасности-3

Аудит событий

ОО должен располагать надлежащими механизмами регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации должны предоставлять администраторам ОО возможность выборочного ознакомления с информацией о произошедших в ОО событиях.

Цель безопасности-4

Защита данных аудита

ОО должен обеспечивать доступ к данным аудита только уполномоченным администраторам ОО и предотвращать потерю данных аудита в случае

переполнения их хранилища, а также в случае невозможности дальнейшего ведения аудита вследствие исчерпания свободного дискового пространства.

Цель безопасности-5

Наличие средств администрирования

ОО должен располагать надлежащими корректно функционирующими средствами администрирования, доступными только уполномоченным администраторам ОО.

Цель безопасности-6

Защита данных ФБО и ресурсов ОО

ОО должен обеспечивать защиту данных ФБО и ресурсов ОО, поддерживая домен для функционирования ФБО.

Д 4.2 Цели безопасности для среды

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

Цель для среды функционирования ОО-1

Доверительная среда функционирования

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Цель для среды функционирования ОО-2

Контролируемые точки доступа

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, т.е. охраняемой территории и помещении, оборудованной средствами и системами физической защиты и охраны

(контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-3

Взаимодействие с доверенными системами

Должно быть обеспечено взаимодействие ОО только с доверенными изделиями (системами) ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

Цель для среды функционирования ОО-4

Эксплуатация ОО

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Цель для среды функционирования ОО-5

Аутентификация с использованием механизмов ОС

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

Цель для среды функционирования ОО-6

Функция безопасности

Функционирование ОО должно осуществляться в среде функционирования, предоставляющей механизм аутентификации.

Цель для среды функционирования ОО-7

Физическая защита ОО

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-8

Требования к администраторам ОО

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

Цель для среды функционирования ОО-9

Требования к пользователям ОО

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

Цель для среды функционирования ОО-10

Защита данных ФБО и ресурсов ОО

Должна быть обеспечена защита данных ФБО и ресурсов ОО, а также поддержка домена для функционирования ФБО.

Цель для среды функционирования ОО-11

Поддержка аудита

Должна быть обеспечена поддержка средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

Цель для среды функционирования ОО-12

Защита на уровне файловой системы

Должна быть обеспечена защита данных, размещаемых в базах данных ОО, на уровне файлов файловой системы ОС от несанкционированного доступа.

Цель для среды функционирования ОО-13

Восстановление ОО

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

Д 5 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ

В данном разделе ПЗ представлены требования безопасности ИТ, которым должен удовлетворять ОО и его среда. Функциональные требования, представленные в настоящем ПЗ, основаны на функциональных компонентах из части 2 РД БИТ. Требования доверия основаны на компонентах требований доверия из части 3 РД БИТ и представлены в настоящем ПЗ в виде оценочного уровня доверия ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий».

Д 5.1 Требования безопасности для ОО

Д 5.1.1 Функциональные требования безопасности ОО

Функциональные компоненты из части 2 РД БИТ, на которых основаны функциональные требования безопасности ОО, приведены в таблице 5.1.

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.4	Предотвращение потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах

Идентификатор компонента требований	Название компонента требований
	безопасности
FIA_ATD.1	Определение атрибутов пользователя
FIA_UID.2	Идентификация до любых действий пользователя
FIA_USB.1	Связывание пользователь-субъект
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_REV.1	Отмена
FMT_SMR.1	Роли безопасности
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FTA_TSE.1	Открытие сеанса с ОО

Д 5.1.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

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

- а) запуск и завершение выполнения функций аудита;
- б) все события, потенциально подвергаемые аудиту, на неопределенном уровне аудита;
- в) [события, приведенные во втором столбце таблицы 5.2, а также [назначение: *другие специально определенные события, потенциально подвергаемые аудиту*]].

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

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

- б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ, [информацию, определенную в третьем столбце таблицы 5.2, а также **[назначение: другую относящуюся к аудиту информацию]**].

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во время сбора данных аудита	
FAU_STG.3	Предпринимаемые действия после превышения порога заполнения журнала аудита	
FAU_STG.4	Факт останова ОО при отсутствии свободного дискового пространства для создания журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на именованном объекте, на который распространяется политика дискреционного управления доступом	Идентификатор объекта
FIA_UID.2	Все случаи использования механизма идентификации субъектов доступа	
FIA_USB.1	Факт создания пользователя	
FMT_MOF.1	Все модификации режима выполнения аудита	
FMT_MSA.1	Все модификации значений атрибутов безопасности, используемых в политике дискреционного управления доступом	
FMT_MSA.3	Модификации настройки по умолчанию	

