

СОГЛАСОВАНО

Начальник 4 отдела 2 управления
ФСТЭК России

Ю.Попов

« » _____ 2005 года

УТВЕРЖДАЮ

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
ООО «МАЙКРОСОФТ РУС»

Б.СТЕЕН

« » _____ 2005 года

**ОФИСНЫЙ ПРОГРАММНЫЙ КОМПЛЕКС
MICROSOFT® OFFICE
ПРОФЕССИОНАЛЬНЫЙ ВЫПУСК 2003
РУССКАЯ ВЕРСИЯ
ЗАДАНИЕ ПО БЕЗОПАСНОСТИ
MS.OFFICE2003.3Б**

Версия 1.0

СОДЕРЖАНИЕ

1	ВВЕДЕНИЕ ЗБ	5
1.1	Идентификация ЗБ	5
1.2	Аннотация ЗБ	6
1.3	Соответствие ОК	6
1.4	Соглашения	7
1.5	Термины и определения	7
1.6	Организация ЗБ	10
2	ОПИСАНИЕ ОО	11
2.1	Тип продукта ИТ	11
2.2	Основные функциональные возможности ОО	11
2.2.1	<i>Основные функциональные возможности обеспечения функционирования.</i>	<i>11</i>
2.2.2	<i>Основные функциональные возможности обеспечения безопасности</i>	<i>13</i>
2.3	Границы ОО	16
2.4	Службы безопасности ОО	17
	<i>Защита данных пользователя</i>	<i>17</i>
3	СРЕДА БЕЗОПАСНОСТИ ОО	18
3.1	Предположения безопасности	18
3.1.1	<i>Предположения относительно предопределенного использования ОО</i>	<i>18</i>
3.1.2	<i>Предположения относительно среды функционирования ОО</i>	<i>19</i>
3.2	Угрозы	19
3.2.1	<i>Угрозы, которым противостоит ОО</i>	<i>19</i>
3.2.2	<i>Угрозы, которым противостоит среда</i>	<i>25</i>
3.3	Политика безопасности организации	27
4	ЦЕЛИ БЕЗОПАСНОСТИ	29
4.1	Цели безопасности для ОО	29
4.2	Цели безопасности для среды	31
5	ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ	34
5.1	Требования безопасности для ОО	34
5.1.1	<i>Функциональные требования безопасности ОО</i>	<i>34</i>
5.1.2	<i>Требования доверия к безопасности ОО</i>	<i>56</i>
5.2	Требования безопасности для среды ИТ	61
5.2.1	<i>Идентификация и аутентификация (FIA)</i>	<i>62</i>

5.2.2	Защита ФБО (FPT).....	63
6	КРАТКАЯ СПЕЦИФИКАЦИЯ ОО.....	64
6.1	ФУНКЦИИ БЕЗОПАСНОСТИ ОО.....	64
6.1.1	Функции безопасности ОО «Защита данных пользователя».....	64
6.1.2	Функции безопасности ОО «Идентификация и аутентификация».....	75
6.1.3	Функции безопасности ОО «Управление безопасностью».....	77
6.1.4	Функции безопасности ОО «Защита ФБО».....	83
6.1.5	Функции безопасности ОО «Управление доступом к ОО».....	86
6.2	МЕРЫ ДОВЕРИЯ К БЕЗОПАСНОСТИ ОО.....	90
6.2.1	Управление конфигурацией.....	90
6.2.2	Представление руководств.....	90
6.2.3	Представление проектной документации.....	91
6.2.4	Тестирование.....	92
6.2.5	Оценка стойкости функций безопасности.....	92
7	УТВЕРЖДЕНИЯ О СООТВЕТСТВИИ ПЗ.....	93
7.1	ССЫЛКА НА ПЗ.....	93
7.2	КОНКРЕТИЗАЦИЯ ПЗ.....	93
7.3	ДОПОЛНЕНИЕ ПЗ.....	95
8	ОБОСНОВАНИЕ.....	97
8.1	ОБОСНОВАНИЕ ЦЕЛЕЙ БЕЗОПАСНОСТИ.....	97
8.1.1	Обоснование целей безопасности для ОО.....	97
8.1.2	Обоснование целей безопасности для среды.....	100
8.2	ОБОСНОВАНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ.....	104
8.2.1	Обоснование требований безопасности для ОО.....	104
8.2.2	Обоснование требований безопасности для среды ИТ.....	115
8.2.3	Обоснование зависимостей требований.....	117
8.3	ОБОСНОВАНИЕ КРАТКОЙ СПЕЦИФИКАЦИИ ОО.....	121
8.4	ОБОСНОВАНИЕ ТРЕБОВАНИЙ К СТОЙКОСТИ ФУНКЦИЙ БЕЗОПАСНОСТИ.....	124
8.5	ОБОСНОВАНИЕ УТВЕРЖДЕНИЙ О СООТВЕТСТВИИ ПЗ.....	125
8.5.1	Обоснование конкретизации требований безопасности ИТ.....	125
8.5.2	Обоснование добавления политик безопасности организации.....	125
8.5.3	Обоснование добавления целей безопасности для ОО.....	126
8.5.4	Обоснование добавления требований безопасности ИТ.....	126

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АС	– автоматизированная система
БД	– база данных
ИТ	– информационные технологии
ОДФ	– область действия ФБО
ОК	– Общие критерии
ОО	– объект оценки
ОС	– операционная система
ОУД	– оценочный уровень доверия к безопасности
ПБО	– политика безопасности ОО
ПЗ	– профиль защиты
ПФБ	– политика функции безопасности
СФБ	– стойкость функции безопасности
ФБО	– функции безопасности ОО
ФТБ	– функциональные требования безопасности
IRM	– Information Right Management
RMS	– Right Management Services
XML	– Extensible Markup Language

1 Введение ЗБ

Данный раздел содержит информацию общего характера. Подраздел «Идентификация ЗБ» предоставляет маркировку и описательную информацию, которые необходимы, чтобы контролировать и идентифицировать ЗБ и ОО, к которому оно относится. Подраздел «Аннотация ЗБ» содержит общую характеристику ЗБ, позволяющую определить применимость ОО, к которому относится настоящее ЗБ, 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 ЗБ. В подразделе «Организация ЗБ» дается пояснение организации документа.

1.1 Идентификация ЗБ

Название ЗБ:	Офисный программный комплекс Microsoft® Office. Профессиональный выпуск 2003. Русская версия. Задание по безопасности.
Версия ЗБ:	Версия 1.0.
Обозначение ЗБ:	MS.Office2003.ЗБ.
Идентификация ОО:	Офисный программный комплекс Microsoft® Office. Профессиональный выпуск 2003. Русская версия.
Уровень доверия:	ОУД1, усиленный компонентом AVA_SOF.1 (Оценка стойкости функции безопасности).
Идентификация ОК:	ГОСТ Р ИСО/МЭК 15408–2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. Руководящий документ Безопасность информационных технологий Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель, Гостехкомиссия России, 2002. Руководящий документ Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные

требования безопасности, Гостехкомиссия России, 2002.

Руководящий документ Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.

Ключевые слова: Офисный программный комплекс, средство защиты информации, задание по безопасности, ОУД1, Microsoft®.

1.2 Аннотация ЗБ

Настоящее ЗБ определяет требования безопасности для программного комплекса «Офисный программный комплекс Microsoft® Office. Профессиональный выпуск 2003. Русская версия» (далее – офисный программный комплекс Microsoft® Office 2003).

Офисный программный комплекс Microsoft® Office 2003 состоит из комплекса программ (компонентов), предназначенных для организации офисного рабочего места и решения стандартных офисных задач, включая организацию групповой работы.

1.3 Соответствие ОК

Объект оценки и ЗБ согласованы со следующими спецификациями:

- ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005» (**соответствие ПЗ** – ОО соответствует всем частям данного ПЗ);
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002 (**расширение части 2 ОК** – ОО соответствует функциональным требованиям, основанным на функциональных компонентах из части 2 ОК, а также включающим функциональные компоненты, не содержащиеся в части 2 ОК);
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002 (**усиление части 3 ОК** – требования доверия представлены в виде ОУД1 и, кроме того, включают компонент AVA_SOF.1 из части 3 ОК).

1.4 Соглашения

Руководящий документ Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (далее – Общие критерии) допускает выполнение определенных в части 2 ОК операций над функциональными требованиями. Соответственно в настоящем ЗБ 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 ЗБ обозначается полужирным текстом.

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

Операция **«назначение»** используется для присвоения конкретного значения ранее не конкретизированному параметру. Результат операции **«назначение»** в настоящем ЗБ обозначается заключением значения параметра в квадратные скобки, [назначаемое значение].

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

В настоящее ЗБ включены компоненты функциональных требований безопасности, сформулированные в явном виде. Краткая форма имени функциональных компонентов, сформулированных в явном виде, содержит текст (EXT).

1.5 Термины и определения

В настоящем ЗБ применяются следующие термины с соответствующими определениями.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

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

Адресная книга – инструментарий, представляющий собой набор адресных книг и списков адресов, содержащий контактную информацию по всем пользователям ОО и внешним пользователям и предназначенный для поиска и выбора имен пользователей ОО и внешних пользователей, адресов электронной почты и списков рассылки, а также другой контактной информации.

Активы – информация или ресурсы, подлежащие защите контрмерами ОО.

Вредоносный программный код – завуалированная («замаскированная») программная конструкция, находящаяся в составе защищаемого объекта, наличие которой при определенных условиях нарушает свойства безопасности активов.

Встроенный программный код – исполняемый программный код или интерпретированный набор инструкций, встроенный непосредственно в документ.

Документ – файл, содержащий данные, созданные с использованием ОО.

Достоверность – свойство безопасности активов, обеспечивающее соответствие предусмотренным значениям.

Доступность – свойство безопасности активов, обеспечивающее возможность доступа и готовность к использованию на запрос уполномоченного объекта или субъекта.

Зависимость – соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть удовлетворено, чтобы и другие требования могли отвечать своим целям.

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО (в данном случае – офисный программный комплекс Microsoft® Office 2003).

Идентификатор – уникальный признак администратора ОО или пользователя ОО, однозначно его идентифицирующий.

Конфиденциальность – свойство безопасности активов предотвращать возможность доступа к информации и/или ее раскрытия неуполномоченным лицам, объектам или процессам.

Метаданные – данные, содержащие сведения о документе, встроенные непосредственно в документ (например, сведения о разработчике документа, версии документа).

Объект – сущность в пределах ОДФ, которая содержит или получает информацию, и над которой субъекты выполняют операции.

Объект оценки – подлежащий оценке офисный программный комплекс Microsoft® Office 2003 с руководствами по эксплуатации.

Подконтрольность – свойство безопасности активов, обеспечивающее однозначное отслеживание действий объектов и субъектов информационных отношений.

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

Политика функции безопасности – политика безопасности, осуществляемая ФБ.

Пользователь – любая сущность (человек-пользователь или внешняя сущность ИТ) вне ОО, которая взаимодействует с ОО.

Программный вирус – исполняемый программный код или интерпретированный набор инструкций, обладающий свойством несанкционированного распространения и самовоспроизведения (репликации).

Продукт ИТ – совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы (в данном случае продукт ИТ совпадает с ОО, идентифицированным в настоящем ЗБ).

Профиль защиты – независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

Ресурс ОО – все, что может использоваться или потребляться в ОО (вычислительные возможности, физическая память, дисковое пространство).

Система ИТ – специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Субъект ОО (субъект доступа) – сущность в пределах ОДФ, которая инициирует выполнение операций.

Функции безопасности ОО – совокупность всех функций безопасности ОО, направленных на осуществление ПБО.

Функция безопасности – функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО.

Целостность – свойство безопасности активов, обеспечивающее поддержание полноты и неизменности информации.

1.6 Организация ЗБ

Раздел 1 «Введение ЗБ» содержит информацию управления документооборотом и описательную информацию, необходимую для идентификации ЗБ 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 продукта.

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 ОК определены, соответственно, функциональные требования безопасности ИТ и требования доверия к безопасности ОО.

В раздел 6 «Краткая спецификация ОО» включено описание реализуемых ОО функций безопасности ИТ, соответствующих специфицированным в ЗБ функциональным требованиям безопасности, а также мер доверия к безопасности, соответствующих специфицированным в ЗБ требованиям доверия к безопасности ОО.

В разделе 7 «Утверждения о соответствии ПЗ» идентифицируется ПЗ, о соответствии которому заявляется в ЗБ, а также дополнения и уточнения аспектов среды безопасности, целей и требований безопасности.

В Разделе 8 «Обоснование» демонстрируется, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что ОО учитывает идентифицированные аспекты среды безопасности ИТ, а также что функции безопасности ИТ и меры доверия к безопасности соответствуют требованиям безопасности ОО.

2 Описание ОО

Объектом оценки является офисный программный комплекс Microsoft® Office 2003.

2.1 Тип продукта ИТ

Объект оценки – комплекс программ (компонентов) предназначенных для организации офисного рабочего места и решения стандартных офисных задач, включая организацию групповой работы.

