Система управления контентом МСВСфера Инфооборот 6.2

Задание по безопасности

МСВСфера_Инфооборот_6.2_ЗБ

Версия 1.0

Содержание

Перечень сокращений

ACL	Access control list (Список контроля доступа)
LDAP	Lightweight Directory Access Protocol (Протокол доступа к каталогам)
RBAC	Role-based access control (Управление доступом на основе ролей)
RPM	RPM Package Manager (Система управления пакетами в формате RPM)
ЗБ	Задание по безопасности
ИС	Информационная система
ИТ	Информационная технология
ИФБО	Интерфейс ФБО
ОДФ	Область действия ФБО
ОО	Объект оценки
ОС	Операционная система
ОУД	Оценочный уровень доверия
ПБО	Политика безопасности организации
ПЗ	Профиль защиты
ПО	Программное обеспечение
ПФБ	Политика функций безопасности
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
ТДБ	Требования доверия к безопасности объекта оценки
УК	Управление конфигурацией
ФБ	Функция безопасности
ФБО	Функциональные возможности безопасности ОО
ФТБ	Функциональные требования безопасности к ОО

1 Введение

1.1 Ссылка на ЗБ

Название ЗБ: Система управления контентом МСВСфера Инфооборот 6.2. Задание по безопасности
Версия ЗБ: 1.0
Обозначение ЗБ: МСВСфера_Инфооборот_6.2_ЗБ
Разработчик ЗБ: ООО «Национальный центр поддержки и разработки»
Дата выпуска ЗБ: 28 ноября 2020 года

1.2 Ссылка на ОО

Разработчик ОО: ООО «Национальный центр поддержки и разработки»
Название ОО: Система управления контентом МСВСфера Инфооборот 6.2
Версия ОО: 6.2
Обозначение ОО: МСВСфера Инфооборот 6.2

1.3 Аннотация ОО

1.3.1 Использование и основные характеристики безопасности ОО

ОО является системой управления контентом, ориентированной на создание информационных платформ корпоративного масштаба, обеспечивающих решение задач самого широкого спектра назначения, в том числе, управление документами, управление бизнес-процессами, организация совместной работы.

ОО обладает обширными функциональными возможностями и следующими отличительными характеристиками: высокая масштабируемость и производительность, отказоустойчивость, функциональная расширяемость, поддержка открытых стандартов, интуитивно понятный настраиваемый веб-интерфейс.

Имеющиеся в ОО средства обеспечения безопасности реализуют функции, включающие: идентификацию и аутентификацию, управление доступом, аудит информационной безопасности, управление механизмами безопасности.

1.3.2 Тип ОО

ОО относится к типу многофункциональных систем управления контентом с сервис-ориентированной архитектурой и поддержкой открытых стандартов.

1.3.3 Требуемые аппаратные средства и программное обеспечение, не входящие в ОО

ОО предназначен для функционирования на средствах вычислительной техники с 64-разрядными процессорами Intel/AMD под управлением операционной системы МСВСфера 7.3 Сервер.

1.4 Описание ОО

1.4.1 Физические границы ОО

ОО поставляется в виде верифицированного ISO-образа инсталляционного дистрибутива вместе с эксплуатационной документацией, включающей руководство администратора, руководство пользователя, задание по безопасности и формуляр в котором изложены условия, ограничения и требования по эксплуатации.

Поставка может осуществляться с помощью почтовой и/или курьерской служб на оптических дисках, упакованных в футляры, опечатанные специальными защитными стикерами, а также по общедоступным каналам связи из специального защищенного репозитория в подписанном усиленной квалифицированной подписью виде.

1.4.2 Логические границы ОО

В состав системы в общем случае входят следующие компоненты:

сервер управления контентом, предназначенный для организации репозитория контента и реализации сервисов безопасного доступа к нему;

сервер портала, предназначенный для предоставления пользовательского интерфейса и обеспечения доступа пользователей к системе с помощью браузера;

сервер документов, предназначенный для хранения документов в репозитории;

сервер метаднных, предназначенный для хранения метаданных документов;

сервер индексации, предназначенный для реализации атрибутивного и полнотекстового поиска по репозиторию;

балансировщик нагрузки, предназначенный для распределения вычислительной нагрузки.

Архитектура системы обладает гибкостью и допускает эффективное использование ее компонентов в различных вариантах развертывания на одном или нескольких компьютерах с использованием технологий виртуализации и кластеризации.

Логические границы ОО определяются функциями безопасности, которые реализуются сервером управления контентом и могут быть кратко описаны нижеследующим образом.

1.4.2.1 Идентификация и аутентификация

Идентификация и аутентификация пользователей осуществляется до разрешения им любых действий. Средства, реализующие данную функцию, обеспечивают идентификацию пользователей по именам, заданным при регистрации, аутентификацию пользователей на основе предъявляемых ими паролей, исключение отображения действительного значения паролей при их

вводе в диалоговом интерфейсе и защиту при хранении, возможность проверки соответствия паролей заданной метрике качества, возможность устанавливать пороговое значение количества последовательных неуспешных попыток аутентификации и блокировать доступ пользователя при его достижении на заданное время, возможность ассоциировать атрибуты безопасности пользователя с выполняемыми от его имени действиями.

1.4.2.2 Управление доступом

Средства, реализующие данную функцию, обеспечивают постоянный контроль и проверку правомочности обращений пользователей к объектам доступа, осуществляемые на основе прав доступа, определяемых разрешениями и ролями, присваиваемыми пользователям и группам пользователей в отношении объектов доступа и их содержимого. Разрешения определяют права доступа к объектам, а роли представляют собой именованные наборы разрешений. При включении пользователя в группу у него появляются все права, предоставленные группе, а при удалении пользователя из группы права группы у него пропадают. Пользователь, включенный в несколько групп, обладает всеми правами этих групп. Права могут быть не только приобретенными явным образом, но и наследованными, иначе говоря, перешедшими от верхнего по иерархии уровня. Создавший объект пользователь автоматически становится его владельцем и получает права на все действия с созданным объектом, включая определение прав доступа к нему для других пользователей.

1.4.2.3 Аудит

Средства, реализующие данную функцию, обеспечивают возможность регистрации данных о происходящих событиях и действиях пользователей. Регистрируемые данные хранятся в журнале аудита и могут быть просмотрены с помощью специально предназначенного для этого приложения в удобочитаемом виде с заданной степенью детализации. Возможности включения и выключения функций аудита, задания так называемых фильтров, определяющих какие данные и о каких событиях будут регистрироваться, настройки степени детализации и формы вывода данных аудита при их просмотре, а также сама возможность просмотра данных аудита предоставляется только пользователям с правами администратора. Простым непривилегированным пользователям эти возможности недоступны.

1.4.2.4 Управление безопасностью

Настройки механизмов обеспечения безопасности содержатся в системных конфигурационных файлах, которые можно редактировать. Дополнительными средствами управления механизмами обеспечения безопасности являются так называемые средства консоли администрирования и средства консоли администрирования репозитория, позволяющие управлять учетными записями

пользователей, задавать сценарии аутентификации и осуществлять распределение прав доступа к ресурсам системы на основе ролей.

2. Утверждения о соответствии

2.1 Утверждение о соответствии ГОСТ Р ИСО/МЭК 15408

Настоящее ЗБ основано на комплексе национальных стандартов Российской Федерации: ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности».

2.2 Утверждение о соответствии ПЗ

Настоящее ЗБ не претендует на соответствие какому-либо ПЗ.