Компонент	Событие	Детализация
	ограничительных правил, все модификации начальных значений атрибутов безопасности, которые используются для политики дискреционного управления доступом	
FMT_MTD.1	Все модификации значений данных ФБО	
FMT_REV.1 (1)	Все попытки отмены полномочий у пользователей ОО на доступ к объектам, отмены прав доступа к объекту (модификация списка дискреционного доступа)	
FMT_REV.1 (2)	Все попытки отмены прав доступа к объекту (модификация списка дискреционного доступа)	
FMT_SMR.1	Модификация множества администраторов ОО и пользователей ОО и других определенных ролей	
FTA_TSE.1	Все попытки открытия сеанса доступа к ОО со стороны субъектов	

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 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.2 «Идентификация до любых действий пользователя».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченному администратору ОО] возможность читать [всю информацию аудита] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **уполномоченному администратору ОО** 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 **уполномоченных администраторов ОО**, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны **предоставить** возможность выполнить поиск данных аудита, основанный на
[
 следующих критериях:
 а) тип события;
 б) [**назначение: другие критерии**]
].

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SEL.1 Избирательный аудит

FAU_SEL.1.1 ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой совокупности по следующим атрибутам:
а) тип события;
б) [**назначение: список дополнительных атрибутов, на которых основана избирательность аудита**].

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FMT_MTD.1 «Управление данными ФБО».

FAU_STG.1 Защищенное хранение журнала аудита

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

FAU_STG.1.2 ФБО должны быть способны предотвращать модификации записей 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, направленные на сохранение данных журнала аудита и обеспечивающие непрерывность процесса аудита*], если журнал аудита **превысит** [установленный уполномоченным администратором ОО размер].

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны игнорировать события, подвергающиеся аудиту и [назначение: *действия, направленные на невозможность совершения дальнейших событий, связанных с безопасностью ОО*] при **отсутствии свободного дискового пространства для создания журнала аудита.**

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

Замечание по применению:

Разработчиком ЗБ должны быть специфицированы действия, обеспечивающие, в случае отсутствия свободного дискового пространства для создания и ведения журнала аудита, невозможность совершения любых событий, связанных с безопасностью ОО. Примерами таких действий может служить временная приостановка функционирования ОО, полный останов ОО и т.п.

Д 5.1.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику информационного управления доступом] для
[
а) [назначение: список субъектов ОО], действующих от имени пользователей;
б) [назначение: список именованных объектов ОО];
в) всех операций между субъектами и объектами
].

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 дискреционного управления доступом] к объектам, основываясь на
[
следующем:
а) ассоциированные с субъектом идентификатор учетной записи пользователя, принадлежность к роли (ролям);
б) следующие, ассоциированные с объектами, атрибуты управления доступом: [назначение: список атрибутов управления доступом, которые должны обеспечить возможность:
 ♣ ассоциировать разрешение или запрет на выполнение операций с идентификаторами одного или более пользователей;
 ♣ ассоциировать разрешение или запрет на выполнение операций с идентификаторами одной или более ролей;
 ♣ ассоциировать разрешение или запрет на выполнение операций по умолчанию]

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: *[назначение: набор правил, определяющих политику дискреционного доступа, в которых:*

- а) для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда идентификатор субъекта соответствует идентификатору, определенному в атрибутах контроля доступа объекта;*
- б) для каждой операции должно быть определено правило или правила использования атрибутов разрешения в случаях, когда субъект является участником роли, идентификатор которой, определен в атрибутах контроля доступа объекта;*
- в) для каждой операции должно быть определено правило или правила использования атрибутов разрешения по умолчанию в случаях, когда идентификатор субъекта не соответствует определенному в атрибутах контроля доступа объекта и субъект является участником роли, идентификатор которой, не определен в атрибутах контроля доступа объекта*

].

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».

Д 5.1.1.3 Идентификация и аутентификация (FIA)

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

[

- а) идентификатор пользователя;
- б) идентификатор роли, участником которой является пользователь;
- в) [назначение: *другие атрибуты безопасности пользователя*]

].

Зависимости: отсутствуют.

Замечание по применению:

Под пользователями в настоящем компоненте требований понимаются все идентифицированные в FMT_SMR.1 роли.

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый **субъект доступа** был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: отсутствуют.

FIA_USB.1 Связывание пользователь-субъект

FIA_USB.1.1 ФБО должны ассоциировать соответствующие атрибуты безопасности **субъекта доступа** с субъектами, действующими от имени этого **субъекта доступа**.

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

Д 5.1.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность определять режим выполнения, модифицировать режим выполнения функций, **связанных с:**

[

а) аудитом;

б) [назначение: *другие функции*]

]

только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предоставляющую** возможность модифицировать атрибуты безопасности, [перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1], только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предусматривающую** ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления **политики дискреционного управления доступом**.