Объект оценки состоит из следующих компонентов:

- Microsoft® Office Word 2003;
- Microsoft® Office Excel 2003;
- Microsoft® Office Outlook® 2003 с Диспетчером контактов;
- Microsoft® Office PowerPoint® 2003;
- Microsoft® Office Access 2003;
- Microsoft® Office Publisher 2003.

Компоненты могут функционировать независимо друг от друга и использовать в процессе функционирования результаты работы каждого из компонентов. ОО предоставляет возможность осуществлять настройку безопасности отдельно для каждого компонента. Настройка безопасности ОО (каждого компонента ОО) может осуществляться как непосредственно средствами самого ОО, так и средствами клиентских и серверных ОС.

2.2 Основные функциональные возможности ОО

2.2.1 Основные функциональные возможности обеспечения функционирования Текстовый редактор Microsoft® Office Word 2003

Текстовый редактор Microsoft® Office Word 2003 предназначен для создания и редактирования документов, располагает средствами позволяющими оформлять документы надлежащим образом и выводить на печать. В текстовый редактор встроен модуль проверки орфографии на русском и английском языках (при необходимости в текстовый процессор могут быть встроены другие языки). Текстовый редактор Microsoft® Office Word 2003 поддерживает возможность ведения версий документов. Для часто

используемых видов документов (письма, отчеты, доклады и т.д.) имеется возможность использования «шаблонов» документов. В текстовый редактор интегрированы средства организации групповой работы, позволяющие осуществлять коллективную разработку и сопровождение документов.

Средство работы с электронными таблицами Microsoft® Office Excel 2003

Средство работы с электронными таблицами Microsoft® Office Excel 2003 предназначено для обработки информации, представленной в табличном виде (электронных таблиц). Microsoft® Office Excel 2003 снабжено всем необходимым инструментарием для создания, надлежащего оформления и сопровождения электронных таблиц, выдачи и оформления результатов работы. Наряду с текстовым редактором средство работы с электронными таблицами Microsoft® Office Excel 2003 интегрированы средства организации групповой работы, позволяющие осуществлять коллективную разработку и сопровождение электронных таблиц.

Средство работы с презентациями (компьютерными слайдами) Microsoft® Office PowerPoint® 2003

Средство работы с презентациями (компьютерными слайдами) предназначено для оформления информационного содержимого в наглядной форме (презентации), позволяющей проводить презентационные мероприятия и отображать презентаций на экран монитора или посредством проектора.

Диспетчер личных данных и клиент электронной почты Microsoft® Office Outlook® 2003

Microsoft® Office Outlook® 2003 представляет собой программное средство для работы с сообщениями электронной почты, календарными планами, а также планирования собраний и управления ресурсами. Клиент электронной почты снабжен всем необходимым инструментарием для формирования электронных сообщений и включает адресную книгу, содержащую всю контактную информацию по пользователям, с которыми осуществляется информационный обмен в рамках электронной почты.

Настольная система управления базами данных Microsoft® Office Access 2003

Настольная система управления базами данных Microsoft® Office Access 2003 представляет собой приложение, предназначенное для управления реляционными базами

данных со встроенными средствами для создания запросов, отчетов, ввода данных, анализа и построения диаграмм.

Система подготовки публикаций Microsoft® Office Publisher 2003

Система подготовки публикаций Microsoft® Office Publisher 2003 предназначена для создания, оформления и публикации в электронном виде различных графических материалов (бюллетеней, брошюр, объявлений, открыток, бланков и т.п.).

2.2.2 Основные функциональные возможности обеспечения безопасности

К основным функциональным возможностям обеспечения безопасности ОО относятся следующие:

- управление правами на доступ к данным;
- защита документов с помощью пароля;
- ограничения по изменению и форматированию документов;
- ограничение распространения метаданных;
- защита адресной книги;
- блокировка вложений сообщений электронной почты;
- управление уровнем безопасности для макросов;
- безопасность пакетов расширения XML;
- обеспечение безопасного способа завершения работы приложения, которое прекратило отвечать на запросы;
- автоматическое восстановление данных;
- восстановление документов и извлечение из них данных, которые невозможно исправить.

Управление доступом к данным

Объект оценки реализует политику управления доступом к данным документов. ФБО обеспечивают опосредованный доступ между субъектами (пользователями ОО и внешними пользователями) и объектами (данными документов). Решение о доступе принимается на основе сравнительного анализа атрибутов безопасности, связанных с запрашивающим субъектом, и атрибутов безопасности, связанных с объектом, к которому осуществляется доступ. Атрибуты безопасности субъекта включают идентификатор пользователя, идентификатор стиля и введенный пароль при доступе к документу.

Атрибуты объекта включают список доступа, список разрешенных стилей, пароль для доступа к документу на чтение, пароль для доступа к документу на изменение. Такие атрибуты безопасности данных документа, как список доступа, в котором указываются идентификаторы пользователей, которым разрешена модификация данных документа и список разрешенных стилей, в котором указываются идентификаторы стилей, разрешенных к использованию в документе, составляют дополнительные атрибуты безопасности данных документа.

Объект оценки реализует политику управления доступом к адресной книге. ФБО обеспечивают опосредованный доступ между субъектами (приложениями и встроенным программным кодом) и объектом (адресной книгой). Решение о доступе принимается на основе установленного значения атрибута доступа к адресной книге на субъекте. В случае разрешающего значения атрибута доступа к адресной книге доступ приложений и встроенного программного кода к адресной книге разрешается, в случае запрещающего значения – запрещается.

Объект оценки реализует политику управления доступом к вложениям электронной почты. ФБО обеспечивают опосредованный доступ между субъектами (пользователями ОО) и объектами (файлами вложений электронной почты). Решение о доступе принимается на основе сравнительного анализа атрибутов безопасности, связанных с запрашивающим субъектом, и атрибутов безопасности, связанных с объектом, к которому осуществляется доступ. Атрибуты безопасности субъекта включают список запрещенных типов файлов вложений электронной почты. Атрибуты объекта включают тип файла вложения электронной почты. Таким образом, если пользователь ОО осуществляет попытку доступа к определенному типу файла вложения электронной почты, который указан в списке запрещенных типов файлов вложений электронной почты, то ФБО блокируют такую попытку доступа и, соответственно, если данный тип файла не содержится в списке запрещенных, то доступ к файлу предоставляется.

Объект оценки реализует политику управления встроенным программным кодом. ФБО обеспечивают опосредованный доступ между субъектами (пользователями ОО) и объектами (встроенными программными кодами). Решение о доступе принимается на основе наличия либо отсутствия электронной подписи у встроенных программных кодов. В случае наличия подобной подписи у встроенного программного кода доступ пользователей ОО к данному программному коду разрешается, в случае отсутствия подписи – запрещается.

Объект оценки реализует политику фильтрации почтовых сообщений. ФБО обеспечивают фильтрацию передаваемых между пользователями ОО и внешними пользователями почтовых сообщений. Решение о возможности прохождения почтового сообщения либо его блокирования принимается на основе наличия или отсутствия разрешающих значений у атрибутов безопасности, ассоциированных с почтовыми сообщениями (адрес электронной почты и наименование домена). В случае наличия разрешающих значений почтовое сообщение не блокируется и соответственно обратное.

Объект оценки обеспечивает предупреждение пользователей относительно попыток выполнения ими действий или связанных с их действиями событий, являющихся потенциально небезопасными (попытки доступа приложений и встроенного программного кода к адресной книге, доступа пользователей ОО к запрещенным типам файлов вложений электронной почты, доступа к документам, содержащим встроенный программный код, не имеющий подписи и доступа к почтовым сообщениям, содержащим запрещенные типы файлов вложений).

Защита данных

Объект оценки обеспечивает конфиденциальность и целостность данных документов при перемещении документов между пользователями ОО и при обмене документами с внешними пользователями. Конфиденциальность и целостность обеспечивается применением механизмов шифрования и генерации электронной цифровой подписи, использующих соответствующие аттестованные алгоритмы. ОО также предоставляет возможность пользователям, уполномоченным на изменение документов, осуществлять удаление метаданных из документов.

Объект оценки обеспечивает согласованную интерпретацию данных, совместно используемых ОО и средой ИТ (управляющая информация и атрибуты безопасности, передающиеся ОО из среды ИТ, корректно воспринимаются и обрабатываются ОО).

Управление безопасностью

Объект оценки предоставляет возможность установления полномочий на доступ к защищаемым данным документов (установление пароля на доступ по чтению и пароля на доступ по записи, модификация дополнительных атрибутов безопасности и установление пароля на доступ к модификации дополнительных атрибутов безопасности) пользователям, создающим документ, а также уполномоченным на это пользователям

(пользователям, которым известен пароль для доступа к документу на изменение и пароль для доступа к модификации дополнительных атрибутов безопасности).

Объект оценки предоставляет возможность установления и модификации значений атрибутов безопасности, используемых в политиках управления доступом к адресной книге, вложениям электронной почты и встроенным в документы программным кодам, а также в политике фильтрации почтовых сообщений только администраторам ОО. Установление и модификация указанных атрибутов безопасности может проводиться администратором ОО непосредственно средствами самого ОО, либо с использованием соответствующего инструментария клиентских и серверных операционных систем.

В случаях сбоев (отказов) программного и аппаратного обеспечения, в том числе сбоях источников электропитания, ОО обеспечивает корректное восстановление функционирования и производит (по возможности) восстановление документов, коллективная или индивидуальная работа с которыми происходила в момент сбоя. Для поддержания функций корректного восстановления после сбоев, а также восстановления документов, в ОО предусмотрена возможность периодически, во время нормального функционирования, осуществлять тестирование среды ИТ и механизмов, реализующих функции безопасности ОО.

2.3 Границы ОО

Границы ОО определены следующими компонентами, входящими в состав ОО:

- Microsoft® Office Word 2003;
- Microsoft® Office Excel 2003;
- Microsoft® Office Outlook® 2003 с Диспетчером контактов;
- Microsoft® Office PowerPoint® 2003;
- Microsoft® Office Access 2003;
- Microsoft® Office Publisher 2003.

2.4 Службы безопасности ОО

В данном подразделе приводится краткое описание служб безопасности ОО, реализующих оцениваемые (в соответствии с настоящим ЗБ) функции безопасности ОО.

2.4.1 Защита данных пользователя

Включает функции, обеспечивающие управление доступом к файлам на основе пароля, политику управления правами на доступ к данным IRM, управление распространением метаданных в документах и управление доступом к объектам БД.

2.4.2 Идентификация и аутентификация

Включает функции, обеспечивающие идентификацию пользователей и групп пользователей при управлении доступом к документам, а также аутентификацию при осуществлении доступа к объектам БД.

2.4.3 Управление безопасностью

Включает функции, обеспечивающие управление различными характеристиками безопасности ОО.

2.4.4 Защита ФБО

Включает функции, обеспечивающие защиту функций безопасности ОО.

2.4.5 Управление доступом к ОО

Включает функции, обеспечивающие управление доступом приложений и программного кода к адресной книге Microsoft® Office Outlook 2003, доступом к документам, содержащим встроенный программный код, не имеющий подписи, а также к запрещенным типам файлов вложений электронной почты.

3 Среда безопасности ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

- предположений относительно аспектов безопасности среды ОО;
- угроз безопасности, которым нужно противостоять средствами ОО;
- политики безопасности организации, которой должен следовать ОО.

3.1 Предположения безопасности

Для обеспечения безопасности функционирования ОО необходимо обеспечить выполнение следующих условий.

3.1.1 Предположения относительно предопределенного использования ОО

A.OSAuth

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

A.Environment

Функционирование ОО должно осуществляться в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.

A.Security

Все составляющие ОО компоненты должны быть надлежащим образом настроены по безопасности администратором ОО. В составе ОО не должны функционировать такие компоненты, уровень безопасности которых (определяемый настройками администратора ОО) мог бы приводить к небезопасному использованию ОО в целом.

A.RecoverySafeState

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

3.1.2 Предположения относительно среды функционирования ОО

Предположение, связанное с физической защитой ОО

A.LocateTOE

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

Предположения, имеющие отношения к персоналу

A.NoEvilAdm

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

3.2 Угрозы

3.2.1 Угрозы, которым противостоит ОО

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

T.UnauthAccess

1. Аннотация угрозы – пользователи ОО и внешние пользователи могут предпринять действия, направленные на раскрытие и/или несанкционированное (может быть, даже злонамеренное) изменение данных документов (чувствительных данных и конфиденциальной информации).

2. Источники угрозы – пользователи ОО и внешние пользователи.

3. Способ реализации угрозы – доступ к документам с чувствительной (конфиденциальной информацией), раскрытие и/или изменение содержащейся в них чувствительных данных (конфиденциальной информации).

4. Используемые уязвимости – недостатки механизмов защиты документов от несанкционированного доступа и злонамеренного изменения (подделки).

5. Виды активов, потенциально подверженных угрозе – данные документов.