2.3 Утверждение о соответствии пакетам

Настоящее ЗБ соответствует требованиям к разработке и производству, проведению испытаний и поддержке безопасности программного средства, соответствующего 4 уровню доверия согласно документу «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденному приказом ФСТЭК России от 2 июня 2020 г. № 76.

2.4 Обоснование соответствия

Включение требований доверия к ОО в настоящее ЗБ определяется «Требованиями по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденными приказом ФСТЭК России от 2 июня 2020 г. № 76.

3. Определение проблемы безопасности

Данный раздел содержит определение проблемы безопасности, а именно:

описание угроз безопасности, которым должны противостоять ОО и среда его функционирования;

описание политик безопасности, которые должны выполняться средствами ОО;

описание предположений относительно безопасности среды функционирования ОО.

3.1 Угрозы безопасности

Угроза безопасности-1

1. Аннотация угрозы – несанкционированный доступ к информационным ресурсам со стороны пользователей, для которых запрашиваемый доступ не разрешен.
2. Источники угрозы – внешний нарушитель, не являющийся зарегистрированным в ОО пользователем, или внутренний нарушитель, который является зарегистрированным в ОО пользователем, но не уполномочен на доступ к запрашиваемым информационным ресурсам.
3. Способ реализации угрозы – использование средств взаимодействия с ОО и маскировка под зарегистрированного в ОО уполномоченного пользователя путем подбора или восстановления его идентификационной и аутентификационной информации
4. Используемые уязвимости – недостатки механизмов идентификации и аутентификации, в том числе, касающиеся управления идентификационной и аутентификационной информацией.
5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, содержащаяся в объектах постоянной или временной памяти, включая определяющую функционал безопасности и данные функций безопасности.
6. Нарушаемые свойства безопасности информационных ресурсов – конфиденциальность, целостность, доступность.
7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, несанкционированные действия по отношению к информационным ресурсам, недоступность информации и функциональных возможностей.

Угроза безопасности-2

1. Аннотация угрозы – несанкционированный доступ к информационным ресурсам со стороны пользователей, для которых запрашиваемый доступ не разрешен.
2. Источники угрозы – внутренний нарушитель, который является зарегистрированным в ОО пользователем, но не уполномочен на доступ к запрашиваемым информационным ресурсам.

3. Способ реализации угрозы – использование средств взаимодействия с ОО и осуществление несанкционированного доступа к информационным ресурсам не имея на то полномочий.

4. Используемые уязвимости – недостатки механизмов управления доступом в том числе, касающиеся задания правил управления доступом.

5. Вид информационных ресурсов, потенциально подверженных угрозе – информация, содержащаяся в объектах постоянной или временной памяти, включая определяющую функционал безопасности и данные функций безопасности.

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

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, несанкционированные действия по отношению к информационным ресурсам, недоступность информации и функциональных возможностей.

Угроза безопасности-3

1. Аннотация угрозы – неправильное управление функционалом безопасности и данными функций безопасности со стороны уполномоченных субъектов доступа, для которых соответствующее управление разрешено.

2. Источники угрозы – внутренний нарушитель, который является зарегистрированным в ОО пользователем и уполномочен на доступ к функционалу безопасности и данным функций безопасности.

3. Способ реализации угрозы – использование средств взаимодействия с ОО и внесение изменений в системные конфигурационные файлы и данные функций безопасности.

4. Используемые уязвимости – недостатки механизмов контроля внесения изменений в функционал и данные функций безопасности.

5. Вид информационных ресурсов, потенциально подверженных угрозе – системные конфигурационные файлы и данные функций безопасности.

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

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, несанкционированные действия по отношению к информационным ресурсам, недоступность информации и функциональных возможностей.

3.2 Политики безопасности

Политика безопасности-1

Должны быть установлены и применяться правила идентификации и аутентификации, в соответствии с которыми доступ к функциональным возможностям и информационным ресурсам ОО должен предоставляться только уполномоченным пользователям, успешно прошедшим идентификацию и аутентификацию, должно осуществляться управление идентификационными и аутентификационными данными пользователей и их качеством.

Политика безопасности-2

Должны быть установлены и применяться правила управления доступом, в соответствии с которыми доступ к информационным ресурсам ОО должен предоставляться только уполномоченным пользователям, успешно прошедшим авторизацию, должно осуществляться задание правил управления доступом, определяющих для пользователей и ресурсов разрешенные типы доступа.

Политика безопасности-3

Должно осуществляться администрирование ОО, включающее регистрацию пользователей и управление их идентификационными и аутентификационными данными, а также задание правил управления доступом, определяющих для пользователей и информационных ресурсов разрешенные типы доступа. Доступ к средствам администрирования должен предоставляться только уполномоченным на это пользователям (администраторам), успешно прошедшим авторизацию.

Политика безопасности-4

Пользователи ОО должны быть подотчетны и нести ответственность за свои действия, имеющие отношение к безопасности. Должен осуществляться аудит событий безопасности с возможностью выборочного ознакомления с результатами аудита только для уполномоченных на это администраторов, успешно прошедших авторизацию.

3.3 Предположения безопасности

Предположение безопасности-1

Предполагается, что среда функционирования ОО является доверенной и обеспечивает безопасные установку, настройку и функционирование ОО в соответствии с эксплуатационной документацией; генерацию надежных меток времени; защиту информационных ресурсов от несанкционированного доступа, резервное копирование и восстановление работоспособности и ресурсов в случае отказов или аварийных ситуаций. Предполагается также, что ее администрирование и администрирование ОО согласованны и осуществляются в рамках единых требований безопасности.

Предположение безопасности-2

Предполагается, что средства вычислительной техники, на которых функционирует ОО, размещены в контролируемой зоне и обеспечивается их физическая защита, соизмеримая с ценностью защищаемых информационных ресурсов, и что все каналы связи между физически разделенными компонентами ОО и подключения к доверенным системам являются защищенными и обеспечивают конфиденциальность и целостность передаваемых данных.

Предположение безопасности-3

Предполагается, что авторизованные пользователи ОО уполномочены на доступ к выделенным и принадлежащим им информационным ресурсам, являются успешно обученными и имеющими практические навыки специалистами, выполняющими свои обязанности в соответствии с эксплуатационной документацией, содержащими в тайне свои аутентификационные данные и меняющими их с требуемой регулярностью.

Предположение безопасности-4

Предполагается, что администрирование и аудит ОО осуществляются авторизованными администраторами, уполномоченными на доступ к средствам администрирования и аудита, являющимися компетентными и опытными специалистами, выполняющими свои обязанности с соблюдением требований политик безопасности и эксплуатационной документации, и не являющимися беспечными, небрежным или преднамеренно враждебными.

4. Цели безопасности

Данный раздел содержит определение целей безопасности для ОО и среды его функционирования, а также обоснование того, что, если все цели безопасности будут достигнуты, то будет обеспечено противодействие всем угрозам безопасности, будут реализованы все политики безопасности и осуществлены все предположения.

4.1 Цели безопасности для ОО

Цель безопасности для ОО-1

ОО должен осуществлять идентифицикацию и аутентификацию пользователей до предоставления им доступа к своим функциональным возможностям, а также обеспечивать управление идентификационными и аутентификационными данными пользователей.

Цель безопасности для ОО-2

ОО должен предоставлять доступ к информационным ресурсам только успешно прошедшим авторизацию пользователям, а также обеспечивать уполномоченным на это пользователям задание правил управления доступом, определяющих для информационных ресурсов и других пользователей разрешенные типы доступа.