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

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 [*выполнения операций, указанных во втором столбце таблицы 5.3, а также [назначение: другие операции]*] **над данными**, [указанными в третьем столбце таблицы 5.3, а также [назначение: *список других данных ФБО*]] только [назначение: *уполномоченные идентифицированные роли*].

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.3 – Управляемые данные ФБО

Компонент	Операция	Данные ФБО
FAU_SAR.1	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих чтение записей аудита
FAU_STG.3	установление, модификация	размер журнала аудита
FIA_UID.2	создание, модификация, удаление	идентификационная информация пользователя
FMT_MOF.1	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих доступ к управлению режимами аудита
FMT_MSA.1	удаление, модификация, добавление	состав уполномоченных пользователей, являющихся участниками ролей, предусматривающих модификацию

Компонент	Операция	Данные ФБО
		атрибутов безопасности
FMT_MSA.3	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих модификацию начальных значений атрибутов безопасности
FMT_MTD.1	удаление, модификация, добавление	состав уполномоченных пользователей, являющихся участниками ролей, предусматривающих модификацию данных ФБО, определенных в настоящей таблице
FMT_REV.1 (1)	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих возможность отмены атрибутов безопасности, ассоциированных с пользователями и объектами
FMT_SMR.1	удаление, модификация, добавление	состав пользователей ОО, являющихся участниками ролей администратор ОО и пользователь ОО
FTA_TSE.1	установление, модификация	значение параметров, запрещающих установление соединения с ОО

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны **предоставлять** возможность отмены атрибутов безопасности, ассоциированных с **пользователями ОО и объектами**, в пределах ОДФ только [уполномоченному администратору ОО].

FMT_REV.1.2 ФБО должны **осуществлять следующие** правила:

[

- а) отмена полномочий у пользователей ОО на доступ к объектам должна вступать в силу при следующем сеансе работы пользователя ОО;
 - б) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;
 - в) [**назначение:** *другие правила отмены*]
-].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны **предоставлять** возможность отмены атрибутов безопасности, ассоциированных с **объектами**, в пределах ОДФ только [**назначение:** *пользователи, уполномоченные на изменение атрибутов безопасности в соответствии с политикой дискреционного управления доступом*].

FMT_REV.1.2 ФБО должны **осуществлять следующие** правила:

- [
- а) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;
 - б) [**назначение:** *другие правила отмены*]
-].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

[

- а) администратор ОО;
 - б) пользователь ОО;
 - в) [**назначение:** *другие уполномоченные идентифицированные роли*]
-].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать **субъектов доступа** с ролями.

Зависимости: FIA_UID.2 «Выбор момента идентификации».

Д 5.1.1.5 Защита ФБО (FPT)

FPT_RVM.1 (1) Невозможность обхода ПБО

FPT_RVM.1.1 ФБО должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 (1) Отделение домена ФБО

FPT_SEP.1.1 ФБО должны поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 ФБО должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

Д 5.1.1.6 Доступ к ОО (FTA)

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса **доступа к ОО**, основываясь на

[

следующих атрибутах:

- а) идентификатор пользователя;
- б) [назначение: *другие атрибуты*]

].

Зависимости: отсутствуют.

Д 5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 РД БИТ и образуют ОУД4, усиленный компонентами ALC_FLR.1 «Базовое устранение недостатков», AVA_VLA. 3 «Умеренно стойкий» (см. таблицу 5.5).

Таблица 5.5 – Требования доверия к безопасности ОО

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Управление конфигурацией	ACM_AUT.1	Частичная автоматизация УК
	ACM_CAP.4	Поддержка генерации, процедуры приемки
	ACM_SCP. 2	Охват УК отслеживания проблем
Поставка и эксплуатация	ADO_DEL.2	Обнаружение модификации
	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP. 2	Полностью определенные внешние интерфейсы
	ADV_HLD. 2	Детализация вопросов безопасности в проекте верхнего уровня
	ADV_IMP.1	Подмножество реализации ФБО
	ADV_LLD.1	Описательный проект нижнего уровня
	ADV_RCR. 1	Неформальная демонстрация соответствия
	ADV_SPM. 1	Неформальная модель политики безопасности ОО
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя

Классы доверия	Идентификаторы компонентов доверия	Названия компонентов доверия
Поддержка жизненного цикла	ALC_DVS.1	Идентификация мер безопасности
	ALC_FLR. 1	Базовое устранение недостатков
	ALC_LCD. 1	Определение модели жизненного цикла разработчиком
	ALC_TAT. 1	Полностью определенные инструментальные средства разработки
Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.1	Тестирование: проект верхнего уровня
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
Оценка уязвимостей	AVA_MSU.2	Подтверждение правильности анализа
	AVA_SOF.1	Оценка стойкости функции безопасности ОО
	AVA_VLA. 3	Умеренно стойкий

Д 5.1.3 Управление конфигурацией (АСМ)

АСМ_AUT.1 Частичная автоматизация УК

Элементы действий разработчика

АСМ_AUT.1.1D Разработчик должен использовать систему УК.