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

7. **Возможные последствия реализации угрозы** – раскрытие и/или несанкционированное (может быть, даже злонамеренное) изменение чувствительных данных.

T.ModifStyle

1. **Аннотация угрозы** – пользователи ОО и внешние пользователи, уполномоченные на изменение документа, но неуполномоченные на использование отличных от принятых в ОО стилей оформления документов, могут предпринять действия, направленные на изменение формы представления документа (использование стилей, отличных от принятых в АС).

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

3. **Способ реализации угрозы** – использование при изменении документа стилей, отличных от принятых в АС.

4. **Используемые уязвимости** – недостатки механизмов защиты документов от использования стилей, отличных от принятых в АС.

5. **Виды активов, потенциально подверженных угрозе** – данные документов.

6. **Нарушаемое свойство безопасности активов** – целостность.

7. **Возможные последствия реализации угрозы** – изменение формы представления документа.

T.AccAddrBook

1. **Аннотация угрозы** – приложения и встроенный программный код, содержащие программные вирусы и другой вредоносный программный код, могут предпринять попытку доступа к адресной книге с целью получения персональной информации о пользователях ОО и внешних пользователях, а также для злонамеренной модификации данных адресной книги и использования данных, содержащихся в адресной книге, для последующего распространения программных вирусов и другого вредоносного программного кода.

2. **Источники угрозы** – приложения и встроенный программный код.

3. **Способ реализации угрозы** – доступ к адресной книге; раскрытие и/или изменение содержащейся в ней информации; использование информации, содержащейся в адресной книге, для последующего распространения программных вирусов и другого вредоносного программного кода.

4. Используемые уязвимости – недостатки механизмов защиты адресной книги от несанкционированного доступа, злонамеренного изменения и использования.

5. Виды активов, потенциально подверженных угрозе – адресная книга.

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

7. Возможные последствия реализации угрозы – раскрытие и/или несанкционированное (может быть, даже злонамеренное) изменение данных адресной книги, использование данных адресной книги для распространения программных вирусов и другого вредоносного программного кода.

T.AccEnclosure

1. Аннотация угрозы – пользователи ОО могут осуществить доступ и последующее выполнение файлов вложений электронной почты, содержащих программные вирусы и другой вредоносный программный код, способные в процессе своего выполнения осуществить действия, критичные для безопасности АС.

2. Источники угрозы – пользователи ОО, инициирующие выполнение программных вирусов и вредоносного программного кода.

3. Способ реализации угрозы – доступ и выполнение файлов вложений электронной почты, содержащих программные вирусы и другой вредоносный программный код.

4. Используемые уязвимости – недостатки механизмов защиты от выполнения пользователями ОО файлов вложений электронной почты, содержащих программные вирусы и другой вредоносный программный код.

5. Виды активов, потенциально подверженных угрозе – программное обеспечение ОО, защищаемые документы и другая информация, вычислительные ресурсы.

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

7. Возможные последствия реализации угрозы – нарушение режимов функционирования программного обеспечения и ОО в целом; нарушение свойств безопасности защищаемых активов ОО.

T.AccFirmware

1. Аннотация угрозы – пользователи ОО могут осуществить доступ и последующее выполнение встроенного в документы программного кода, содержащего программные вирусы или направленного на деструктивные воздействия, способные в процессе своего выполнения осуществить действия, критичные для безопасности АС.

2. Источники угрозы – пользователи ОО, инициирующие выполнение встроенного в документы программного кода, содержащего программные вирусы или осуществляющего деструктивные воздействия.

3. Способ реализации угрозы – доступ и выполнение встроенного в документы программного кода, содержащего программные вирусы или направленного на деструктивные воздействия.

4. Используемые уязвимости – недостатки механизмов защиты от выполнения пользователями ОО встроенного в документы программного кода, содержащего программные вирусы или направленного на деструктивные воздействия.

5. Виды активов, потенциально подверженных угрозе – программное обеспечение ОО, защищаемые документы и другая информация, вычислительный процесс.

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

7. Возможные последствия реализации угрозы – нарушение режимов функционирования программного обеспечения и ОО в целом; нарушение свойств безопасности защищаемых активов ОО.

T.FiltrPostMessage

1. Аннотация угрозы – внешние нарушители могут осуществлять рассылку нежелательных (не имеющих отношение к функциональным обязанностям пользователей) почтовых сообщений, в том числе потенциально содержащих программные вирусы и другой вредоносный программный код.

2. Источники угрозы – внешние субъекты ИТ.

3. Способ реализации угрозы – рассылка нежелательных почтовых сообщений.

4. Используемые уязвимости – недостатки механизмов блокирования и удаления нежелательных почтовых сообщений.

5. Виды активов, потенциально подверженных угрозе – вычислительные ресурсы; память.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – отвлечение пользователей от выполнения функциональных обязанностей; ненадлежащее использование вычислительных ресурсов и памяти.

T.ViolationConf

1. Аннотация угрозы – пользователи ОО и внешние пользователи, неуполномоченные на доступ к данным документа, а также внешние субъекты ИТ могут осуществить попытку перехвата и последующего ознакомления с данными документов, передаваемых в рамках АС, а также – при взаимодействии с внешними пользователями.

2. Источники угрозы – пользователи ОО; внешние пользователи; внешние субъекты ИТ.

3. Способ реализации угрозы – перехват документов при их передаче и последующее ознакомление с данными документа.

4. Используемые уязвимости – недостатки механизмов защиты конфиденциальности передаваемых документов.

5. Виды активов, потенциально подверженных угрозе – данные документов.

6. Нарушаемое свойство безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с защищаемыми данными.

T.ViolationInt

1. Аннотация угрозы – пользователи ОО и внешние пользователи, а также внешние субъекты ИТ могут осуществить попытку перехвата и последующей злонамеренной модификации (подделки) данных, передаваемых в рамках АС и при взаимодействии с внешними пользователями, а также попытку передачи документа от имени уполномоченного пользователя.

2. Источники угрозы – пользователи ОО; внешние пользователи; внешние субъекты ИТ.

3. Способ реализации угрозы – перехват документов при их передаче и последующая злонамеренная модификация данных документов; передача документа от имени уполномоченного пользователя ОО.

4. Используемые уязвимости – недостатки механизмов защиты целостности передаваемых документов и подтверждения подлинности документов.

5. Виды активов, потенциально подверженных угрозе – данные документов.

6. Нарушаемое свойство безопасности активов – достоверность, целостность.

7. Возможные последствия реализации угрозы – несанкционированная подмена данных документов; отправление документа от имени уполномоченного пользователя ОО.

T.AccMetadata

1. Аннотация угрозы – внешние пользователи, а также внешние субъекты ИТ могут осуществить доступ к метаданным документа при получении или перехвате документа.

2. Источники угрозы – внешние пользователи; внешние субъекты ИТ.

3. Способ реализации угрозы – доступ к метаданным документа при получении или перехвате документа.

4. Используемые уязвимости – недостатки механизмов удаления метаданных из документа.

5. Виды активов, потенциально подверженных угрозе – метаданные документа.

6. Нарушаемое свойство безопасности активов – конфиденциальность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с персональной информацией, содержащейся в метаданных документов.

T.LostData

1. Аннотация угрозы – потеря данных, формируемых лично пользователем ОО, либо группой пользователей ОО и внешних пользователей с использованием среды совместной обработки данных, вследствие сбоя (отказа) программного обеспечения и аппаратных средств, в том числе сбоя источников энергоснабжения.

2. Источники угрозы – сбои (отказы) программного обеспечения и аппаратных средств.

3. Способ реализации угрозы – потеря данных вследствие сбоя (отказа) программного обеспечения и аппаратных средств.

4. Используемые уязвимости – недостатки механизмов предотвращения потери данных и восстановления данных при сбоях программного обеспечения и аппаратных средств.

5. Виды активов, потенциально подверженных угрозе – данные документов.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – потеря данных, сформированных лично пользователем ОО, либо сформированных группой пользователей ОО и внешних пользователей с использованием среды совместной обработки данных.

3.2.2 Угрозы, которым противостоит среда

В настоящем ЗБ определены следующие угрозы, которым необходимо противостоять средствами среды функционирования ОО.

TE.UnauthAccessTOE

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией.

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 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; защищаемая информация.

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

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией.

TE.MasqAdmin&User

- 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 средств, 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.
- 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.

TE.UnauthAccessTSF

- 1. Аннотация угрозы** – осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами.
- 2. Источники угрозы** – пользователи ОО; администраторы ОО.
- 3. Способ реализации угрозы** – осуществление доступа к данным ФБО с использованием средств, 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, служебная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

TE.UnauthAccessData

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.

3.3 Политика безопасности организации

Объект оценки должен следовать приведенным ниже правилам политики безопасности организации.

P.Reference

Должна быть предоставлена возможность установления полномочий на доступ к защищаемым данным документа только уполномоченным на это пользователям ОО и администраторам ОО. Полномочия на доступ к защищаемым данным документа должны устанавливаться в соответствии с политикой безопасности, принятой в АС.

P.Admin

Должно быть обеспечено наличие надлежащих корректно функционирующих средств администрирования ОО доступных только уполномоченным администраторам ОО.

P.ConformOperation

Должно быть обеспечено корректное и надлежащее функционирование ОО в среде функционирования (операционной системе). Должна быть обеспечена согласованная интерпретация данных, совместно используемых ОО и средой функционирования.

P.Caution

Должно осуществляться предупреждение пользователей относительно попыток выполнения ими действий, являющихся потенциально небезопасными, согласно политике безопасности АС, а также при выполнении ОО блокирования действий оцененных ОО как небезопасные.

P.AccessDoc

Должен быть обеспечен доступ к защищаемым документам только уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям. Должна быть обеспечена возможность уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям ограничивать права доступа к защищаемым документам для других пользователей ОО и администраторов ОО, а также внешних пользователей.

4 Цели безопасности

4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

O.AccessData

Разграничение доступа к данным

ОО должен обеспечивать доступ к защищаемым данным документов для ознакомления и модификации (в том числе и изменение формы представления документа, использование стилей, отличных от определенных в документе) только уполномоченным на это пользователям ОО, администраторам ОО, а также внешним пользователям.

O.AccessDoc

Разграничение доступа к документам

ОО должен обеспечивать доступ к защищаемым документам только уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям. ОО должен обеспечивать возможность уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям ограничивать права доступа к защищаемым документам для других пользователей ОО и администраторов ОО, а также внешних пользователей.

O.Establishment

Установление полномочий

ОО должен предоставлять возможность установления полномочий на доступ к защищаемым данным документа только уполномоченным на это пользователям ОО и администраторам ОО. Полномочия на доступ к защищаемым данным документа должны устанавливаться в соответствии с политикой безопасности, принятой в АС.

O.AddressBook

Защита адресной книги

ОО должен предотвращать попытки доступа приложений и встроенного в документы программного кода к адресной книге несанкционированные администратором ОО.

O.Enclosure

Ограничение доступа к файлам вложений

ОО должен предотвращать попытки доступа пользователей ОО к запрещенным файлам вложений электронной почты.

O.Firmware

Предотвращение выполнения встроенного программного кода

ОО должен предотвращать доступ и выполнение пользователями ОО неподписанного встроенного в документы программного кода.

O.Filtration

Фильтрация почтовых сообщений

ОО должен обеспечить фильтрацию почтовых сообщений, поступающих в ОО и/или выходящих из ОО.

O.Protect

Обеспечение безопасности при перемещении документов

ОО должен обеспечить конфиденциальность, целостность и подлинность данных документов при перемещении документов внутри АС, а также при передаче документов внешним пользователям. Должна быть обеспечена возможность однозначного определения подлинности пользователя, осуществившего передачу документа.

O.Metadata

Удаление метаданных

ОО должен обеспечить удаление метаданных в документах при запросе уполномоченных пользователей ОО и администраторов ОО.

O.Recovery

Обеспечение восстановления

ОО должен обеспечивать корректное восстановление функционирования ОО, а также возможность восстановления данных, которые формировались пользователем ОО лично, либо группой пользователей с использованием среды совместной разработки, в

случаях сбоев (отказов) ПО и аппаратных средств, в том числе сбоях источников электропитания.

O.Administration

Управление безопасностью

ОО должен располагать надлежащими корректно функционирующими средствами администрирования ОО доступными только уполномоченным администраторам ОО.

O.Operation

Обеспечение согласованного взаимодействия со средой

ОО должен обеспечить корректное и надлежащее функционирование ОО в среде функционирования (операционной системе) и согласованную интерпретацию данных, совместно используемых ОО и средой функционирования.

O.Caution

Предупреждение пользователей

ОО должен обеспечить предупреждение пользователей ОО относительно попыток выполнения ими действий, являющихся потенциально небезопасными, согласно политике безопасности АС, а также при выполнении ОО блокирования действий оцененных ОО как небезопасные.

4.2 Цели безопасности для среды

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

OE.OSAuth

Аутентификация с использованием механизмов ОС

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

OE.Environment

Стойкость функции безопасности

Функционирование ОО должно осуществляться в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от

прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.