Цель безопасности для ОО-3

ОО должен предоставлять возможности и средства администрирования, позволяющие управлять функциями и атрибутами безопасности ОО, причем доступ к средствам администрирования должен предоставляться только уполномоченным на это администраторам, успешно прошедшим авторизацию.

Цель безопасности для ОО-4

ОО должен располагать возможностями и средствами аудита событий, относящихся к безопасности ОО, регистрируемые данные о событиях безопасности должны содержать идентификационную информацию пользователей, имеющих к ним отношение, должна предоставляться возможность выборочного просмотра данных аудита, доступ к средствам аудита должен предоставляться только уполномоченным на это администраторам, успешно прошедшим авторизацию.

4.2 Цели безопасности для среды функционирования ОО

Цель безопасности для среды функционирования ОО-1

Среда фунционирования ОО должна быть доверенной и обеспечивать безопасную доставку, установку, настройку и функционирование ОО в соответствии с эксплуатационной документацией; генерацию надежных меток времени; резервное копирование и безкомпрометационное восстановление работоспособности и информационных ресурсов ОО в случае отказов или аварийных ситуаций. Ее администрирование и администрирование ОО должны быть согласованными и осуществляться в рамках единых требований безопасности.

Цель безопасности для среды функционирования ОО-2

Средства вычислительной техники среды функционирования ОО должны быть размещены в контролируемой зоне и находиться под физической защитой, соизмеримой с ценностью защищаемых информационных ресурсов. Все каналы связи между физически разделенными компонентами ОО и подключения к доверенным системам должны быть защищены и обеспечивать конфиденциальность и целостность передаваемых данных.

Цель безопасности для среды функционирования ОО-3

Все пользователи должны успешно пройти обучение и иметь практические навыки работы с ОО, выполнять свои обязанности с учетом требований политик безопасности и эксплуатационной документации.

Цель безопасности для среды функционирования ОО-4

Все пользователи, назначаемые администраторами, должны быть компетентными и опытными, выполнять свои обязанности с соблюдением требований политик безопасности и эксплуатационной документации, быть заслуживающими доверия, внимательными, аккуратными и лояльными.

4.3 Обоснование целей безопасности

Достижение **Цели безопасности для ОО-1** обеспечит реализацию **Политики безопасности-1** и противодействие **Угрозе безопасности-1**, поскольку будет осуществляться идентифицикация и аутентификация пользователей до предоставления им доступа к функциональным возможностям

и ресурсам ОО, управление идентификационными и аутентификационными данными пользователей будет реализовано таким образом, чтобы доступ к функциональным возможностям ОО предоставлялся только пользователям, успешно прошедшим идентификацию и аутентификацию, подтверждающую правомочность такого доступа.

Достижение **Цели безопасности для ОО-2** обеспечит реализацию **Политики безопасности-2** и противодействие **Угрозе безопасности-2**, поскольку уполномоченным на это пользователям будет предоставлена возможность задания правил управления доступом, определяющих разрешенные типы доступа для информационных ресурсов, и разрешенные типы доступа будут предоставляться только пользователям, успешно прошедшим авторизацию, подтверждающую правомочность такого доступа.

Достижение **Цели безопасности для ОО-3** обеспечит реализацию **Политики безопасности-3** и противодействие **Угрозе безопасности-1, Угрозе безопасности-2**, поскольку будет осуществляться администрирование ОО, включающее присвоение всем пользователям идентификационных и аутентификационных данных, а также определение им разрешенных типов доступа в отношении конкретных информационных ресурсов, средства администрирования будут доступны только администраторам, успешно прошедшим авторизацию, подтверждающую правомочность такого доступа.

Достижение **Цели безопасности для ОО-4** обеспечит реализацию **Политики безопасности-4** и противодействие **Угрозе безопасности-1, Угрозе безопасности-2**, поскольку будет осуществляться аудит событий безопасности, содержащий идентификационную информацию пользователей с возможностью выборочного просмотра данных аудита, что позволит сделать всех пользователей ОО подотчетными и ответственными за действия, имеющие отношение к безопасности. Средства управления аудитом будут доступны только для уполномоченных на это администраторов, успешно прошедших авторизацию, подтверждающую правомочность такого доступа,

Достижение **Цели безопасности для среды функционирования ОО-1** обеспечит осуществление **Предположения безопасности-1**, поскольку среда функционирования ОО будет доверенной, с возможностью безопасной установки, настройки и поддержки функционирования ОО в соответствии с эксплуатационной документацией, с возможностью резервного копирования и безкомпрометационного восстановления работоспособности, режимов функционирования и информационных ресурсов ОО в случае отказов или аварийных ситуаций, а ее администрирование и администрирование ОО будут согласованными и осуществляться в рамках единых требований безопасности.

Достижение **Цели безопасности для среды функционирования ОО-2** обеспечит осуществление **Предположения безопасности-2**, поскольку средства вычислительной техники среды функционирования ОО будут размещены в контролируемой зоне и находиться под физической защитой, соизмеримой с ценностью защищаемых информационных ресурсов, а все каналы связи между физически разделенными компонентами ОО и подключения к доверенным

системам будут защищены и обеспечивать конфиденциальность и целостность передаваемых данных.

Достижение **Цели безопасности для среды функционирования ОО-3** обеспечит осуществление **Предположения безопасности-3**, реализацию **Политики безопасности-1, Политики безопасности-2**, противодействие **Угрозе безопасности-1, Угрозе безопасности-2**, поскольку все пользователи будут успешно обучены, будут иметь практические навыки работе с ОО, будут выполнять свои обязанности с учетом требований безопасности и эксплуатационной документации, т.е. сохраняя в тайне свои аутентификационные данные и ограничивая доступ к выделенным и используемым информационным ресурсам.

Достижение **Цели безопасности для среды функционирования ОО-4** обеспечит осуществление **Предположения безопасности-4**, реализацию **Политики безопасности-3,** противодействие **Угрозе безопасности-3**, поскольку будут назначаться компетентные и опытные администраторы, которые будут выполнять свои обязанности с соблюдением требований безопасности и эксплуатационной документации, будут внимательны, аккуратны и лояльны, не допустят к функционалу и данным функций безопасности неуполномоченных на это пользователей, и не будут вносить несанкционированных изменений в системные конфигурационные файлы и данные функций безопасности, приводящие к нарушениям требования безопасности.

Достаточность целей безопасности для нейтрализации угроз безопасности, реализации политик безопасности и обеспечения предположений безопасности обоснована следующим.

Угроза безопасности-1 нейтрализуется достижением **Цели безопасности для ОО-1,** требующей идентифицикации и аутентификации пользователей до предоставления им доступа к функциональным возможностям ОО, а также надлежащего управления идентификационными и аутентификационными данными пользователей; достижением **Цели безопасности для ОО-3**, требующей администрирования, позволяющего управлять функционалом и данными безопасности с предоставлением доступа к средствам администрирования только для уполномоченных администраторов, успешно прошедших авторизацию; достижением **Цели безопасности для ОО-4,** требующей организации аудита событий безопасности включающего идентификационную информацию пользователей и возможность выборочного просмотра данных аудита с предоставлением доступа к средствам аудита только уполномоченным на это администраторам, успешно прошедшим авторизацию; достижением **Цели безопасности для среды функционирования ОО-3,** требующей, чтобы все пользователи успешно прошли обучение и имели практические навыки работы с ОО, выполняли свои обязанности с учетом требований политик безопасности и эксплуатационной документации.