АСМ_AUT.1.2D Разработчик должен представить план УК.

Элементы содержания и представления свидетельств

АСМ_AUT.1.1C Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО производятся только санкционированные изменения.

АСМ_AUT.1.2C Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.

АСМ_AUT.1.3C План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.

АСМ_AUT.1.4С План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.

Элементы действий оценщика

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

АСМ_CAP.4 Поддержка генерации, процедуры приемки

Элементы действий разработчика

АСМ_CAP.4.1D Разработчик должен предоставить маркировку для ОО.

АСМ_CAP.4.2D Разработчик должен использовать систему УК.

АСМ_CAP.4.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

АСМ_CAP.4.1С Маркировка ОО должна быть уникальна для каждой версии ОО.

АСМ_CAP.4.2С ОО должен быть помечен маркировкой.

АСМ_CAP.4.3С Документация УК должна включать в себя список конфигурации, план УК и план приемки.

АСМ_CAP.4.4С Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

АСМ_CAP.4.5С Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

АСМ_CAP.4.6С Система УК должна уникально идентифицировать все элементы конфигурации.

АСМ_CAP.4.7С План УК должен содержать описание, как используется система УК.

АСМ_CAP.4.8С Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

АСМ_CAP.4.9С Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

АСМ_САР.4.10С Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

АСМ_САР.4.11С Система УК должна поддерживать генерацию ОО.

АСМ_САР.4.12С План приемки должен содержать описание процедур, используемых для приемки модифицированного или вновь созданного элемента конфигурации как части ОО.

Элементы действий оценщика

АСМ_САР.4.1Е Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АСМ_SCP.2 Охват УК отслеживания проблем

Элементы действий разработчика

АСМ_SCP.3.1D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

АСМ_SCP.2.1С Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора, документацию УК **и недостатки безопасности.**

АСМ_SCP.2.2С Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.

Элементы действий оценщика

АСМ_SCP.2.1Е Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

Д 5.1.4 Поставка и эксплуатация (ADO)

ADO_DEL.2 Обнаружение модификации

Элементы действий разработчика

ADO_DEL.2.1D Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

ADO_DEL.2.2 Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ADO_DEL.2.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий к местам использования.

ADO_DEL.2.2C Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.

ADO_DEL.2.3C Документация поставки должна содержать описание, как различные процедуры позволяют обнаружить попытку подмены от имени разработчика, даже в тех случаях, когда разработчик ничего не отсылал к месту использования.

Элементы действий оценщика

ADO_DEL.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

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

Д 5.1.5 Разработка (ADV)

ADV_FSP.2 Полностью определенные внешние интерфейсы

Элементы действий разработчика

ADV_FSP.2.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.2.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.2.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.2.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая **полную** детализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.2.4C Функциональная спецификация должна полностью представить ФБО.

ADV_FSP.2.5C Функциональная спецификация должна включать в себя логическое обоснование, что ФБО полностью представлены.

Элементы действий оценщика

ADV_FSP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.2.2E Оценщик должен сделать независимое заключение, что функциональная спецификация - точное и полное отображение функциональных требований безопасности ОО.

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

Элементы действий разработчика

ADV_HLD.3.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.2.1C Представление проекта верхнего уровня должно быть неформальным.

ADV_HLD.2.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.2.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.2.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.2.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.2.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.2.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.2.8C Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_HLD.2.9C Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

Элементы действий оценщика

ADV_HLD.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.2.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня - точное и полное отображение функциональных требований безопасности ОО.

ADV_IMP.1 Подмножество реализации ФБО

Элементы действий разработчика

ADV_IMP.1.1D Разработчик должен обеспечить представление реализации для выбранного подмножества ФБО.

Элементы содержания и представления свидетельств

ADV_IMP.1.1C Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.

ADV_IMP.1.2C Представление реализации должно быть внутренне непротиворечивым.

Элементы действий оценщика

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

ADV_IMP.1.2E Оценщик должен сделать независимое заключение, что наименее абстрактное представление ФБО – точное и полное отображение функциональных требований безопасности ОО.

ADV_LLD.1 Описательный проект нижнего уровня

Элементы действий разработчика

ADV_LLD.1.1D Разработчик должен представить проект нижнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_LLD.1.1C Представление проекта нижнего уровня должно быть неформальным.

ADV_LLD.1.2C Проект нижнего уровня должен быть внутренне непротиворечивым.