OE.Security

Обеспечение надлежащей безопасной настройки

Должна быть обеспечена надлежащая безопасная настройка всех составляющих ОО компонентов. Должно быть обеспечено отсутствие в составе ОО таких компонентов, уровень безопасности которых (определяемый настройками администратора ОО) мог бы приводить к небезопасному использованию всего ОО в целом.

OE.ProtectFileSystem

Защита на уровне файловой системы

Должна быть обеспечена защита данных ОО на уровне файлов файловой системы ОС от несанкционированного доступа.

OE.LocateTOE

Физическая защита ОО

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

OE.NoEvilAdm

Требования к администраторам ОО

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

OE.RecoverySafeState

Восстановление ОО

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

OE.ProtectResTSF

Защита данных ФБО и ресурсов ОО

Должна быть обеспечена защита данных ФБО и ресурсов ОО, а также поддержка домена для функционирования ФБО.

5 Требования безопасности ИТ

В данном разделе ЗБ представлены функциональные требования и требования доверия, которым должен удовлетворять ОО. Функциональные требования, представленные в настоящем ЗБ, основаны на функциональных компонентах из части 2 ОК. Кроме того, в настоящий ЗБ включен ряд требований безопасности, сформулированных в явном виде (расширение части 2 ОК). Требования доверия основаны на компонентах требований доверия из части 3 ОК и представлены в настоящем ЗБ в виде оценочного уровня доверия ОУД1, усиленного компонентом доверия AVA_SOF.1 (Оценка стойкости функции безопасности ОО).

5.1 Требования безопасности для ОО

5.1.1 Функциональные требования безопасности ОО

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

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_IFC.1	Ограниченное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FDP_UCT.1	Базовая конфиденциальность обмена данными
FDP_UIT.1	Целостность передаваемых данных
FDP_MDD.1 (EXT)	Удаление метаданных в документах
FIA_ATD.1	Определение атрибутов пользователя
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.2	Идентификация до любых действий пользователя
FMT_MSA.1	Управление атрибутами безопасности

Идентификатор компонента требований	Название компонента требований
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_SMR.1	Роли безопасности
FPT_AMT.1	Тестирование абстрактной машины
FPT_RCV.3	Автоматическое восстановление без недопустимой потери
FPT_TDC.1	Базовая согласованность данных ФБО между ФБО
FPT_TST.1	Тестирование ФБО
FTA_TAB.2 (EXT)	Предупреждающие сообщения
FTP_ITC.1	Доверенный канал передачи между ФБО

5.1.1.1 Защита данных пользователя (FDP)

FDP_ACC.1 (1) Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику управления доступом к данным, основанную на пароле] для

[

- а) субъектов – пользователей ОО и внешних пользователей;
- б) объектов – отдельных частей документов;
- в) операций – чтения, изменения

].

Зависимости: FDP_ACF.1 (1) «Управление доступом, основанное на атрибутах безопасности».

FDP_ACF.1 (1) Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику управления доступом к данным, основанную на пароле] к объектам, основываясь на **следующих атрибутах безопасности:**

[

- а) субъектов – идентификаторе пользователя; введенном пароле при доступе к документу; идентификаторе стиля;

- б) объектов – списке доступа; списке разрешенных стилей; пароле для доступа к документу на чтение; пароле для доступа к документу на изменение

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[

- а) пользователю ОО или внешнему пользователю разрешено чтение данных документа, если введенный пользователем ОО или внешним пользователем пароль, запрашиваемый при обращении к документу, совпадает с соответствующим паролем, установленным на документе;
- б) пользователю ОО или внешнему пользователю разрешено изменение данных документа, если введенный пользователем ОО или внешним пользователем пароль, запрашиваемый при обращении к документу, совпадает с соответствующим паролем, установленным на документе, а также список доступа, сопоставленный с данными документа либо не установлен, либо идентификатор пользователя, обращающегося к данным документа, присутствует в списке доступа;
- в) пользователю ОО или внешнему пользователю разрешено изменение данных документа и добавление других (отличных от существующих в документе) стилей, если введенный пользователем ОО или внешним пользователем пароль, запрашиваемый при обращении к документу, совпадает с соответствующим паролем, установленным на документе, список доступа, сопоставленный с данными документа либо не установлен, либо идентификатор пользователя, обращающегося к данным документа, присутствует в списке доступа, и список разрешенных стилей либо не установлен, либо идентификатор стиля, добавляемого в документ, присутствует в списке разрешенных стилей

].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах:

[

- а) пользователю ОО или внешнему пользователю разрешено чтение данных документа, если пароль для доступа к документу на чтение не установлен;
- б) пользователю ОО или внешнему пользователю разрешено изменение данных документа, если пароль для доступа к документу на изменение и список доступа, сопоставленный с данными документа, не установлены

].

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

Зависимости: FDP_ACC.1 (1) «Ограниченное управление доступом»,
FMT_MSA.3 (1) «Инициализация статических атрибутов».

FDP_ACC.1 (2) Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику управления доступом к адресной книге] для

[

- а) субъектов – приложений и встроенного программного кода;
- б) объектов – файлов адресной книги;
- в) операций – чтения

].

Зависимости: FDP_ACF.1 (2) «Управление доступом, основанное на атрибутах безопасности».

FDP_ACF.1 (2) Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику управления доступом к адресной книге] к объекту, основываясь на следующих атрибутах безопасности:

[

- а) субъектов – атрибут доступа к адресной книге

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[

- а) приложению или встроенному программному коду разрешено чтение адресной книги, если для данного приложения или встроенного программного кода установлено разрешающее значение атрибута доступа к адресной книге

].

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

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

Зависимости: FDP_ACC.1 (2) «Ограниченное управление доступом»,
FMT_MSA.3 (2) «Инициализация статических атрибутов».

FDP_ACC.1 (3) Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику управления доступом к вложениям электронной почты] для

[

- а) субъектов – пользователей ОО;
- б) объектов – файлов вложений электронной почты;
- в) операций – выполнения

].

Зависимости: FDP_ACF.1 (3) «Управление доступом, основанное на атрибутах безопасности».

FDP_ACF.1 (3) Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику управления доступом к вложениям электронной почты] к объектам, основываясь на **следующих атрибутах безопасности:**

- [
- а) субъектов – списке запрещенных типов файлов вложений электронной почты;
 - б) объектов – типе файла вложения электронной почты
-].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

- [
- а) пользователю ОО разрешено выполнение файла вложения электронной почты, если тип файла вложения электронной почты не указан в списке запрещенных типов файлов вложений электронной почты
-].

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

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

Зависимости: FDP_ACC.1 (3) «Ограниченное управление доступом»,
FMT_MSA.3 (3) «Инициализация статических атрибутов».

FDP_ACC.1 (4) Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику управления встроенным программным кодом] для

- [
- а) субъектов – пользователей ОО;

б) объектов – встроенных программных кодов;

в) операций – выполнения

].

Зависимости: FDP_ACF.1 (4) «Управление доступом, основанное на атрибутах безопасности».

FDP_ACF.1 (4) Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику управления встроенным программным кодом] к объектам, основываясь на **следующих атрибутах безопасности:**

[

а) объектов – подписи

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[

а) пользователю ОО разрешено выполнение встроенного программного кода, если встроенный программный код имеет подпись

].

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

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

Зависимости: FDP_ACC.1 (4) «Ограниченное управление доступом»,
FMT_MSA.3 (4) «Инициализация статических атрибутов».

FDP_ACC.1 (5) Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику управления доступом к документам] для

[

- а) субъектов – пользователей ОО и внешних пользователей;
- б) объектов – документов;
- в) операций – просмотра, редактирования, сохранения, извлечения, экспорта, печати, запуска встроенного программного кода, распространения, ответа, ответа всем, просмотра прав

].

Зависимости: FDP_ACF.1 (5) «Управление доступом, основанное на атрибутах безопасности».

FDP_ACF.1 (5) Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику управления доступом к документам] к объектам, основываясь на

[

- а) ассоциированных с субъектом идентификаторе пользователя;
- б) следующих, ассоциированных с объектом, атрибутах управления доступом:
 - владелец объекта;
 - список управления доступом IRM

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[

доступ к объекту разрешен, если, по крайней мере, выполняется одно из следующих условий:

- а) запись, содержащаяся в списке IRM, явно разрешает доступ пользователю;
- б) список IRM отсутствует;
- в) субъект является владельцем объекта

].

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

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

Зависимости: FDP_ACC.1 (5) «Ограниченное управление доступом»,
FMT_MSA.3 (6) «Инициализация статических атрибутов».

FDP_ACC.1 (6) Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] для

[

- а) субъектов – процессов, действующих от имени пользователей;
- б) именованных объектов – база данных, таблица, запрос, форма, отчет, макрос;
- в) операций между субъектами и объектами – открытие и запуск, монопольный доступ, чтение макета, изменение макета, чтение данных, вставка данных, удаление данных, обновление данных, административная операция.

].

Зависимости: FDP_ACF.1 (6) «Управление доступом, основанное на атрибутах безопасности».

FDP_ACF.1 (6) Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] к объектам БД, основываясь на

[

следующем:

- а) ассоциированные с субъектом идентификатор учетной записи пользователя, принадлежность к группе (группам);

б) следующие, ассоциированные с объектами, атрибуты управления доступом:

[

- владелец объекта;
- список дискреционного управления доступом, который сопоставлен с объектом доступа и содержит записи:
 - идентификатор учетной записи пользователя или группы;
 - тип (разрешение или запрет);
 - право доступа к объекту;

]

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[

доступ к объекту разрешен, если, по крайней мере, выполняется одно из следующих условий:

- а) субъект является владельцем объекта;
- б) запись, содержащаяся в списке дискреционного управления доступом, явно разрешает доступ субъекту;
- в) запись, содержащаяся в списке дискреционного управления доступом, явно разрешает доступ группе, участником которой является субъект;

в случае если доступ к объекту не разрешен правилами, изложенными в FDP_ACF.1.3, то доступ субъекта к объекту запрещен

].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах:

[

- а) уполномоченному администратору ОО предоставлен доступ к объектам ОО вне зависимости от списков дискреционного управления доступом

].

FDP_ACF.1.4 ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах:

- [
- в доступе к объекту явно отказано, если выполняется, по крайней мере, одно из следующих условий:
- а) запись в списке дискреционного управления доступом явно запрещает доступ для субъекта, и доступ не был разрешен записью, содержащейся в списке дискреционного управления доступом;
 - б) запись в списке дискреционного управления доступом явно запрещает доступ группе, участником которой является субъект, и доступ не был разрешен записью, содержащейся в списке дискреционного управления доступом
-].

Зависимости: FDP_ACC.1 (6) «Ограниченное управление доступом»,
FMT_MSA.3 (7) «Инициализация статических атрибутов».

FDP_IFC.1 Ограниченное управление информационными потоками

FDP_IFC.1.1 ФБО должны осуществлять [политику фильтрации почтовых сообщений] для

- [
- а) субъектов – пользователей ОО и внешних пользователей;
 - б) информации – почтовых сообщений;
 - в) операций – перемещения информации;
-].

Зависимости: FDP_IFF.1 «Простые атрибуты безопасности».

FDP_IFF.1 Простые атрибуты безопасности

FDP_IFF.1.1 ФБО должны осуществлять [политику фильтрации почтовых сообщений], основанную на следующих типах атрибутов безопасности **почтовых сообщений**:

- [
- а) адресе электронной почты;
 - б) наименовании домена

-].
- FDP_IFF.1.2 ФБО должны разрешать информационный поток между управляемым субъектом и управляемой информацией посредством управляемой операции, если выполняются следующие правила:
- [
- а) пользователю, осуществляющему работу с ОО, разрешено принимать и передавать почтовые сообщения внешним пользователям, если все значения атрибутов безопасности почтовых сообщений, определяемые администратором ОО, являются разрешающими
-].
- FDP_IFF.1.3 ФБО должны реализовать [дополнительные правила политики фильтрации почтовых сообщений отсутствуют].
- FDP_IFF.1.4 ФБО должны предоставить следующее [дополнительные возможности политики фильтрации почтовых сообщений отсутствуют].
- FDP_IFF.1.5 ФБО должны явно разрешать информационный поток, основываясь на следующих правилах:
- [
- а) пользователю, осуществляющему работу с ОО, явно разрешено принимать и передавать почтовые сообщения внешним пользователям, если значение адреса электронной почты внешнего пользователя является разрешающим
-].
- FDP_IFF.1.6 ФБО должны явно запрещать информационный поток, основываясь на следующих правилах:
- [
- а) пользователю, осуществляющему работу с ОО, явно запрещено принимать и передавать почтовые сообщения от внешних пользователей, если значение адреса электронной почты внешнего пользователя является запрещающим
-].
- Зависимости: FDP_IFC.1 «Ограниченное управление информационными потоками»,
FMT_MSA.3 (5) «Инициализация статических атрибутов».