Угроза безопасности-2 нейтрализуется достижением **Цели безопасности для ОО-2,** требующей задания правил управления доступом, определяющих для информационных ресурсов и пользователей разрешенные типы доступа;

достижением **Цели безопасности для ОО-3,** требующей администрирования, позволяющего управлять функционалом и данными безопасности с предоставлением доступа к средствам администрирования только для уполномоченных администраторов, успешно прошедших авторизацию; достижением **Цели безопасности для ОО-4,** требующей организации аудита событий безопасности включающего идентификационную информацию пользователей и возможность выборочного просмотра данных аудита с предоставлением доступа к средствам аудита только уполномоченным на это администраторам, успешно прошедшим авторизацию; достижением **Цели безопасности для среды функционирования ОО-3,** требующей, чтобы все пользователи успешно прошли обучение и имели практические навыки работы с ОО, выполняли свои обязанности с учетом требований политик безопасности и эксплуатационной документации.

Угроза безопасности-3 нейтрализуется достижением **Цели безопасности для среды функционирования ОО-4,** требующей**,** чтобы назначаемые администраторы были профессионально подготовленными, компетентными и опытными, выполняли свои обязанности с соблюдением требований политик безопасности и эксплуатационной документации, были лояльными, внимательными и аккуратными.

Политика безопасности-1 реализуется с помощью достижения **Цели безопасности для ОО-1,** требующей идентифицикации и аутентификации пользователей до предоставления им доступа к функциональным возможностям ОО и надлежащего управления идентификационными и аутентификационными данными пользователей; достижением **Цели безопасности для среды функционирования ОО-3,** требующей, чтобы все пользователи успешно прошли обучение и имели практические навыки работы с ОО, выполняли свои обязанности с учетом требований политик безопасности и эксплуатационной документации.

Политика безопасности-2 реализуется с помощью достижения **Цели безопасности для ОО-2,** требующей задания правил управления доступом, определяющих для информационных ресурсов и пользователей разрешенные типы доступа; достижением **Цели безопасности для среды функционирования ОО-3,** требующей, чтобы все пользователи успешно прошли обучение и имели практические навыки работы с ОО, выполняли свои обязанности с учетом требований политик безопасности и эксплуатационной документации.

Политика безопасности-3 реализуется с помощью достижения **Цели безопасности для ОО-3,** требующей администрирования, позволяющего управлять функционалом и данными безопасности с предоставлением доступа к средствам администрирования только для уполномоченных администраторов, успешно прошедших авторизацию; достижением **Цели безопасности для среды функционирования ОО-4,** требующей**,** чтобы назначаемые администраторы были профессионально подготовленными, компетентными и опытными, выполняли свои обязанности с соблюдением требований политик

безопасности и эксплуатационной документации, были лояльными, внимательными и аккуратными.

Политика безопасности-4 реализуется с помощью достижения **Цели безопасности для ОО-4,** требующей организации аудита событий безопасности включающего идентификационную информацию пользователей и возможность выборочного просмотра данных аудита с предоставлением доступа к средствам аудита только уполномоченным на это администраторам, успешно прошедшим авторизацию.

Предположение безопасности-1 обеспечивается достижением **Цели безопасности для среды функционирования ОО-1,** требующей, чтобы среда фунционирования ОО должна быть доверенной, обеспечивала безопасное функционирование ОО в соответствии с эксплуатационной документацией, генерацию надежных меток времени, резервное копирование и безкомпрометационное восстановление работоспособности и информационных ресурсов ОО в случае отказов или аварийных ситуаций, и чтобы ее администрирование и администрирование ОО были согласованными и осуществлялись в рамках единых требований безопасности.

Предположение безопасности-2 обеспечивается достижением **Цели безопасности для среды функционирования ОО-2,** требующей, чтобы средства вычислительной техники среды функционирования ОО размещались в контролируемой зоне и находились под физической защитой, соизмеримой с ценностью защищаемых информационных ресурсов, и чтобы все каналы связи между физически разделенными компонентами ОО и подключения к доверенным системам были защищены и обеспечивали конфиденциальность и целостность передаваемых данных.

Предположение безопасности-3 обеспечивается достижением **Цели безопасности для среды функционирования ОО-3,** требующей, чтобы все пользователи успешно прошли обучение и имели практические навыки работы с ОО, выполняли свои обязанности с учетом требований политик безопасности и эксплуатационной документации.

Предположение безопасности-4 обеспечивается достижением **Цели безопасности для среды функционирования ОО-4,** требующей**,** чтобы назначаемые администраторы были профессионально подготовленными, компетентными и опытными, выполняли свои обязанности с соблюдением требований политик безопасности и эксплуатационной документации, были лояльными, внимательными и аккуратными.

В Таблице 4.1 приведена иллюстрация вышеизложенного сопоставления целей безопасности с угрозами безопасности, на противостояние которым они направлены, политиками безопасности, реализацию которых они обеспечивают, и предположениями безопасности, которые они поддерживают, демонстрирующая, что, если все цели безопасности будут достигнуты, то будет обеспечено противодействие всем угрозам безопасности, будут реализованы все политики безопасности и осуществлены все предположения безопасности.

Таблица 4.1 Сопоставление целей безопасности с угрозами безопасности, политикам безопасности и предположениям безопасности

	Цель безопасности для ОО-1	Цель безопасности для ОО-2	Цель безопасности для ОО-3	Цель безопасности для ОО-4	Цель безопасности для среды функционирования ОО-1	Цель безопасности для среды функционирования ОО-2	Цель безопасности для среды функционирования ОО-3	Цель безопасности для среды функционирования ОО-4
Угроза безопасности- 1	**X**		**X**	**X**			**X**	
Угроза безопасности- 2		**X**	**X**	**X**			**X**	
Угроза безопасности- 3								**X**
Политика безопасности-1	**X**						**X**	
Политика безопасности-2		**X**					**X**	
Политика безопасности-3			**X**					**X**
Политика безопасности-4				**X**				
Предположение безопасности-1					**X**			
Предположение безопасности-2						**X**		
Предположение безопасности-3							**X**	
Предположение безопасности-4								**X**

5. Использование расширенных компонентов

В настоящем ЗБ расширенные компоненты функциональных требований безопасности для ОО не используются.

6. Требования безопасности

В данном разделе определены требования безопасности для ОО, включающие функциональные требования безопасности и требования доверия к безопасности, которые должны быть выполнены, чтобы достигнуть

сформулированных выше целей безопасности для ОО, и которые согласуются с требованиями 4 уровня доверия, определенными в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденном приказом ФСТЭК России от 2 июня 2020 г. № 76.

Здесь представлено также сопоставление функциональных требований безопасности для ОО с ранее сформулированными целями безопасности для ОО и дано логическое обоснование для такого сопоставления, показывающее, что каждое функциональное требование безопасности для ОО сопоставлено, по крайней мере, с одной целью безопасности для ОО, и что все цели безопасности для ОО надлежащим образом учтены в функциональных требованиях безопасности для ОО.

Иначе говоря, если все функциональные требования безопасности для ОО выполнены, то все цели безопасности для ОО достигнуты и имеется доверие к тому, что всем угрозам обеспечено противостояние, все политики безопасности организации осуществлены и все предположения безопасности реализованы, т.е. проблема безопасности решена.