ADV_LLD.1.3C Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

ADV_LLD.1.4C Проект нижнего уровня должен содержать описание назначения каждого модуля.

ADV_LLD.1.5C Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

ADV_LLD.1.6C Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.

ADV_LLD.1.7C Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

ADV_LLD.1.8C Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

ADV_LLD.1.9C Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя, при необходимости, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_LLD.1.10C Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

Элементы действий оценщика

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

ADV_LLD.1.2E Оценщик должен сделать независимое заключение, что проект нижнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

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

ADV_SPM.1 Неформальная модель политики безопасности ОО

Элементы действий разработчика

ADV_SPM.1.1D Разработчик должен представить модель ПБО.

ADV_SPM.1.2D Разработчик должен демонстрировать или доказать, где это требуется, соответствие между функциональной спецификацией и моделью ПБО.

Элементы содержания и представления свидетельств

ADV_SPM.1.1C Модель ПБО должна быть неформальной.

ADV_SPM.1.2C Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.1.3C Модель ПБО должна включать в себя логическое обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.1.4C Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.

Элементы действий оценщика

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

Д 5.1.6 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

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

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

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

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

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

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

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

Элементы действий оценщика

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

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

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

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

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

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

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

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

Элементы действий оценщика

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

Д 5.1.7 Поддержка жизненного цикла (ALC)

ALC_DVS.1 Идентификация мер безопасности

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

ALC_DVS.1.2C Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.

Элементы действий оценщика

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

ALC_DVS.1.2E Оценщик должен подтвердить применение мер безопасности.

ALC_FLR.1 Базовое устранение недостатков

Элементы действий разработчика

ALC_FLR.1.1D Разработчик должен задокументировать процедуры устранения недостатков.

Элементы содержания и представления свидетельств

ALC_FLR.1.1C Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждой редакции ОО.

ALC_FLR.1.2C Процедуры устранения недостатков должны содержать требование представления описания природы и проявлений каждого недостатка безопасности, а также статуса завершения исправления этого недостатка.

ALC_FLR.1.3C Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

ALC_FLR.1.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

Элементы действий оценщика

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

ALC_LCD.1 Определение модели жизненного цикла разработчиком

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 свидетельств

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

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

Элементы действий оценщика

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

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Элементы действий разработчика

ALC_TAT.1.1D Разработчик должен идентифицировать инструментальные средства разработки ОО.

ALC_TAT.1.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.

Элементы содержания и представления свидетельств

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

ALC_TAT.1.2C Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

ALC_TAT.1.3C Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.

Элементы действий оценщика

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

Д 5.1.8 Тестирование (ATE)

ATE_COV.2 Анализ покрытия

Элементы действий разработчика

ATE_COV.2.1D Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

ATE_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

ATE_COV.2.2C Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.

Элементы действий оценщика

ATE_COV.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_DPT.1 Тестирование: проект верхнего уровня

Элементы действий разработчика

ATE_DPT.1.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE_DPT.1.1C Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня.

Элементы действий оценщика

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

ATE_FUN.1 Функциональное тестирование

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 свидетельств

ATE_FUN.1.1C Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.

ATE_FUN.1.2C Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей тестирования.

ATE_FUN.1.3C Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.

ATE_FUN.1.4C Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.

ATE_FUN.1.5C Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.

Элементы действий оценщика

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

ATE_IND.2 Выборочное независимое тестирование

Элементы действий разработчика

ATE_IND.2.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

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 представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.2.2E Оценщик должен протестировать подмножество ФБО, **как необходимо**, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

ATE_IND.2.3E Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

Д 5.1.9 Оценка уязвимостей (AVA)

AVA_MSU.2 Подтверждение правильности анализа

Элементы действий разработчика

AVA_MSU.2.1D Разработчик должен представить руководства по применению ОО.

AVA_MSU.2.2D Разработчик должен задокументировать анализ руководств.

Элементы содержания и представления свидетельств

AVA_MSU.2.1C Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.2.2C Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

AVA_MSU.2.3C Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.2.4C Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

AVA_MSU.2.5C Документация анализа должна демонстрировать, что руководства полны.

Элементы действий оценщика

AVA_MSU.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_MSU.2.2E Оценщик должен повторить все процедуры конфигурирования и установки и выборочно другие процедуры для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

AVA_MSU.2.3E Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

AVA_MSU.2.4E Оценщик должен подтвердить, что документация анализа показывает обеспечение руководствами безопасного функционирования во всех режимах эксплуатации ОО.

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

AVA_SOF.1.1C Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее

стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.

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

Элементы действий оценщика

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

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

AVA_VLA.3 Умеренно стойкий

Элементы действий разработчика

AVA_VLA.3.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску путей, которыми пользователь может нарушить ПБО.