FDP_UCT.1 Базовая конфиденциальность обмена данными

FDP_UCT.1.1 ФБО должны осуществлять [политику управления доступом к данным, основанную на пароле], предоставляющую возможность отправления и получения данных пользователя способом, защищенным от несанкционированного раскрытия.

Зависимости: FTP_ИТС.1 «Доверенный канал передачи между ФБО»,
FDP_ACC.1 (1) «Ограниченное управление доступом»

FDP_UIT.1 Целостность передаваемых данных

FDP_UIT.1.1 ФБО должны осуществлять [политику управления доступом к данным, основанную на пароле], предоставляющую возможность отправления и получения данных пользователя способом, защищенным от ошибок модификации, удаления, вставки.

FDP_UIT.1.2 ФБО должны быть способны определить после получения данных пользователя, произошли ли следующие ошибки: модификация, удаление, вставка, повторение.

Зависимости: FDP_ACC.1 (1) «Ограниченное управление доступом»,
FTP_ИТС.1 «Доверенный канал передачи между ФБО».

FDP_MDD.1 (EXT) Удаление метаданных в документах

FDP_MDD.1.1 ФБО должны обеспечить возможность удаления метаданных в документах по запросу пользователей, уполномоченных на изменение документа.

Зависимости: отсутствуют.

5.1.1.2 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) принадлежность к группе;
-].

Зависимости: отсутствуют.

FIA_UAU.2 (1) Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны требовать, чтобы каждый **субъект доступа к объектам БД** 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 к объектам БД** [возможность ввода аутентификационной информации в скрытом виде] во время выполнения аутентификации.

Зависимости: FIA_UAU.2 (1) «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.

5.1.1.3 Управление безопасностью (FMT)

FMT_MSA.1 (1) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом к данным, основанную на пароле], **предоставляющую** возможность модифицировать атрибуты безопасности

[

- а) пароль для доступа к документу на чтение;
- б) пароль для доступа к документу на изменение

]

только [пользователю, уполномоченному на изменение документа].

Зависимости: FDP_ACC.1 (1) «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (2) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом к данным, основанную на пароле], **предоставляющую** возможность модифицировать атрибуты безопасности

[

- а) список доступа;
- б) список разрешенных стилей

]

только [пользователю, уполномоченному на изменение дополнительных атрибутов безопасности данных документа].

Зависимости: FDP_ACC.1 (1) «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (1) Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику управления доступом к данным, основанную на пароле], **предусматривающую** разрешающие значения по умолчанию для атрибутов безопасности, которые используются для осуществления **политики управления доступом к данным, основанной на пароле**.

FMT_MSA.3.2 ФБО должны позволять [пользователю, владельцу документа] определять альтернативные начальные значения для отмены значений по умолчанию при создании **документа**.

Зависимости: FMT_MSA.1 (1) «Управление атрибутами безопасности»,
FMT_MSA.1 (2) «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (3) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом к адресной книге], **предоставляющую** возможность модифицировать атрибуты безопасности

[

- а) атрибут доступа к адресной книге

]

только [администратору ОО].

Зависимости: FDP_ACC.1 (2) «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (2) Инициализация статических атрибутов

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

FMT_MSA.3.2 ФБО должны позволять [администратору ОО] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

Зависимости: FMT_MSA.1 (3) «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (4) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом к вложениям электронной почты], **предоставляющую** возможность модифицировать атрибуты безопасности

[

а) список запрещенных типов файлов вложений электронной почты

]

только [администратору ОО].

Зависимости: FDP_ACC.1 (3) «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (3) Инициализация статических атрибутов

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

FMT_MSA.3.2 ФБО должны позволять [администратору ОО] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

Зависимости: FMT_MSA.1 (4) «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (5) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления встроенным программным кодом], **предоставляющую** возможность [установления] и модификации атрибутов безопасности

[

а) подписи встроенных программных кодов

]

только [администратору ОО].

Зависимости: FDP_ACC.1 (4) «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (4) Инициализация статических атрибутов

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

FMT_MSA.3.2 ФБО должны позволять [администратору ОО] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

Зависимости: FMT_MSA.1 (5) «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (6) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику фильтрации почтовых сообщений], **предоставляющую** возможность модификации атрибутов безопасности

[

а) адреса электронной почты;

б) наименования домена
]

только [администратору ОО].

Зависимости: FDP_ACC.1 (4) «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (5) Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику фильтрации почтовых сообщений],
предусматривающую разрешающие значения по умолчанию для атрибутов
безопасности, которые используются для осуществления **политики
фильтрации почтовых сообщений**.

FMT_MSA.3.2 ФБО должны позволять [администратору ОО] определять альтернативные
начальные значения для отмены значений по умолчанию при создании
объекта или информации.

Зависимости: FMT_MSA.1 (6) «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (7) Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику управления доступом к документам],
предоставляющую возможность модификации атрибутов безопасности
[
а) идентификатор пользователя;
б) список управления доступом IRM
]

только [пользователю, владельцу документа].

Зависимости: FDP_ACC.1 (4) «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (6) Инициализация статических атрибутов

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

FMT_MSA.3.2 ФБО должны позволять [пользователю, владельцем документа] определять альтернативные начальные значения для отмены значений по умолчанию при создании документа.

Зависимости: FMT_MSA.1 (7) «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 (8) 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 (6)], только [уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта].

Зависимости: FDP_ACC.1 (6) «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 (7) Инициализация статических атрибутов

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

FMT_MSA.3.2 ФБО должны позволять [уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта] определять альтернативные начальные значения для отмены значений по умолчанию при создании **объекта**.

Зависимости: FMT_MSA.1 (8) «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 5.2] над данными, [указанными в третьем столбце таблицы 5.2], только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.2 – Управляемые данные ФБО

Компонент	Операция	Данные ФБО
FIA_ATD.1	установка, модификация	атрибуты безопасности пользователя
FIA_UAU.2 (1)	установка, модификация	аутентификационные данные (пароль) для доступа к объектам БД
FIA_UID.2	установка, модификация	идентификатор пользователя

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

- [
- а) администратор ОО;
 - б) пользователь ОО;
 - в) внешний пользователь
-].

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

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

5.1.1.4 Защита ФБО (FPT)

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ периодически во время нормального функционирования для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая положена в основу ФБО.

Зависимости: отсутствуют.

FPT_RCV.3 Автоматическое восстановление без недопустимой потери

FPT_RCV.3.1 Когда автоматическое восстановление после сбоя или прерывания обслуживания невозможно, ФБО должны перейти в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию.

FPT_RCV.3.2 В случае [сбоев (отказов) программного и аппаратного обеспечения ОО] ФБО должны обеспечить возврат ОО к безопасному состоянию с использованием автоматических процедур.

FPT_RCV.3.3 Функции из числа ФБО, предназначенные для преодоления последствий сбоя или прерывания обслуживания, должны обеспечить восстановление безопасного начального состояния без превышения [количественная мера не определена] потери документов в пределах ОДФ.

FPT_RCV.3.4 ФБО должны обеспечить способность определения, какие документы могут, а какие не могут быть восстановлены.

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

FPT_TDC.1 Базовая согласованность данных ФБО между ФБО

FPT_TDC.1.1 ФБО должны обеспечить способность согласованно интерпретировать [

- а) атрибуты безопасности пользователей ОО и внешних пользователей;
- б) атрибуты безопасности данных документов;
- в) атрибуты безопасности адресной книги;
- г) атрибуты безопасности приложений и встроенного программного кода;
- д) атрибуты безопасности почтовых сообщений;
- е) атрибуты безопасности файлов вложений электронной почты

],
совместно используемые ФБО и ОС.

FPT_TDC.1.2 ФБО должны использовать [правила интерпретации, применяемых ФБО, не определены] при интерпретации данных ФБО, полученных от другого доверенного продукта ИТ.

Зависимости: отсутствуют.

FPT_TST.1 Тестирование ФБО

FPT_TST.1.1 ФБО должны выполнять пакет программ самотестирования 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».

5.1.1.5 Доступ к ОО (FTA)

FTA_TAB.2 (EXT) Предупреждающие сообщения

FTA_TAB.2.1 ФБО должны отобразить предупреждающее сообщение относительно следующего:

- [
- а) доступа приложений и программного кода к адресной книге;
 - б) попыток доступа пользователей ОО к запрещенным типам файлов вложений электронной почты;
 - в) попыток доступа к документам, содержащим встроенный программный код, не имеющий подписи;
 - г) попыток доступа к почтовым сообщениям, содержащим запрещенные типы файлов вложений
-].

Зависимости: отсутствуют.

5.1.1.6 Доверенный маршрут/канал (FTR)

FTR_ITS.1 Доверенный канал передачи между ФБО

FTR_ITS.1.1 ФБО должны предоставлять канал связи между собой и удаленным доверенным продуктом ИТ, который логически отличим от других каналов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту данных канала от модификации или раскрытия.

FTR_ITS.1.2 ФБО должны позволить ФБО инициировать связь через доверенный канал.

FTR_ITS.1.3 ФБО должны инициировать связь через доверенный канал для выполнения

[

- а) перемещения документов

].

Зависимости: отсутствуют.

5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 ОК и образуют ОУД1, усиленный компонентом AVA_SOF.1 (см. таблицу 5.2).

Таблица 5.2 – Требования доверия к безопасности ОО

Класс доверия	Идентификатор компонента доверия	Название компонента доверия
Управление конфигурацией	ACM_CAP.1	Номера версий
Поставка и эксплуатация	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1	Неформальная функциональная спецификация
	ADV_RCR.1	Неформальная демонстрация соответствия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Тестирование	ATE_IND.1	Независимое тестирование на соответствие
Оценка уязвимостей	AVA_SOF.1	Оценка стойкости функции безопасности ОО

5.1.2.1 Управление конфигурацией (АСМ)

АСМ_CAP.1 Номера версий

АСМ_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

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

АСМ_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

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

5.1.2.2 Поставка и эксплуатация (ADO)

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

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

5.1.2.3 Разработка (ADV)

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

ADV_FSP.1.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

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

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

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

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

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

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

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

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

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

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

5.1.2.4 Руководства (AGD)

AGD_ADM.1 Руководство администратора

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.

5.1.2.5 Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

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

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

5.1.2.6 Оценка уязвимостей (AVA)

AVA_SOF.1 Оценка стойкости функции безопасности ОО

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 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 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.

5.2 Требования безопасности для среды ИТ

Функцией безопасности, реализуемой средой ИТ (операционной системой) в интересах обеспечения безопасности ОО, является функция безопасности «Аутентификация». Данная функция реализуется механизмом паролей среды ИТ (операционной системы). Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости. В качестве минимального уровня стойкости функции безопасности «Аутентификация» в настоящем ЗБ заявлена «Средняя СФБ».

Другие механизмы (некриптографические), реализуемые средой ИТ в интересах обеспечения безопасности ОО, нельзя отнести к вероятностным и перестановочным механизмам, поэтому заявлений об их стойкости в настоящем ЗБ не делается.

Функциональные компоненты из части 2 ОК, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.3.

Таблица 5.3 – 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	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО

5.2.1 Идентификация и аутентификация (FIA)

FIA_AFL.1 Обработка отказов аутентификации

FIA_AFL.1.1 **Функции безопасности среды ИТ** должны обнаруживать, когда произойдет [установленное администратором ОС число (не более 10)] 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:

- [
- а) сделать невозможным доступ субъекта доступа к ОО, осуществив блокировку регистрационной записи на 30 минут;
 - б) по истечении 30 минут осуществить сброс счетчика неуспешных попыток аутентификации
-].

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

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 **Функции безопасности среды ИТ** должны предоставить механизм для верификации того, что **пароли на доступ к ОО** отвечают **следующей метрики качества**

- [
- а) минимальная длина – 6 символов;

- б) пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- в) в пароле должны присутствовать символы как минимум трех категорий из числа следующих:
 - прописные буквы английского алфавита от А до Z;
 - строчные буквы английского алфавита от а до z;
 - десятичные цифры от 0 до 9;
 - символы, не принадлежащие алфавитно-цифровому набору;

].

Зависимости: отсутствуют.

FIA_UAU.2 (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».

5.2.2 Защита ФБО (FPT)

FPT_RVM.1 Невозможность обхода ПБО

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

Зависимости: отсутствуют.

FPT_SEP.1 Отделение домена ФБО

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

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

Зависимости: отсутствуют.

6 Краткая спецификация ОО

В данном подразделе представлено описание функций безопасности ОО и мер доверия к безопасности ОО, а также их сопоставление с требованиями безопасности для ОО.

6.1 Функции безопасности ОО

Объект оценки реализует следующие функции безопасности:

- защита данных пользователя;
- идентификация и аутентификация;
- управление безопасностью;
- защита ФБО;
- управление доступом к ОО.

6.1.1 Функции безопасности ОО «Защита данных пользователя»

К предоставляемым ОО механизмам обеспечения защиты данных пользователя относятся:

- управление правами на доступ к данным;
- защита документов с помощью пароля;
- ограничения по изменению и форматированию;
- ограничение распространения метаданных;
- безопасность пакетов расширения XML.