Требования безопасности для среды функционирования ОО здесь не определяются и не обосновываются, поскольку фактически они определены самими целями безопасности для среды функционирования ОО, сформулированными ранее.

6.1 Функциональные требования безопасности

Функциональные требования безопасности, определенные в настоящем ЗБ, основаны на компонентах функциональных требований безопасности, определенных в ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности», и перечислены ниже в Таблице 6.1.

Исходя из особенностей ОО при формулировании функциональных требований безопасности используются уточнения стандартных определений, отмечаемые жирным шрифтом.

6.1.1 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) все события, потенциально подвергаемые аудиту, на [**базовом]** уровне аудита;

б) [**все попытки аутентификации пользователя**].

Таблица 6.1 – Функциональные компоненты, на которых основаны функциональные требования безопасности

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
FDP_ACC.1	Ограниченное управление доступом
FDP_ACC.2	Полное 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_UID.2	Идентификация до любых действий пользователя
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными функций безопасности
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности

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

а) дата и время события, тип события, идентификатор объекта (в случае действий с объектами), результат события;

б) [имя пользователя].

Зависимости: FPT_STM.1 «Надежные метки времени».

FAU_GEN.2 Ассоциация идентификатора пользователя

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

Зависимости: FAU_GEN.1 Генерация данных аудита,
FIA_UID.1 Выбор момента идентификации.

FAU_SAR.1 Просмотр аудита

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

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **администратору** 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 **администраторов**, 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 использовать:[

а) поиск;

б) фильтацию;

в) выборку]

данных аудита, основанные на: [

а) имени пользователя,

б) типе события,

в) дате и времени события].

Зависимости: FAU_SAR.1 Просмотр аудита.

6.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять **[политику ролевого управления доступом]** для: **[**

а) субъектов: [пользователей];

б) объектов: [каталогов и их содержимого (подкаталогов, файлов), сайтов и их содержимого (документов, вики-страниц, записей блогов)];

в) действий с объектами: [создание, просмотр, копирование, редактирование, удаление]].

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

FDP_ACC.2 Полное управление доступом

FDP_ACC.2.1 ФБО должны осуществлять **[политику ролевого управления доступом]** для: **[**

а) субъектов: [пользователей];

б) объектов: [каталогов и их содержимого (подкаталогов, файлов), сайтов и их содержимого (документов, вики-страниц, записей блогов)]];

и всех **действий** субъектов **с** объектами, на которые распространяется политика ролевого управления доступом**].**

FDP_ACC.2.2 ФБО должны обеспечить, чтобы на **действия** любого субъекта, контролируемого ФБО, на любом объекте, контролируемом ФБО, распростанялась **политика ролевого управления доступом**.

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 ролевого управления доступом]** к объектам, основываясь на: **[**

а) атрибутах безопасности пользователей: [именах пользователей, членстве пользователей в различных группах];

б) атрибутах безопасности объектов: [идентификаторах объектов, допустимых для применения по отношению к объектам ролях для различных пользователей и групп и разрешенных действий с объектами для различных ролей]].

FDP_ACF.1.2 ФБО должны осуществлять следующие правила определения того, **разрешено** ли **действие** управляемого субъекта **с управляемым объектом [выполнение действия разрешается, если ассоциированный с субъектом пользователь может применить роль, для которой действие с объектом разрешено].**

FDP_ACF.1.3 ФБО должны явно разрешать **действия** субъектов доступа **с** объектам доступа, основываясь на следующих дополнительных правилах: **[нет дополнительных правил].**

FDP_ACF.1.4 ФБО должны явно отказывать в **действиях** субъектов **с** объектам доступа, основываясь на следующих дополнительных правилах: **[выполнение действия запрещается, если ассоциированный с субъектом пользователь не может применить роль, для которой действие с объектом разрешено].**

Зависимости: FDP_ACC.1 Ограниченное управление доступом,
FMT_MSA.3 Инициализация статических атрибутов.

6.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [**устанавленное администратором пороговое число (по умолчанию 5)]** неуспешных попыток аутентификации**,** относящихся к **[последовательным попыткам неуспешной аутентификации пользователя**].

FIA_AFL.1.2 При достижении **порогового числа** неуспешных попыток аутентификации ФБО должны: **[**

а) сделать невозможным доступ пользователя к ОО на установленное администратором время блокировки (по умолчанию 60 секунд);

б) по истечении времени блокировки осуществить сброс счетчика неуспешных попыток аутентификации пользователя].

Зависимости: FIA_UAU.1 Выбор момента аутентификации

FIA_ATD.1 Определение атрибутов пользователя

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

а) имя пользователя;

б) пароль;

в) статус текущего состояния учетной записи пользователя (включена, отключена, заблокирована, разблокирована);

г) членство пользователя в различных группах].

Зависимости: отсутствуют.

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 ФБО должны предоставить механизм для верификации того, что **пароли пользователей** отвечают **[следующей метрике качества:**

а) минимальная длина значения пароля должна быть не меньше установленного администратором количества символов (по умолчанию 8);

б) значение пароля не может содержать имя пользователя или какую-либо его часть;

в) в значении пароля должны присутствовать символы как минимум трех категорий из числа следующих:

прописные буквы английского алфавита от A до Z,

строчные буквы английского алфавита от a до z,

цифры от 0 до 9,

не принадлежащие алфавитно-цифровому множеству служебные символы].

Зависимости: отсутствуют.

FIA_UAU.2 Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Зависимости: FIA_UID.2 Выбор момента идентификации.

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Зависимости: отсутствуют.

6.1.4 Управление безопасностью (FMT)

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять **[политику ролевого управления доступом],** предоставляющую возможность: **[модифицировать]** атрибуты безопасности, **[перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1]** только: **[администратору, пользователю создавшему объект и являющемуся его владельцем, пользователям которым явно предоставлен доступ с использованием соответствующих ролей]**

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или FDP_IFC.1 Ограниченное управление информационными потоками], FMT_SMR.1 Роли безопасности, FMT_SMF.1 Спецификация функций управления.

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны позволять **[администратору]** определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта.

Зависимости: FMT_SMR.1 Роли безопасности,
FMT_MSA.1Управление атрибутами безопасности.

FMT_MTD.1 Управление данными ФБО

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

а) изменения значений умолчанию;

б) просмотра;

в) модификации]

следующих данных **[**

а) минимальная длина значения пароля;

б) пороговое число неуспешных попыток аутентификации относящихся к последовательным попыткам неуспешной аутентификации;

в) время блокировки пользователя при достижении порогового число неуспешных попыток аутентификации;

г) **статус текущего состояния учетной записи пользователя (включена, отключена);**

д) настройки аудита безопасности, определяющие запуск и завершение выполнения функций аудита, а также осуществление выборочного просмотра данных аудита]

только **[администратору].**

Зависимости: FMT_SMR.1 Роли безопасности;
FMT_SMF.1 Спецификация функций управления.

FMT_SMF.1 Спецификация функций управления

FMT_SMF.1.1 ФБО должны быть способны к выполнению следующих функций управления: [

а) запуск и завершение выполнения функций аудита;

б) настройка функций аудита для осуществления выборочного просмотра данных аудита согласно требованиям элемента FAU_SAR.3.1 компонента FAU_SAR.3:

в) определение и изменение атрибутов безопасности, используемых для осуществления политики ролевого управления доступом согласно требованиям элемента FDP_ACF.1.1 компонента FDP_ACF.1;

г) создание и модификация атрибутов безопасности пользователей, перечисленных в элементе FIA_ATD.1.1 компонента FIA_ATD.1;

д) изменение значений умолчанию, просмотр и модификация данных ФБО согласно требованиям элемента FMT_MTD.1.1 компонента FMT_MTD.1].