AVA_VLA.3.2D Разработчик должен задокументировать местоположение идентифицированных уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.3.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.3.2C Документация должна содержать строгое обоснование, что ОО с идентифицированными уязвимостями является стойким к явным нападениям проникновения.

AVA_VLA.3.3C Свидетельство должно показать, что поиск уязвимостей является систематическим.

Элементы действий оценщика

- AVA_VLA.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.
- AVA_VLA.3.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.
- AVA_VLA.3.3E Оценщик должен выполнить независимый анализ уязвимостей.
- AVA_VLA.3.4E Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.
- AVA_VLA.3.5E Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим **умеренным** потенциалом нападения.

Д 5.2 Требования безопасности для среды ИТ

Функцией безопасности, реализуемой средой в интересах обеспечения безопасности ОО, является функция безопасности «Аутентификация». Данная функция реализуется механизмом паролей среды ИТ. Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости.

Функциональные компоненты из части 2 РД БИТ, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.5.

Таблица 5.6 – Функциональные компоненты, на которых основаны ФТБ среды ИТ

Идентификатор компонента требований	Название компонента требований
FIA_AFL.1	Обработка отказов аутентификации
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FPT_RVM.1 (2)	Невозможность обхода ПБО
FPT_SEP.1 (2)	Отделение домена ФБО
FPT_STM.1	Надежные метки времени

Д 5.2.1 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

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

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

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

Замечание по применению:

Конкретизация данного требования совместно с требованием FIA_SOS.1 в ЗБ должна обеспечивать возможность для механизмов безопасности, реализующих функции безопасности «Аутентификация», предоставлять адекватную защиту от нарушения безопасности ОО нарушителем с низким потенциалом нападения.

FIA_SOS.1 Верификация секретов

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

Зависимости: отсутствуют.

Замечание по применению:

Конкретизация данного требования совместно с требованием FIA_AFL.1 в ЗБ должна обеспечивать возможность для механизмов безопасности, реализующих функции безопасности «Аутентификация», предоставлять адекватную защиту от нарушения безопасности ОО нарушителем с низким потенциалом нападения.

FIA_UAU.2 Аутентификация до любых действий пользователя

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

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

Д 5.2.2 Защита ФБО (FPT)

FPT_RVM.1 (2) Невозможность обхода ПБО

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

Зависимости: отсутствуют.

FPT_SEP.1 (2) Отделение домена ФБО

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

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

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 **Функции безопасности среды ИТ** должны быть способны предоставить надежные метки времени для **использования ФБО**.

Зависимости: отсутствуют.

Д 6 ОБОСНОВАНИЕ

В данном разделе дано обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ПЗ. В разделе «Обоснование» также демонстрируется справедливость утверждений о СФБ.

Д 6.1 Обоснование целей безопасности

Д 6.1.1 Обоснование целей безопасности для ОО

В таблице 6.1 приведено отображение целей безопасности на угрозы и политику безопасности объекта эксплуатации.

Таблица 6.1 – Отображение целей безопасности на угрозы и политику безопасности объекта эксплуатации

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

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6
Политика безопасности-3	X					

Цель безопасности-1

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-1**, и реализацией политики безопасности организации **Политика безопасности-3**, так как обеспечивает доступ к объектам ОО только уполномоченным пользователям ОО, а также обеспечивает возможность уполномоченным пользователям ОО определять доступность объектов ОО для других пользователей ОО.

Цель безопасности-2

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-2** и **Угроза-3**, так как обеспечивает доступ к ОО только уполномоченным на это пользователям.

Цель безопасности-3

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-2**, так как обеспечивает наличие надлежащих механизмов регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации предоставляют администраторам ОО возможность выборочного ознакомления с информацией о произошедших в ОО событиях.

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-4**, **Угроза-5** и **Угроза-6**, так как обеспечивает доступ к данным аудита только уполномоченным администраторам ОО и предотвращает потерю данных аудита в случае переполнения их хранилища, а также в случае невозможности дальнейшего ведения аудита вследствие исчерпания свободного дискового пространства.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-1**, так как обеспечивает наличие надлежащих корректно функционирующих средств администрирования, доступных только уполномоченным администраторам ОО.

Цель безопасности-6

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **Угроза-7** и **Угроза-8**, так как обеспечивает защиту данных ФБО и ресурсов ОО, поддерживая домен для функционирования ФБО.