6.1.1.1 Управление правами на доступ к данным

Объект оценки обеспечивает управление правами на доступ к защищаемым данным посредством технологии IRM, предоставляющей возможность ограничить доступ субъектов на уровне отдельных документов, предотвращая тем самым их несанкционированное использование. IRM представляет собой технологию защиты данных, которая допускает совместный доступ к документам и позволяет отправлять их в сообщениях электронной почты, одновременно ограничивая круг лиц, имеющих право на просмотр и изменение документа.

Технология IRM позволяет уполномоченному администратору или владельцу документа, задавать круг субъектов доступа, имеющих право на просмотр и изменение

документов или сообщений электронной почты, блокировать копирование или печать файлов, устанавливать ограничение по сроку действия документов.

Механизм IRM, реализованный в ОО, является расширением основной технологии управления правами RMS – службы управления правами и применяется для защиты конфиденциальных данных независимо от того, кем и каким образом они используются. Поскольку защита с использованием технологии IRM обеспечивается на уровне отдельных файлов, то ограничения на их использование действуют постоянно, в любой среде использования. Это означает, что права применяются к защищенным данным даже при открытии электронного письма или документа на автономном компьютере или после их сохранения на жесткий диск.

Использование технологии IRM в Microsoft® Office Outlook® 2003

Службу IRM можно использовать в программе Office Outlook 2003 для предотвращения пересылки, копирования или распечатки сообщений. Разрешения документа Office 2003, вложенного в сообщение с ограниченными разрешениями, также ограничиваются, если они не были ограничены ранее, в таком случае для вложенного документа сохраняются старые разрешения.

Использование технологии IRM в Microsoft® Office Word 2003, Excel 2003 и PowerPoint® 2003

Разрешения для документов Office 2003 можно ограничить для пользователей и для групп (для задания разрешений для групп нужно расширение Active Directory для групп). Для каждого пользователя или группы задается набор разрешений, зависящий от определенных авторами документа уровней доступа: чтение, изменение или полный доступ. Авторы документа имеют полный доступ. Пользователи, обладающие правом на полный доступ, как и авторы документа, могут ограничить печать документа, задать даты истечения сроков действия разрешений и даже выдавать разрешения другим лицам или менять разрешения существующих пользователей. После истечения срока действия разрешения для зарегистрированных пользователей документ может быть открыт только его авторами или пользователями с правом на полный доступ.

Если документ с ограниченными разрешениями пересылается несанкционированному пользователю, сообщение отображается с указанием адреса электронной почты автора документа, чтобы пользователь мог запросить у автора разрешения на этот документ. Если автор документа решает не включать свой адрес

электронной почты в сообщение, для несанкционированных пользователей будет отображаться сообщение об ошибке.

Технология IRM использует различные уровни разрешений для задания ограничений доступа субъектов к содержимому IRM-защищенных документов:

1. **полный доступ (Full Control)** – предоставляет субъекту всю полноту действий по управлению доступом к файлу или его содержимому других субъектов доступа. Ограничения по сроку действия документа не затрагивают субъектов доступа, обладающих правом «Полный доступ»;
2. **просмотр (View)** – предоставляет субъекту доступа возможность просмотра содержимого IRM-защищенных документов. Данный уровень разрешений аналогичен разрешению только на чтение (Read Access), определяемому через графический интерфейс ОО;
3. **редактирование (Edit)** – предоставляет субъекту доступа возможность вносить изменения в содержимое IRM-защищенных документов;
4. **сохранять (Save)** – позволяет субъекту выполнять только операции сохранения документов;
5. **извлечь (Extract)** – позволяет субъекту доступа выполнять копирование любой части документа и использовать его в другом приложении;
6. **экспорт (Export)** – позволяет субъекту доступа сохранять содержимое документа в альтернативном месте или в формате, который поддерживает или не поддерживает технологию IRM;
7. **печать (Print)** – позволяет субъекту доступа распечатывать содержимое документа;
8. **запуск макросов (Allow Macros)** – позволяет субъекту доступа осуществлять исполнение макросов в отношении содержимого документа;
9. **распространение (Forward)** – предоставляет возможность получателям почтовых сообщений пересылать IRM-защищенные сообщения электронной почты;
10. **ответить (Reply)** – предоставляет возможность получателям почтовых сообщений отвечать на полученные IRM-защищенные сообщения электронной почты;

11. **ответить всем (Reply All)** – предоставляет возможность получателям почтовых сообщений отвечать всем пользователям, указанным в поле «Кому...» и «Копия» IRM-защищенного сообщения электронной почты;
12. **просмотр прав (View Rights)** – позволяет субъекту доступа просматривать права на доступ к указанному документу. ОО не поддерживает указанное право.

Кроме того, при создании IRM-защищенного документа его владелец (создатель) может использовать один из следующих предопределенных наборов разрешений доступа:

1. **чтение (Read)** – пользователь, обладающий данным набором разрешений доступа, имеет только право просмотра содержимого IRM-защищенного документа;
2. **не распространять (Do Not Forward)** – данный набор разрешений доступа включает права «Просмотр», «Ответить» и «Ответить всем»;
3. **изменить (Change)** – данный набор разрешений доступа включает права «Просмотр», «Редактирование», «Извлечь», «Экспорт» и «Сохранять».

6.1.1.2 Защита файлов с использованием пароля

Объект оценки обеспечивает три вида защиты документов Microsoft® Office Word 2003 и книг Microsoft® Office Excel 2003 с использованием пароля, препятствующие открытию или изменению документа злоумышленниками:

- защита, ограничивающая возможность открытия файла. Данный вид защиты документов обеспечивает возможность открытия файла субъектом доступа только после правильного указания им пароля;
- защита, ограничивающая возможности изменения файла. Данный вариант защиты не требует ввода какой-либо аутентификационной информации для открытий файла документа, однако изменить файл и сохранить изменения без ввода субъектом доступа пароля невозможно;
- защита с рекомендацией открыть файл исключительно для чтения. Данный вид защиты документов обеспечивает возможность открытия файла документа исключительно в режиме чтения. Однако субъект доступа имеет возможность открыть файл в режиме чтения/записи без ввода пароля.

Объект оценки также реализует поддержку возможности обеспечения защиты доступа к базам данных Microsoft® Office Access 2003 с использованием пароля. В случае, если пароль установлен, то при попытке доступа к базе данных ОО выводит диалоговое окно, в котором осуществляющему доступ субъекту предлагается ввести пароль. В случае ввода неправильного пароля в доступе субъекта к БД будет отказано.

Защита с использованием пароля действует исключительно при открытии базы данных. После открытия БД все ее объекты доступны пользователю в полном объеме, если только они не защищены другими средствами Microsoft® Office Access 2003.

Хранение пароля на открытие БД осуществляется ОО в самой БД в преобразованном виде, что делает его недоступным для прямого чтения из файла данных БД.

6.1.1.3 Ограничения по изменению и форматированию

Объект оценки обеспечивает различные возможности управления ограничениями на форматирование и редактирование документов Microsoft® Office Word 2003, книг Microsoft® Office Excel 2003.

Microsoft® Office Word 2003

Ограничения на форматирование документов Microsoft® Office Word 2003 предоставляет владельцу документа возможность заблокировать документ для других пользователей с той целью, чтобы другие субъекты могли изменять его содержимое, но не могли изменять ни одного из имеющихся в документе стилей форматирования.

Ограничения на редактирование документов Microsoft® Office Word 2003 предоставляют владельцу документа определять указанный способ редактирования документа. Владелец документа имеет возможность разрешить другим пользователям вносить изменения в документ в режиме записи исправлений или же сделать весь документ доступным только для чтения. Кроме того, ОО обеспечивает возможность запрета владельцем документа внесения изменений в определенные разделы документа кем-либо, кто не имеет на это соответствующих прав.

В качестве возможных вариантов защиты документа его владельцем могут быть определены следующие способы редактирования:

- **запись исправлений** – при выборе данного варианта защиты любому пользователю разрешается вносить в документ изменения, при этом все

исправления отображаются и видны на экране, а автор исправлений имеет право их принимать или отклонять. Пользователи, не являющиеся владельцем документа, не могут отключить запись исправлений, принять или отклонить их;

- **примечания** – в данном режиме пользователю разрешается вставлять примечания, однако запрещает изменять содержимое документа;
- **ввод данных в поля форм** – в данном варианте пользователям разрешается изменять исключительно поля форм и незащищенные разделы. Все другие изменения в документе запрещены;
- **только чтение** – данный вариант защиты документа делает его доступным остальным пользователям только для чтения.

В тоже время, ОО обеспечивает возможность задания владельцем документа исключений для отдельных категорий пользователей или групп безопасности, что позволяет им редактировать определенные части документа.

Microsoft® Office Excel 2003

Объект оценки в Microsoft® Office Excel 2003 поддерживается ряд функциональных возможностей обеспечения защиты дополнительных элементов листа или книги, а именно:

- **защиту целого листа или отдельных ячеек** – данная возможность обеспечивает способность выполнения всеми пользователями данного листа заданного множества операций, таких как форматирование ячеек, строк и столбцов, вставка и удаление строк и столбцов, изменение и вставка гиперссылок и т.д.;
- **задание диапазонов ячеек защищенного листа** – изменение которых требует знания пароля. Данная возможность позволяет обеспечить защиту заданного диапазона ячеек от неуполномоченной модификации и определить группы пользователей, пользователей или компьютеры, которые обладают возможностью изменять отдельные ячейки и диапазоны ячеек защищенного листа без знания пароля;
- **защиту отдельной книги** – данная возможность позволяет указывать элементы (структуру или окна), которые должны быть защищены, а также задавать пароль с целью запрета снятия защиты книги злоумышленниками;

- **установка защиты книги на общий доступ с исправлениями** – данная возможность позволяет управлять общим доступом на совместное использование книги несколькими пользователями с запретом на отмену режима исправлений. Для отключения режима записи исправлений требуется ввести пароль.

6.1.1.4 Защита данных в приложениях Microsoft® Office Access 2003

Система управления базами данных Microsoft® Office Access 2003 включает в себя ряд способов управления уровнем доступа пользователей к базам данных и их объектам. К указанным способам относятся следующие:

- **отображение и скрывание объектов в окне базы данных** – данный способ защиты предоставляет возможность защитить объекты базы данных от других пользователей путем их скрывания в окне базы данных;
- **запрет на репликацию БД, установку паролей и параметров автозагрузки** – данный способ защиты предоставляет возможность запрещения уполномоченным администратором копирования БД в среде с несколькими пользователями. В случае если копирование разрешено, то пользователи имеют возможность копировать совместно используемые БД, добавлять в них поля и выполнять другие изменения, к примеру, устанавливать пароль, снимать защиту с паролем, изменять свойства автозагрузки. В случае если безопасность совместно используемой БД на уровне пользователей не определена, то запретить пользователям указанные выше изменения невозможно. В случае, если же безопасность на уровне пользователей определена, пользователь или группа могут осуществлять репликацию БД, устанавливать пароли или изменять свойства автозагрузки исключительно в том случае, если они обладают правами администратора БД. В случае если пользователь или группа не имеют прав администратора, выполнять вышеупомянутые изменения они не смогут;
- **управление разрешениями на уровне отдельных пользователей или групп БД** – данный способ позволяет уполномоченному администратору или владельцу БД различные уровни доступа к данным и объектам БД для различных категорий пользователей или групп, определяемых в самой БД. В случае если ограничение доступа пользователей к БД осуществляется с

использованием данного способа, то для осуществления доступа к ней пользователю необходимо указать собственный пароль, на основании которого ОО выполнит процедуру аутентификации и в последующем, при доступе к объектам БД, авторизацию. С помощью паролей и разрешений доступа (набор атрибутов, определяющих права пользователя на данные или объекты в базе данных.) ОО предоставляется или ограничивается доступ пользователей или групп к объектам базы данных. Пользователи и группы, которым определен доступ к объектам в рамках БД, представлены в системе учетными записями. Данная информация хранится в информационном файле сведений рабочей группы (файл, который считывается при запуске, и содержит сведения об учетных записях пользователей и групп и их правах доступа. Эти сведения включают имена учетных записей пользователей, их пароли и имена групп, в которые входят пользователи). В рамках каждой БД учетная запись пользователя или группы защиты однозначно определяется уникальным значением, созданным на основе его имени и личного кода (буквенно-цифровой строки, содержащей от 4 до 20 символов).

Объектом оценки в Microsoft® Office Access 2003 определены две стандартные группы пользователей: администраторы (группа «Admins») и пользователи БД (группа «Users»). Участники группы «Admins» полные разрешения на все базы данных, используемые рабочей группой. Данная группа является уникальной в каждом файле рабочей группы. По умолчанию пользователь «Admin» является членом группы «Admins». В каждый момент в группу «Admins» должен входить по крайней мере один пользователь.

Группа «Users» включает учетные записи всех пользователей. Данная группа является одинаковой в каждом файле рабочей группы, однако этот файл содержит только учетные записи пользователей, созданные членами группы «Admins», входящими в данную рабочую группу. По умолчанию данная группа имеет все разрешения на все создаваемые новые объекты.