Зависимости: отсутствуют.

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО **по отношению к объектам** должны поддерживать следующие роли: **[**

а) роль «читатель» дает права только на просмотр и копирование объектов, но не дает права на их создание;

б) роль «корректор» дает права на просмотр и копирование объектов, а также на их загрузку, выгрузку и изменение свойств, но не дает права на их создание;

в) роль «писатель» дает права на создание, просмотр, копирование, редактирование и удаление принадлежащих ему объектов, но не дает права на редактирование или удаление объектов, созданных другими пользователями;

г) роль «редактор» дает права на создание, просмотр, копирование, редактирование и удаление принадлежащих ему объектов, а также на редактирование объектов, созданных другими пользователями, но без права на их удаление;

д) роль «координатор» дает права на создание, просмотр, копирование, редактирование и удаление объектов, созданных как им самим, так и другими пользователями;

е) роль «менеджер» дает права на создание, просмотр, копирование, редактирование и удаление объектов, созданных как им самим, так и другими пользователями, а также на определение по отношению к объектам допустимых ролей для пользователей и групп;

ж) роль «администратор» дает права на все действия со всеми объектами и на определение по отношению к ним допустимых ролей для всех пользователей и групп].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать пользователей с ролями **по отношению к объектам.**

Зависимости: FIA_UID.1 Выбор момента идентификации.

6.2. Требования доверия к безопасности

Требования доверия к безопасности ОО совпадают с требованиями к разработке, проведению испытаний и поддержке безопасности средства, соответствующего 4 уровню доверия согласно документу «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденному приказом ФСТЭК России от 2 июня 2020 г. № 76.

6.3 Обоснование требований безопасности

6.3.1 Обоснование функциональных требований безопасности

Ниже описано, каким образом выполнение функциональных требований безопасности способствует достижению целей безопасности для ОО**.**

FAU_GEN.1 Генерация данных аудита

Выполнение данного требования способствует достижению **Цели безопасности для ОО-4,** поскольку обеспечивает возможность регистрации событий, относящихся к безопасности ОО, с фиксацией даты и времени событий, идентификаторов субъектов и результатов событий, идентификационной информации пользователей, имеющих к ним отношение.

FAU_GEN.2 Ассоциация идентификатора пользователя

Выполнение данного требования способствует достижению **Цели безопасности для ОО-4,** поскольку обеспечивает возможность идентифицировать пользователей, которые были инициаторами регистрируемых событий безопасности.

FAU_SAR.1 Просмотр аудита

Выполнение данного требования способствует достижению **Цели безопасности для ОО-4,** поскольку обеспечивает возможность читать все записи аудита в виде, позволяющем воспринимать содержащуюся в них информацию.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение данного требования способствует достижению **Цели безопасности для ОО-4,** поскольку обеспечивает ограничение доступа к записям аудита и возможность их просмотра только для уполномоченных на это администраторов, успешно прошедших авторизацию.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение данного требования способствует достижению **Цели безопасности для ОО-4,** поскольку обеспечивает возможность выборочного просмотра записей аудита.

FDP_ACC.1 Ограниченное управление доступом

Выполнение данного требования способствует достижению **Цели безопасности для ОО-2,** поскольку обеспечивает возможность осуществления политики ролевого управления доступом субъектов к объектам.

FDP_ACC.2 Полное управление доступом

Выполнение данного требования способствует достижению **Цели безопасности для ОО-2,** поскольку обеспечивает возможность выполнения всех операций всех субъектов на всех объектах на которые распространяется политика ролевого управления доступом.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

Выполнение данного требования способствует достижению **Цели безопасности для ОО-2,** поскольку обеспечивает возможность осуществления политики ролевого управления доступа, основываясь на атрибутах безопасности субъектов и объектов, в том числе на ролях с учетом разрешенных для ролей типов доступа.

FIA_AFL.1 Обработка отказов аутентификации

Выполнение данного требования способствует достижению **Цели безопасности для ОО-1,** поскольку обеспечивает предотвращение подбора пароля перебором с ограничением количества неуспешных попыток пройти аутентификацию и их блокировкой.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение данного требования способствует достижению **Цели безопасности для ОО-1,** поскольку обеспечивает возможность управления идентификационными и аутентификационными данными пользователей.

FIA_SOS.1 Верификация секретов

Выполнение данного требования способствует достижению **Цели безопасности для ОО-1,** поскольку обеспечивает возможность верификации того, что пароли пользователей отвечают установленной метрике качества.

FIA_UAU.2 Аутентификация до любых действий пользователя

Выполнение данного требования способствует достижению **Цели безопасности для ОО-1,** поскольку предполагает аутентификацию пользователя до выполнения им любых действий по доступу к ресурсам ОО.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение данного требования способствует достижению **Цели безопасности для ОО-1,** поскольку предполагает идентификацию пользователя до выполнения им любых действий по доступу к ресурсам ОО.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение данного требования способствует достижению **Цели безопасности для ОО-3,** поскольку обеспечивает возможность управления атрибутами безопасности объектов при осуществлении политики ролевого управления доступом.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение данного требования способствует достижению **Цели безопасности для ОО-3,** поскольку обеспечивает возможность администратору определять и переопределять значения атрибутов безопасности, используемых для осуществления политики ролевого управления доступом.

FMT_MTD.1 Управление данными функций безопасности

Выполнение данного требования способствует достижению **Цели безопасности для ОО-3,** поскольку обеспечивает возможность определения и переопределения ограничительных значений параметров аутентификации только для администраторов.

FMT_SMF.1 Спецификация функций управления

Выполнение данного требования способствует достижению **Цели безопасности для ОО-3,** поскольку обеспечивает возможность управления атрибутами безопасности субъектов и объектов.

FMT_SMR.1 Роли безопасности

Выполнение данного требования способствует достижению **Цели безопасности для ОО-3,** поскольку обеспечивает возможность поддерживать роли и ассоциировать с ними пользователей.

Достаточность вышеперечисленных функциональных требований безопасности для достижения целей безопасности для ОО основана на нижеследующем.

Достижению **Цели безопасности для ОО-1** способствует выполнение требования безопасности **FIA_AFL.1**, обеспечивающего защиту от подбора пароля перебором с ограничением количества неуспешных попыток пройти аутентификацию и их блокировкой, требования безопасности **FIA_ATD.1**, обеспечивающего управление идентификационными и аутентификационными данными пользователей, требования безопасности **FIA_SOS.1**, обеспечивающего возможность верификации того, что пароли пользователей отвечают установленной метрике качества, требования безопасности **FIA_UAU.2**, обеспечивающего необходимость успешной аутентификации пользователя до выполнения им любых действий по доступу к ресурсам ОО, требования безопасности **FIA_UID.2**, обеспечивающего успешной идентификации пользователя до выполнения им любых действий по доступу к ресурсам ОО.

Достижению **Цели безопасности для ОО-2** способствует выполнение требования безопасности **FDP_ACC.1**, обеспечивающего реализацию политики ролевого управления доступом, требования безопасности **FDP_ACC.2**, обеспечивающего осуществление политики ролевого управления доступом в отношении всех субъектов, всех объектов и всех типов доступа, требования безопасности **FDP_ACF.1**, обеспечивающего управление доступом на основе атрибутов безопасности субъектов и объектов, в том числе допустимых ролей и разрешенных для них типов доступа.