Д 6.1.2 Обоснование целей безопасности для среды

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

Таблица 6.2 – Отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности объекта эксплуатации

	Цель для среды функционирования ОО-1	Цель для среды функционирования ОО-2	Цель для среды функционирования ОО-3	Цель для среды функционирования ОО-4	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-6	Цель для среды функционирования ОО-7	Цель для среды функционирования ОО-8	Цель для среды функционирования ОО-9	Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11	Цель для среды функционирования ОО-12	Цель для среды функционирования ОО-13
Предположение-1	X												
Предположение-2		X											
Предположение-3			X										
Предположение-4				X									
Предположение-5	3				X								
Предположение-6						X							
Предположение-7													X
Предположение-8							X						
Предположение-9								X					
Предположение-10									X				
Угроза-9					X								
Угроза-10					X								
Угроза-11										X			
Угроза-12												X	
Политика безопасности-4											X		

Цель для среды функционирования ОО-1

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-1**, так как обеспечивает отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

Цель для среды функционирования ОО-2

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-2**, так как обеспечивает осуществление доступа к ОО только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-3

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-3**, так как обеспечивает взаимодействие ОО только с доверенными системами ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

Цель для среды функционирования ОО-4

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-4**, так как обеспечивает установку конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

Цель для среды функционирования ОО-5

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-5** и противостояния угрозам **Угроза-9** и **Угроза-10**, так как обеспечивает осуществление аутентификации

субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов ОС, под управлением которой функционирует ОО.

Цель для среды функционирования ОО-6

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-6**, так как обеспечивает осуществление функционирования ОО в среде функционирования, предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от нарушения безопасности ОО нарушителями с низким потенциалом нападения.

Цель для среды функционирования ОО-7

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-8**, так как обеспечивает, для предотвращения несанкционированного физического доступа, размещение компьютера с установленным ОО в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Цель для среды функционирования ОО-8

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-9**, так как обеспечивает прохождение персоналом, ответственным за администрирование ОО, проверок на благонадежность и компетентность, а также деятельность согласно соответствующей документации.

Цель для среды функционирования ОО-9

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-10**, так как обеспечивает прохождение уполномоченными на доступ к ОО пользователями проверок на

благонадежность, а их совместные действия направлены исключительно на выполнение своих функциональных обязанностей.

Цель для среды функционирования ОО-10

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-11**, так как обеспечивает защиту данных ФБО и ресурсов ОО, а также поддержку домена для функционирования ФБО.

Цель для среды функционирования ОО-11

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **Политика безопасности-4**, так как обеспечивает поддержку средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

Цель для среды функционирования ОО-12

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-12**, так как обеспечивает защиту данных, размещаемых в БД, на уровне файлов файловой системы ОС от несанкционированного доступа.

Цель для среды функционирования ОО-13

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **Предположение-7**, так как обеспечивает выполнение мероприятий, направленных на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

Д 6.2 Обоснование требований безопасности

Д 6.2.1 Обоснование требований безопасности для ОО

Д 6.2.1.1 Обоснование функциональных требований безопасности ОО

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

Таблица 6.3 – Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6
FAU_GEN.1			X			
FAU_GEN.2			X			
FAU_SAR.1			X			
FAU_SAR.2				X		
FAU_SAR.3			X			
FAU_SEL.1			X			
FAU_STG.1				X		
FAU_STG.3				X		
FAU_STG.4				X		
FDP_ACC.1	X					
FDP_ACF.1	X					
FIA_ATD.1	X	X	X		X	
FIA_UID.2	X	X				
FIA_USB.1	X	X	X			
FMT_MOF.1					X	
FMT_MSA.1	X				X	
FMT_MSA.3	X				X	

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6
FMT_MTD.1					X	
FMT_REV.1 (1)					X	
FMT_REV.1 (2)	X					
FMT_SMR.1	X			X	X	X
FPT_RVM.1 (1)						X
FPT_SEP.1 (1)						X
FTA_TSE.1		X				

FAU_GEN.1 Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_GEN.2 Ассоциация идентификатора пользователя

Выполнение требований данного компонента обеспечивает возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления уполномоченным администраторам ОО всей информации аудита в

понятном для него виде. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает запрет всем пользователям доступ к чтению записей аудита, за исключением уполномоченных администраторов ОО, которым явно предоставлен доступ для чтения. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает выполнение поиска данных аудита, основанного на определенных критериях (тип события). Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_SEL.1 Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, уполномоченным администратором ОО по таким атрибутам, как тип события. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-3** и способствует ее достижению.

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает защиту хранимых записей аудита от несанкционированного удаления и предотвращает модификацию записей аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_STG.3

Действия в случае возможной потери данных

аудита

Выполнение требований данного компонента обеспечивает выполнение действий, направленных на сохранение данных журнала аудита и обеспечивающих непрерывность процесса аудирования, если журнал аудита превысит установленный уполномоченным администратором ОО размер. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FAU_STG.4

Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает игнорирование событий, подвергающихся аудиту, и выполнение действий, направленных на невозможность совершения дальнейших событий, связанных с безопасностью ОО при отсутствии свободного дискового пространства для создания журнала аудита. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-4** и способствует ее достижению.