Кроме того, ОО в Microsoft® Office Access 2003 поддерживается набор предустановленных групп защиты, участники которых обладают предопределенными полномочиями на выполнение операций на уровне БД или ее отдельных объектов.

Объектом оценки обеспечивается также возможность создания новых групп и добавление новых пользователей в соответствующие группы.

Группам и пользователям предоставляются разрешения, определяющие возможность их доступа к каждому объекту базы данных. Для каждой БД и ее объектов ОО поддерживаются различные уровни разрешений доступа:

- на уровне БД для пользователей и групп защиты могут быть определены следующие разрешения:
 - открытие и запуск;
 - монопольный доступ;
 - административное разрешение;
- на уровне таблиц и запросов БД для пользователей и групп защиты могут быть определены следующие разрешения доступа:
 - чтение макета;
 - изменение макета;
 - административное разрешение;
 - чтение данных;
 - обновление данных;
 - вставка данных;
 - удаление данных;
- на уровне форм, отчетов и макросов БД для пользователей и групп защиты могут быть определены следующие разрешения доступа:
 - открытие и запуск;
 - чтение макета;
 - изменение макета;
 - административное разрешение.

Разрешения на доступ можно разделить на два типа: явные и неявные. Разрешения называются явными, если они непосредственно присвоены учетной записи пользователя; такие разрешения не влияют на разрешения других пользователей. Неявными называются разрешения на доступ, присвоенные учетной записи группы. Пользователь, включенный в такую группу, получает все разрешения, предоставленные ей. В свою очередь, удаление пользователя из данной группы лишает его всех разрешений, присвоенных группе.

При попытке пользователя выполнить какую-либо операцию с защищенным объектом базы данных его текущие разрешения определяются комбинацией явных и неявных разрешений на доступ. На уровне пользователей всегда действуют минимальные

ограничения из налагаемых явными разрешениями для пользователя и для всех групп, к которым принадлежит данный пользователь.

В ряде случаев пользователи, не имеющие разрешения на выполнение какого-либо действия, имеют возможность присвоить их себе. Такая ситуация имеет место для пользователя, являющегося членом группы «Admins» или владельцем объекта.

Изменять разрешения других пользователей на доступ к отдельным объектам БД данных могут следующие категории пользователей:

- члены группы «Admins», определенной в файле рабочей группы, который использовался при создании конкретной базы данных;
- владелец объекта;
- любой пользователь, получивший на этот объект соответствующие разрешения от уполномоченного администратора.

6.1.1.5 Ограничение распространения метаданных

Объект оценки обеспечивает возможность ограничения распространения метаданных в документах (данные об авторе и редакторах документа), что исключает возможность их прочтения злоумышленниками.

Данная возможность обеспечения безопасности поддерживается ОО в приложениях Microsoft® Office Word 2003, PowerPoint® 2003 и Excel 2003.

Объект оценки обеспечивает также возможность вывода на экран предупреждения о наличии в документе Word метаданных (включая исправление и примечания) перед сохранением, печатью или отправкой файла электронной почтой. Это предупреждение носит рекомендательный характер и требует от пользователя самостоятельного удаления метаданных.

6.1.1.6 Безопасность пакетов расширения XML

Данная функциональная возможность обеспечения безопасности, реализуемая ОО предотвращает загрузку пакетов расширения XML (набора файлов, которые расширяют возможности отображения и доступные действия в документах Microsoft® Word или Microsoft® Excel), которые используются в решениях смарт-документов, позволяющих упростить обмен сведениями, взаимодействуя с различными базами данных и другими приложениями ОО (Microsoft® Office 2003).

Сопоставление с ФТБ

Функции безопасности «Защита данных пользователя» удовлетворяют следующим функциональным требованиям безопасности:

- FDP_ACC.1 (1) – ФБО реализуют политику управления доступом к данным, основанную на пароле и разграничивают доступ к данным со стороны пользователей ОО и внешних пользователей;
- FDP_ACF.1 (1) – ФБО обеспечивают доступ к данным документов, основываясь на определенных атрибутах безопасности субъектов и объектов доступа, управление доступом осуществляется на основе правил;
- FDP_ACC.1 (5) – ФБО реализуют политику управления доступом к документам, основанную на IRM технологии и разграничивают доступ к документам со стороны пользователей ОО и внешних пользователей;
- FDP_ACF.1 (5) – ФБО обеспечивают доступ к документам, основываясь на определенных атрибутах безопасности субъектов и объектов доступа, управление доступом осуществляется на основе правил;
- FDP_ACC.1 (6) – ФБО реализуют политику дискреционного управления доступом, разграничивая доступ к объектам БД со стороны пользователей ОО;
- FDP_ACF.1 (6) – ФБО обеспечивают доступ к объектам БД, основываясь на определенных атрибутах безопасности субъектов и объектов доступа, управление доступом осуществляется на основе правил;
- FDP_UCT.1 – ФБО предоставляют возможность отправления и получения данных пользователя способом, защищенным от несанкционированного раскрытия;
- FDP_UTI.1 – ФБО предоставляют возможность отправления и получения данных пользователя способом, защищенным от ошибок модификации, удаления, вставки;
- FDP_MDD.1 (EXT) – ФБО обеспечивают возможность удаления метаданных в документах по запросу пользователей, уполномоченных на изменение документа;
- FTP_ITC.1 – ФБО обеспечивает предоставление доверенного канала связи при перемещении документов внутри АС и между ОО и внешними пользователями.

6.1.2 Функции безопасности ОО «Идентификация и аутентификация»

Объект оценки реализует функции идентификации и аутентификации субъектов при их обращении к БД, поддерживаемых Microsoft® Office Access 2003, а также идентификацию пользователей при задании ограничения на редактирование документов Microsoft® Office Word 2003 и книг Microsoft® Office Excel 2003. Функции аутентификации в этом случае возложены на среду функционирования ОО (операционную систему).

Microsoft® Office Access 2003

Объект оценки требует, чтобы каждый субъект доступа был идентифицирован и аутентифицирован до того момента, как от его имени в базах данных, поддерживаемых Microsoft® Office Access 2003, будут выполнены какие-либо действия.

Каждый пользователь, осуществляющий попытку доступа к БД, должен быть идентифицирован и аутентифицирован. Для обеспечения доступа пользователя к БД и выполнения в ней каких-либо действий, в ней должна существовать учетная запись пользователя, для которой уполномоченный администратор определяет права доступа к БД и назначает соответствующие разрешения на доступ к ее объектам.

Хранение учетных записей пользователей БД осуществляется в информационном файле сведений рабочей группы. Данный файл является единственной в рамках всей рабочей группы, т.е. группы пользователей, работающих с данными БД в режиме общего доступа.

Чтобы пользователь смог осуществить доступ в БД, ОО выполняет проверку того, является ли он зарегистрированным в БД пользователем и имеет ли право доступа к ней. Для этого пользователь указывает имя входа и пароль при открытии БД. В дальнейшем ОО считывает файл рабочей группы, в котором каждый пользователь идентифицируется уникальным кодом. В файле рабочей группы пользователи по их личным кодам и паролям идентифицируются как авторизованные индивидуальные пользователи и как члены конкретных групп.

В случае, если учетной записи пользователя в файле рабочей группе не существует, либо им указаны неправильные имя входа или пароль, в доступе ему будет отказано.

Microsoft® Office Word 2003

При задании уполномоченным администратором или владельцем документа ограничения на редактирование документов Microsoft® Office Word 2003 ими могут быть

указаны исключения для отдельных категорий пользователей или групп безопасности с целью разрешения редактирования определенных частей документа. При последующем доступе указанных пользователей к защищенному документу ОО осуществляет их идентификацию на основе доменной или локальной учетной записи. В случае успешной идентификации пользователей, ОО разрешает редактирование заданных частей документа.

Microsoft® Office Excel 2003

При задании уполномоченным администратором диапазонов ячеек защищенного листа книги Microsoft® Office Excel 2003 им могут быть определены группы пользователей, которые обладают возможностью изменять отдельные ячейки и диапазоны ячеек защищенного листа без знания пароля. При последующем доступе указанных пользователей к защищенным ячейкам ОО осуществляет их идентификацию на основе доменной или локальной учетной записи. В случае успешной идентификации пользователей, ОО разрешает редактирование защищенных ячеек.

Сопоставление с ФТБ

Функции безопасности «Идентификация и аутентификация» удовлетворяют следующим функциональным требованиям безопасности:

- FIA_AFL.1 – функции безопасности среды ИТ обнаруживают, когда происходит установленное администратором ОС число (не более 10) неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя, при достижении установленного числа неуспешных попыток аутентификации функции безопасности среды ИТ осуществляют блокировку регистрационной записи пользователя ОО на 30 минут;
- FIA_ATD.1 – ФБО поддерживают идентификатор пользователя и принадлежность к группе в качестве атрибутов безопасности;
- FIA_SOS.1 – функции безопасности среды ИТ предоставляют механизм для верификации качества паролей на доступ к ОО;
- FIA_UAU.2 (1) – ФБО осуществляют аутентификацию субъектов доступа к объектам БД, основанную на пароле;

- FIA_UAU.7 – ФБО обеспечивают возможность ввода аутентификационной информации в скрытом виде при осуществлении аутентификации субъектов доступа к объектам БД;
- FIA_UAU.2 (2) – функции безопасности среды ИТ обеспечивают аутентификацию до любых действий субъектов доступа к ОО и объектам ОО;
- FIA_UID.2 – ФБО осуществляют идентификацию субъектов доступа к ОО и объектам ОО до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого субъекта доступа.

6.1.3 Функции безопасности ОО «Управление безопасностью»

Объект оценки обеспечивает возможность управления ролями в Microsoft® Office Access 2003, а также предоставляет определенный набор функций управления различными политиками и характеристиками безопасности для всех компонентов ОО.

6.1.3.1 Управление ролями

Представление ролей в рамках Microsoft® Office Access 2003 реализовано через механизм назначения учетной записи пользователя полномочий посредством включения ее в состав предустановленных необязательных групп защиты или групп, самостоятельно определяемых уполномоченным администратором.

При осуществлении доступа к БД объектом оценки пользователю присваивается определенная роль, для которой определено членство и установлены соответствующие полномочия. Несмотря на то, что в ОО могут быть определены различные роли, фактически рассматриваются две логические роли: уполномоченного администратора и уполномоченного пользователя.

Роль администратора может быть представлена любой учетной записью, для которой назначены соответствующие полномочия (например, право создания, изменения и удаления любого объекта БД). Полномочия на выполнение требуемых действий для указанной учетной записи пользователя могут быть назначены напрямую либо посредством добавления данной учетной записи в состав участников предустановленной группы администраторов «Admins». Пользователю будут даны полномочия уполномоченного администратора только в том случае, если он зарегистрируется под учетной записью, для которой определены соответствующие полномочия, или, которая является участником соответствующей административной группы.

Объект оценки поддерживает предустановленных необязательных групп БД, создаваемых в момент установки. Членство в данных группах защиты предоставляет право выполнять ряд административных и системных задач, таких как резервное копирование и сжатие БД, изменение макета объектов БД, управление разрешениями доступа к данным и объектам БД и т.д. В таблице 6.1 перечислены предустановленные необязательные группы БД и представлено описание их возможностей.

Таблица 6.1 – Предустановленные группы БД

№ п/п	Название группы защиты	Описание разрешений для группы
1.	Операторы архива	Члены данной группы могут открывать базу данных с монопольным доступом для резервирования и сжатия, но не могут видеть объекты БД.
2.	Все права на данные	Члены данной группы имеют все разрешения на изменение данных, но не могут изменять макет ни одного объекта БД.
3.	Полные права	Члены данной группы имеют все разрешения на все объекты базы данных, но не могут назначать разрешения для других пользователей.
4.	Новые данные	Члены данной группы могут читать и добавлять данные, но не могут изменять макет ни одного объекта базы данных, а также удалять или обновлять данные.
5.	Разработчики проекта	Члены данной группы имеют все разрешения на изменение данных и всех объектов, но не могут изменять таблицы и связи.
6.	Только чтение	Члены данной группы могут читать все данные, но не могут изменять данные или макеты любых объектов БД.
7.	Обновление данных	Члены данной группы могут читать и обновлять данные, но не могут изменять макет ни одного объекта базы данных, а также удалять или

№ п/п	Название группы защиты	Описание разрешений для группы
		вставлять данные.

Любой пользователь, осуществивший доступ к БД и не являющийся участником какой-либо из предустановленных необязательных групп БД или группы «Admins», рассматривается как участник группы «Users», которая существует в каждой рабочей группе. Участниками группы «Users» автоматически являются все пользователи, которым разрешен доступ к БД. Данная роль обладает минимальным набором полномочий, достаточным для работы с БД и ее объектами.