Достижению **Цели безопасности для ОО-3** способствует выполнение требования безопасности **FMT_MSA.1**, обеспечивающего возможность управления атрибутами безопасности объектов только для уполномоченных на это пользователей, требования безопасности **FMT_MSA.3**, обеспечивающего возможность определения и переопределения функций и атрибутов безопасности, определяющих политику управления доступом, только для администраторов, требования безопасности **FMT_MTD.1**, обеспечивающего возможность установки и изменения ограничительных значений параметров аутентификации только для администраторов, требования безопасности **FMT_SMF.1**, обеспечивающего администраторам возможность управления атрибутами безопасности пользователей, требования безопасности **FMT_SMR.1**, обеспечивающего реализацию политики управления доступом на основе ролей и ассоциацию пользователей с ролями.

Достижению **Цели безопасности для ОО-4** способствует выполнение требования безопасности **FAU_GEN.1**, обеспечивающего регистрацию всех событий безопасности на базовом уровне аудита, требования безопасности **FAU_GEN.2**, обеспечивающего возможность ассоциации подвергаемых аудиту событий безопасности с идентификаторами пользователей, которые были инициаторами этих событий, требования безопасности **FAU_SAR.1**, обеспечивающего восприятие и интерпретацию содержащейся в записях аудита информации, требования безопасности **FAU_SAR.2**, обеспечивающего ограничение доступа к записям аудита за исключением пользователей, которым такой доступ явно предоставлен, требования безопасности **FAU_SAR.3**, обеспечивающего возможность выборочного просмотра записей аудита.

Таблица 6.2 – Отображение функциональных требований безопасности на цели безопасности для ОО

Функциональные требования безопасности	**Цель безопасности для ОО-1**	**Цель безопасности для ОО-2**	**Цель безопасности для ОО-3**	**Цель безопасности для ОО-4**
FAU_GEN.1				**X**
FAU_GEN.2				**X**
FAU_SAR.1				**X**
FAU_SAR.2				**X**
FAU_SAR.3				**X**
FDP_ACC.1		**X**		
FDP_ACC.2		**X**		
FDP_ACF.1		**X**		
FIA_AFL.1	**X**			
FIA_ATD.1	**X**			
FIA_SOS.1	**X**			
FIA_UAU.2	**X**			
FIA_UID.2	**X**			
FMT_MSA.1			**X**	
FMT_MSA.3			**X**	

Функциональные требования безопасности	Цель безопасности для ОО-1	Цель безопасности для ОО-2	Цель безопасности для ОО-3	Цель безопасности для ОО-4
FMT_MTD.1			**X**	
FMT_SMF.1			**X**	
FMT_SMR.1			**X**	

В Таблице 6.2 приведена иллюстрация вышеизложенного сопоставления функциональных требований безопасности с целями безопасности для ОО, демонстрирующая, что если все функциональные требования будут выполнены, то все цели безопасности для ОО будут достигнуты.

6.3.2 Обоснование удовлетворения зависимостей функциональных требований безопасности

В Таблице 6.3 представлены результаты удовлетворения зависимостей функциональных требований безопасности.

Третий столбец таблицы показывает, какие компоненты требований были включены в настоящем ЗБ для удовлетворения зависимостей компонентов, приведенных в первом столбце.

Компоненты требований в третьем столбце таблицы либо совпадают с компонентами во втором столбце, либо иерархичны по отношению к ним. Это свидетельствует, что все зависимости компонентов требований в настоящем ЗБ удовлетворены. Для компонента FAU_GEN.1 невключение по зависимости компонента FPT_STM.1 компенсировано включением в ЗБ Цели для среды функционирования ОО-4.

6.3.3 Обоснование требований доверия к безопасности объекта оценки

Требования доверия к безопасности ОО настоящего ЗБ совпадают с требованиями к разработке и производству, проведению испытаний и поддержке безопасности средства, соответствующего 4 уровню доверия, согласно документу «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденному приказом ФСТЭК России от 2 июня 2020 г. № 76.

Таблица 6.3 – Зависимости функциональных требований безопасности

Функциональные требования безопасности	**Зависимости функциональных требований безопасности**	**Удовлетворение зависимостей**
FAU_GEN.1	FPT_STM.1	Цель для среды функционирования ОО-4
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
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACC.2	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_ATD.1	Отсутствуют	Не требуется
FIA_SOS.1	Отсутствуют	Не требуется
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	Отсутствуют	Не требуется
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	Отсутствуют	Не требуется
FMT_SMR.1	FIA_UID.1	FIA_UID.2

7 Краткая спецификация ОО

В данном разделе представлено краткое описание того, каким образом реализованные в ОО функции безопасности удовлетворяют всем компонентам функциональных требований безопасности, а также описание осуществляемых мер доверия, удовлетворяющих требованиям доверия к безопасности ОО.

7.1 Функции безопасности ОО

Имеющиеся в ОО средства реализуют следующие функции безопасности: идентификация и аутентификация, управление доступом, аудит, управление безлопасностью.

7.1.1 Идентификация и аутентификация

Доступ к ОО и его ресурсам возможен только для зарегистрированных пользователей, успешно прошедших идентификацию и аутентификацию.

Регистрация пользователя осуществляется с помощью средств управления пользователями консоли администрирования путем определения значений атрибутов безопасности, ассоциированных с его учетной записью (имя, пароль), на основе которых он становится обладателем соответствующих прав доступа. Если при идентификации пользователем будет предъявлено недействительное имя, то ему будет отказано в доступе и выдано соответствующее сообщение об ошибке. Если при аутентификации пользователь предъявит неверный пароль, то ему будет отказано в доступе и выдано сообщение о том, что его данные аутентификации неверны. Если пользователем будет достигнуто так называемое пороговое число неуспешных попыток аутентификации, относящихся к последовательным попыткам аутентификации, то его учетная запись будет заблокирована на заданное время, по истечении которого счетчик неуспешных попыток аутентификации будет сброшен (обнулен). Пароль пользователя может быть изменен, но с целью обеспечения безопасности его длина в символах не должна быть меньше установленной минимальной длины пароля, он не должен содержать часть имени пользователя и в нем должны присутствовать символы как минимум трех категорий из числа следующих: прописные буквы английского алфавита, строчные буквы английского алфавита, цифры, не принадлежащие алфавитно-цифровому множеству служебные символы. Невыполнение перечисленных ограничений будет сопровождаться выдачей соответствующих сообщений об ошибке.

Таким образом, реализованные в ОО средства идентификации и аутентификации обеспечивают выполнение следующих ФТБ: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2.

7.1.2 Управление доступом

Управление доступом в ОО осуществляется на основе прав доступа, определяемых разрешениями и ролями, которые присваиваются пользователям и группам пользователей в отношении объектов доступа и их содержимого.

Разрешения определяют права доступа к объектам, а роли представляют собой именованные наборы разрешений. Действие пользователя с объектом разрешается, если он может применить роль, для которой действие с объектом разрешено. Выполнение действия запрещается, если пользователь не может применить роль, для которой действие с объектом разрешено. Включение пользователей в группы осуществляется с помощью средств управления группами консоли администрирования. При включении пользователя в группу у него появляются все права, предоставленные группе, а при удалении пользователя из группы права группы у него пропадают. Пользователь, включенный в несколько групп, обладает всеми правами этих групп. Присвоение ролей пользователям и группам осуществляется с помощью средств настройки прав доступа к объектам. Права доступа могут быть не только приобретенными явным образом, но и наследованными, иначе говоря, перешедшими от верхнего по иерархии уровня. Создавший объект пользователь автоматически становится его владельцем и получает права на все действия с созданным объектом, включая определение прав доступа к нему для других пользователей.