FDP_ACC.1

Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает реализацию политики дискреционного доступа для субъектов, именованных объектов и всех операций между субъектами и объектами. 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 осуществление политики дискреционного доступа, основываясь на атрибутах безопасности, определении правил доступа субъектов к объектам. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-1** и способствует ее достижению.

FIA_ATD.1

Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя (пользователя ОО и администратора ОО) в качестве атрибутов безопасности идентификатора пользователя, идентификатора роли, участником которой является пользователь, а также других атрибутов безопасности. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3, Цель безопасности-5** и способствует их достижению.

FIA_UID.2

Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение идентификации субъекта доступа до того, как ФБО разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2** и способствует их достижению.

FIA_USB.1

Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами, действующими от имени этого субъекта доступа. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-2, Цель безопасности-3** и способствует их достижению.

FMT_MOF.1

Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает модификацию и определение режимов выполнения функций, связанных с аудитом, только уполномоченному администратору ОО, предусмотрена возможность определения других функций. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_MSA.1

Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-5** и способствует их достижению.

FMT_MSA.3

Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом, и возможность для уполномоченных идентифицированных ролей определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-5** и способствует их достижению.

FMT_MTD.1

Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации определенных данных ФБО только уполномоченным идентифицированным ролям. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** по достижению.

FMT_REV.1 (1) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО и объектами, в пределах ОДФ только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_REV.1 (2) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с объектами, в пределах ОДФ только пользователям, уполномоченным на изменение атрибутов безопасности в соответствии с политикой дискреционного управления доступом. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-5** и способствует ее достижению.

FMT_SMR.1 Роли безопасности

Данный компонент включен в ПЗ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту ролей администратора ОО и пользователя ОО, предусмотрена возможность определения других уполномоченных идентифицированных ролей. Рассматриваемый компонент сопоставлен с целями **Цель безопасности-1, Цель безопасности-4, Цель безопасности-5, Цель безопасности-6** и способствует их достижению.

FPT_RVM.1 (1) Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

FPT_SEP.1 (1) Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-6** и способствует ее достижению.

Выполнение требований данного компонента обеспечивает способность отказа ОО в открытии сеанса доступа к ОО, основываясь на идентификаторе пользователя, предусмотрена возможность определения других атрибутов. Рассматриваемый компонент сопоставлен с целью **Цель безопасности-2** и способствует ее достижению.

Д 6.2.1.2 Обоснование требований доверия к безопасности ОО

Включение в настоящий ПЗ ОУД4, усиленный компонентом ALC_FLR.1 «Базовое устранение недостатков» AVA_VLA.3 «Умеренно стойкий», является достаточным при определении допустимости использования ОО в информационных системах, в которых обрабатывается информация ограниченного доступа.

Д 6.2.2 Обоснование требований безопасности для среды ИТ

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

Таблица 6.4 – Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	Цель для среды функционирования ОО-5	Цель для среды функционирования ОО-10	Цель для среды функционирования ОО-11
FIA_AFL.1	X		
FIA_SOS.1	X		
FIA_UAU.2	X		
FPT_RVM.1 (2)		X	
FPT_SEP.1 (2)		X	
FPT_STM.1			X

FIA_AFL.1 Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает выполнение определенных действий, направленных на дальнейшее предотвращение попыток доступа со стороны субъекта, ограниченное временным интервалом, при достижении определенного уполномоченным администратором ОО числа неуспешных попыток аутентификации при доступе к ОО. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает верификацию качества паролей на доступ к ОО. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации субъекта доступа к ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-5** и способствует ее достижению.

FPT_RVM.1 (2) Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-10** и способствует ее достижению.

FPT_SEP.1 (2) Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-10** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ПЗ для удовлетворения зависимости компонента FAU_GEN.1 от наличия в записях аудита точного указания даты и времени. Рассматриваемый компонент сопоставлен с целью **Цель для среды функционирования ОО-11** и способствует ее достижению.

Д 6.2.3 Обоснование зависимостей требований

В таблице 6.5 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворены в настоящем ПЗ либо включением компонентов, определенных в части 2 РД БИТ под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в части 2 РД БИТ под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 6.5 является справочным и содержит компоненты, определенные в части 2 РД БИТ в описании компонентов требований, приведенных в столбце 1 таблицы 6.5, под рубрикой «Зависимости».

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

Таблица 6.5 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по РД БИТ	Удовлетворение зависимостей
Зависимости функциональных требований ОО		
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FAU_STG.4	FAU_STG.1	FAU_STG.1

Функциональные компоненты	Зависимости по РД БИТ	Удовлетворение зависимостей
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (1)	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
Зависимости функциональных требований среды ИТ		
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2

Таким образом, все зависимости включенных в ПЗ функциональных требований были удовлетворены.