Таким образом, реализованные в ОО средства управления доступом обеспечивают выполнение следующих ФТБ: FDP_ACC.1, FDP_ACC.2, FDP_ACF.1.

7.1.3 Аудит

Для осуществления контроля за состоянием безопасности в ОО предусмотрены средства аудита, осуществляющие регистрацию данных о событиях безопасности и предоставляющие возможности их просмотра.

Регистрируемые данные хранятся в так называемом журнале аудита и могут быть просмотрены с помощью специального предназначенного для этого приложения, доступного только пользователям с правами администратора. Обычные непривилегированные пользователи не имеют прав доступа к данным аудита. Просмотр журнала аудита с помощью специального приложения может быть настроен требуемым образом, с поиском, фильтрацией, упорядочиванием, с учетом необходимости отображения с заданной детализацией: имен пользователей, к действиям которых относятся регистрируемые данные аудита, дат и времени действий, результирующих значений действий, адресных ссылок на объекты, по отношению к которым осуществлялись действия, а также других сведений.

Таким образом, реализованные в ОО средства аудита обеспечивают выполнение следующих ФТБ: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3.

7.1.4 Управление безопасностью

Управление механизмами обеспечения безопасности ОО осуществляется путем настройки значений соответствующих параметров, содержащихся в системных конфигурационных файлах, возможность которой предоставляется только пользователям с правами администратора.

Управлять парольной аутентификацией можно корректируя установленные по умолчанию ограничительные значения параметров аутентификации, содержащихся в конфигурационном файле alfresco-global.properties, а именно: infooborot.auth.maxNumberOfFailedAttempts (пороговое число неуспешных попыток аутентификации, относящихся к последовательным попыткам неуспешной аутентификации, при достижении которого учетная запись пользователя блокируется на заданное время блокировки, значение по умолчанию равно 5), infooborot.auth.numberOfMinutesToLockFor (время блокировки учетной записи пользователя в минутах при достижении порогового числа неуспешных попыток аутентификации, по истечении которого осуществляется сброс счетчика неуспешных попыток аутентификации, значение по умолчанию равно 30), infooborot.password.min.length (минимально допустимая длина значения пароля, значение по умолчанию равно 8). Список определений для разрешений по умолчанию, содержится в конфигурационном файле permissionDefinitions, а параметры настройки ролевого управления доступом заданы в конфигурационном файле authority-servises-context. Запуск (включение) и завершение (выключение) выполнения функций аудита может осуществляться путем редактирования значений параметров audit.enable = true/false и audit.alfresco-access.enabled = true/false вышеупомянутого конфигурационного файла alfresco-global.properties.

Таким образом, реализованные в ОО средства управления безопасностью обеспечивают выполнение следующих ФТБ: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

Ниже в Таблице 7.1 представлено обобщенное сопоставление всех вышеописанных функций безопасности и сформулированных в предыдущем разделе функциональных требований безопасности, демонстрирующее, что с помощью реализованных в ОО функций безопасности обеспечивается выполнение всех функциональных требований безопасности.

Таблица 7.1 – Сопоставление функций безопасности с функциональными требованиями безопасности

Функциональные требования безопасности	Идентификация и аутентификация	Управление доступом	Управление безопасностью	Аудит
FAU_GEN.1				**X**
FAU_GEN.2				**X**
FAU_SAR.1				**X**
FAU_SAR.2				**X**
FAU_SAR.3				**X**
FDP_ACC.1		**X**		
FDP_ACC.2		**X**		
FDP_ACF.1		**X**		
FIA_AFL.1	**X**			
FIA_ATD.1	**X**			
FIA_SOS.1	**X**			
FIA_UAU.2	**X**			
FIA_UID.2	**X**			
FMT_MSA.1			**X**	
FMT_MSA.3			**X**	
FMT_MTD.1			**X**	
FMT_SMF.1			**X**	
FMT_SMR.1			**X**	

7.2 Меры доверия к безопасности ОО

Для удовлетворения требований доверия к безопасности ОО были предприняты меры, касающиеся разработки и производства, проведения испытаний и поддержки безопасности.

7.2.1 Разработка и производство

При разработке были предприняты следующие меры:

разработана непротиворечивая модель безопасности, отражающая реализуемую политику управления доступом;

спроектирована архитектура безопасности, обеспечивающая защищенность процесса инициализации и невозможность обхода функциональных возможностей, осуществляющих выполнение функциональных требований безопасности;

разработана функциональная спецификация, описывающая интерфейсы функций безопасности (ИФБО), их назначения и способы использования, связанные с ними режимы функционирования, параметры и действия;

разработан проект на уровне подсистем и модулей, реализующих ИФБО, упомянутые в функциональной спецификации, в котором описано взаимодействие подсистем и модулей между собой, прослеживание их к соответствующим ИФБО, приведен перечень файлов исходных текстов программного обеспечения с указанием значений контрольных сумм и прослеживание их к соответствующим модулям, приведенным в описании проекта;

разработано описание примененных для создания инструментальных средств разработки, содержащее перечень используемых языков программирования, компиляторов, программных библиотек, отдельных инструментальных программных средств, а также описание порядка компиляции и сборки инсталляционного дистрибутива из исходных текстов;

разработан и выполняется план управления конфигурацией, устанавливающий порядок идентификации, учета, контроля и аудита всех элементов и составных частей конфигурации с целью обеспечения ее управляемости;

разработана документация по безопасной разработке, описывающая используемую модель жизненного цикла и содержание всех физических, процедурных, организационных и других мер безопасности, необходимых для защиты конфиденциальности и целостности проекта на всем протяжении его жизненного цикла;

разработано руководство пользователя, содержащее описание принципов безопасной работы, возможных и доступных функций безопасности, включая параметры и режимы функционирования, описание мер безопасности, направленных на достижение имеющих отношение к пользователям целей безопасности, а также руководство администратора, содержащее описание порядка и процедур безопасной приемки, установки, настройки и контроля функционирования в процессе эксплуатации, описание других мер безопасности, предназначенных для достижения имеющих отношение к администрированию целей безопасности.

7.2.2 Проведение испытаний

В ходе проведения испытаний разработан и выполнен план тестирования, включающий сравнение ожидаемых и фактических результатов тестирования функций безопасности, анализ покрытия тестами и анализ глубины тестирования, свидетельствующие о том, что все функции безопасности реализованы в соответствии с проектными спецификациями, и что фактические результаты тестирования соответствуют ожидаемым, а также включающий проведение испытаний по выявлению уязвимостей и недекларированных возможностей и проведение анализа скрытых каналов.

7.2.3 Поддержка безопасности

Поддержка безопасности обеспечивается регламентацией и соблюдением процедур безопасной поставки потребителям, мониторинга обнаруженных недостатков, разработки исправляющих обновлений, анализа влияния обновлений на задание по безопасности и реализованные функции безопасности, информирования пользователей о недостатках и предоставления им исправляющих обновлений с соответствующими инструкциями по установке, информирования об окончании производства и (или) поддержки.