6.1.3.2 Функции управления безопасностью

Объект оценки поддерживает набор политик и характеристик безопасности, которые требуют соответствующего управления. За некоторым исключением, функции по управлению безопасностью предоставлены только уполномоченному администратору. Данное ограничение реализуется через использование ролей и механизмов управления доступом. ОО поддерживает функции управления безопасностью для следующих политик и характеристик безопасности:

Политика назначения разрешений пользователя на доступ к БД – функции управления политикой назначения разрешений пользователя позволяют уполномоченному администратору управлять базой данных учетных записей пользователей БД, а также назначать или отзывать для конкретных учетных записей пользователей БД разрешения на доступ к БД и их объектам.

Политика управления автоматическим восстановлением – функции управления автоматическим восстановлением позволяют уполномоченному администратору определять частоту создания объектом оценки копии документа, содержащей несохраненные данные, которые могли быть потеряны в результате сбоя.

Политика управления правами на доступ к данным – функции управления правами на доступ к данным позволяют уполномоченному администратору управлять защитой данных на уровне отдельных файлов. При этом администратор может определять перечень субъектов, имеющих право на доступ к документам и сообщениям электронной почты, а также защищать информацию в документах, предотвращая их несанкционированный вывод на печать, пересылку и копирование.

Политика управления защитой файлов, основанной на пароле, – функции управления защитой файла, основанной на пароле, позволяют уполномоченному администратору ограничивать доступ субъектов к электронным документам посредством задания пароля на открытие файла и его запись, что позволит обеспечить защиту файла от несанкционированного просмотра и внесения изменений.

Политика управления ограничениями на редактирование и форматирование – функции управления ограничениями на редактирование и форматирование предоставляет уполномоченному администратору ограничивать набор разрешенных стилей форматирования и указывать разрешенный способ редактирования документов Microsoft® Word, а также защищать элементы листа, запретив доступ к ним всем пользователям, или предоставить доступ отдельным пользователям к определенным диапазонам ячеек. Кроме того, администратор способен определять части документа и указывать пользователей которым разрешено их редактировать.

Политика управления уровнем безопасности для макросов – функции управления уровнем безопасности для макросов позволяют уполномоченному администратору устанавливать уровень безопасности, используемый при открытии файлов, которые могут содержать вирусы в макросах, а также задавать надежных издателей макросов.

Политика блокирования вложений почтовых сообщений – функции управления политикой блокировки вложений почтовых сообщений позволяют уполномоченному администратору определять вариант поведения ОО при проверке типа расширения каждого сообщения электронной почты.

Тестирование оборудования и ФБО – функции управления тестированием оборудования и ФБО позволяют уполномоченному администратору определять условия тестирования.

Сопоставление с ФТБ

Функции безопасности «Управление безопасностью» удовлетворяют следующим функциональным требованиям безопасности:

- FMT_MSA.1 (1) – ФБО обеспечивают возможность модификации атрибутов безопасности, используемых политикой управления доступом к данным, основанной на пароле, только пользователю, уполномоченному на изменение документа;

- FMT_MSA.1 (2) – ФБО обеспечивают возможность модификации ряда атрибутов безопасности (в том числе, списка доступа и списка разрешенных стилей), используемых политикой управления доступом к данным, основанной на пароле, только пользователю, уполномоченному на изменение дополнительных атрибутов безопасности данных документа;
- FMT_MSA.3 (1) – ФБО обеспечивают установление разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой управления доступом к данным, основанной на пароле, определение альтернативных начальных значений для отмены значений по умолчанию при создании документа закрепляется за пользователем, владельцем документа;
- FMT_MSA.1 (3) – ФБО обеспечивают возможность модификации атрибутов безопасности, используемых политикой управления доступом к адресной книге, только администратору ОО;
- FMT_MSA.3 (2) – ФБО обеспечивают установление ограничительных значений по умолчанию для атрибутов безопасности, используемых политикой управления доступом к адресной книге, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта или информации закрепляется за администратором ОО;
- FMT_MSA.1 (4) – ФБО обеспечивают возможность модификации атрибутов безопасности, используемых политикой управления доступом к вложениям электронной почты, только администратору ОО;
- FMT_MSA.3 (3) – ФБО обеспечивают установление ограничительных значений по умолчанию для атрибутов безопасности, используемых политикой управления доступом к вложениям электронной почты, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта или информации закрепляется за администратором ОО;
- FMT_MSA.1 (5) – ФБО обеспечивают возможность установления и модификации атрибутов безопасности, используемых политикой управления встроенным программным кодом, только администратору ОО;
- FMT_MSA.3 (4) – ФБО обеспечивают установление ограничительных значений по умолчанию для атрибутов безопасности, используемых политикой управления встроенным программным кодом, определение альтернативных

начальных значений для отмены значений по умолчанию при создании объекта или информации закрепляется за администратором ОО;

- FMT_MSA.1 (6) – ФБО обеспечивают возможность установления и модификации атрибутов безопасности, используемых политикой фильтрации почтовых сообщений, только администратору ОО;
- FMT_MSA.3 (5) – ФБО обеспечивают установление разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой фильтрации почтовых сообщений, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта или информации закрепляется за администратором ОО;
- FMT_MSA.1 (7) – ФБО обеспечивают возможность модификации атрибутов безопасности, используемых политикой управления доступом к документам, только пользователю, владельцу документа;
- FMT_MSA.3 (6) – ФБО обеспечивает установление разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой управления доступом к документам, определение альтернативных начальных значений для отмены значений по умолчанию при создании документа закрепляется за пользователем, владельцем документа;
- FMT_MSA.1 (8) – ФБО обеспечивают возможность модификации атрибутов безопасности, используемых политикой дискреционного управления доступом, только уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта;
- FMT_MSA.3 (7) – ФБО обеспечивает установление разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой дискреционного управления доступом, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта закрепляется за уполномоченным администратором ОО и пользователем ОО, являющимся владельцем объекта;
- FMT_MTD.1 – ФБО предоставляют возможность выполнения определенных операций над данными ФБО только уполномоченному администратору ОО;
- FMT_SMR.1 – ФБО поддерживают ролевую модель, определяя роль администратора ОО и пользователя ОО и внешнего пользователя.

6.1.4 Функции безопасности ОО «Защита ФБО»

Функции безопасности ОО «Защита ФБО» обеспечивают:

- целостность системы;
- отделение домена;
- службу времени.
- автоматическое восстановление данных;
- обеспечение безопасного способа завершения работы приложения, которое прекратило отвечать на запросы.

6.1.3.3 Целостность системы

Аппаратная платформа, обеспечивающая функционирование ОО, была протестирована с целью определения поддержки функций безопасности. Тесты были направлены на определение правильности функционирования системной платы, а также периферийных устройств, таких как модули памяти, жесткий магнитный диск, видеоадаптер, порты I/O. Данные тесты были разработаны, чтобы убедиться в корректной реализации тех возможностей, которые положены в основы функций безопасности (например, обработка прерываний, управление памятью, управление заданиями и т.д.).

6.1.3.4 Разделение доменов

ФБО (при поддержке среды ИТ) обеспечивают изоляцию процессов и поддерживают домен безопасности для собственного безопасного выполнения. Домены безопасности состоят из следующих компонентов:

- аппаратных средств;
- доверенных процессов пользовательского режима;
- инструментальных средств администрирования процессов пользовательского режима.

Управление аппаратными средствами ФБО осуществляется программным обеспечением режима ядра операционной системы, под управлением которой функционирует ОО. Аппаратные средства ФБО не могут быть модифицированы недоверенными субъектами. Защита программного обеспечения ФБО режима ядра от модификации обеспечивается посредством контроля состояния функционирования аппаратных средств и защитой памяти. Аппаратные средства обеспечивают инструкции, генерирующие программные прерывания, позволяющие переходить из состояния режима

пользователя в состояние режима ядра. Программное обеспечение режима ядра осуществляет обработку всех прерываний и определяет обоснованность сделанных вызовов в режиме ядра. Механизм защиты памяти реализован таким образом, что напрямую обращаться к памяти могут только компоненты в режиме ядра. Прямое взаимодействие с памятью внешних подсистем и приложений пользовательского режима невозможно.

Среда функционирования (операционная система) обеспечивает изоляцию всех процессов пользовательского режима посредством контекста выполнения, контекста безопасности и ограничения выделенного им адресного пространства (использование механизма виртуального адресного пространства). Структура данных, определяемая адресным пространством процесса, контекстом выполнения и контекстом безопасности, храниться в защищенной памяти режима ядра.

Процессы, выполняемые в контексте учетных записей пользователей, защищены таким же образом, как и другие процессы пользовательского режима, т.е. через изоляцию посредством виртуального адресного пространства, что, собственно, обеспечивает их защищенность друг от друга.

6.1.3.5 Служба времени

Поддерживаемая ОО аппаратная платформа включает контроллер часов реального времени, представляющий устройство, доступ к которому может быть возможен только через функции, предоставляемые средой функционирования (операционной системой) ОО. В частности, среда функционирования обеспечивает функции, которые позволяют пользователям, включая сам ОО, запрашивать время, а также возможность синхронизации времени с внешним источником времени. Возможность запроса времени ни чем не ограничена, в то время как изменение системного времени требует полномочий на выполнение данной операции. Данная привилегия предоставлена только уполномоченным администраторам операционной системы с целью обеспечения непротиворечивости службы времени.

6.1.3.6 Автоматическое восстановление данных

Функция автоматического восстановления данных, поддерживается ОО для всех ее компонентов и предусматривает выполнение попыток управляемого выхода из программы в случае, если приложение неспособно функционировать вследствие какой-

либо неполадки. В этом случае ОО пытается сохранить текущую версию редактируемого документа, а также все временные версии, которые могли быть ранее записаны на диск. Далее, восстановленные файлы проверяются на наличие ошибок, а затем - в случае, если это возможно, - имеющаяся в них информация восстанавливается.

После этого, объект оценки, используя функциональную возможность автовосстановления, снова запускает программу, в работе которой произошел неустранимый сбой, и предлагает пользователю осуществить выбор в списке восстанавливаемых документов. Во многих случаях данная функция производит полное восстановление документа, что предоставляет пользователям возможность продолжить его редактирование, не потеряв при этом какой-либо информации.

Функция автоматического восстановления данных также позволяет создавать копии документов с заданной уполномоченным администратором частотой, обеспечивая, таким образом, наличие в файле автосохранения (хранимой копии документа) несохраненных данных, которые могли быть потеряны пользователем в результате сбоя.

Сопоставление с ФТБ

Функции безопасности «Защита ФБО» удовлетворяют следующим функциональным требованиям безопасности:

- FPT_AMT.1 – ФБО обеспечивают тестирование правильности выполнения предположений безопасности, представленных базовой абстрактной машиной, периодически во время нормального функционирования;
- FPT_RCV.3 – ФБО обеспечивают возвращение ОО в безопасное состояние после аварийных ситуаций и восстановления документов, с которыми пользователи осуществляли работу во время сбоя;
- FPT_TDC.1 – ФБО обеспечивают способность согласованно интерпретировать данные ФБО совместно используемые ОО и ОС;
- FPT_TST.1 – ФБО обеспечивает верификацию целостности кода ФБО;
- FPT_RVM.1 – функции безопасности среды ИТ обеспечивают, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ;
- FPT_SEP.1 – функции безопасности среды ИТ обеспечивают для ФБО домен безопасности, который защищает их от вмешательства и искажения недоверенными субъектами.

6.1.5 Функции безопасности ОО «Управление доступом к ОО»

Функции безопасности ОО «Управление доступом к ОО» обеспечивают возможность:

- защиты адресной книги;
- блокировки вложений сообщений электронной почты;
- управление уровнем безопасности для макросов;
- ограничение доступа к документам, содержащим встроенный программный код, не имеющий цифровой подписи.

6.1.5.1 Безопасность адресной книги

Объект оценки обеспечивает возможность ограничения автоматического доступа к контактным и адресным данным Outlook программного кода, использующего объектный режим Outlook, а также запрещает программам отправлять сообщения от имени пользователей. Использование данной функциональной возможности позволяет устранить возможную угрозу, связанную с распространением злонамеренного вирусного кода с использованием контактной информации, хранящейся в адресной книге.

Администратором ОО могут быть определены следующие варианты действий, выполняемых ОО при попытке программного кода обратиться напрямую к информации из адресной книги или к сведениям личного характера:

- **спрашивать у пользователя (Prompt user)** – при попытке обращения программы к контактным и адресным данным Outlook в диалоговом окне пользователю предлагается разрешить или запретить доступ к адресной книге;
- **автоматически разрешать (Automatically approve)** – доступ к полям с адресной информацией разрешен постоянно и осуществляется без предупреждения пользователя;
- **автоматически запрещать (Automatically deny)** – доступ к полям с адресной информацией запрещен постоянно и блокирование попыток обращения к ним осуществляется без предупреждения пользователя.

6.1.5.2 Блокировка вложений сообщений электронной почты

Объектом оценки обеспечивается поддержка встроенных средств блокировки вложений сообщений электронной почты, направленных на воспрепятствование распространения вирусов и других вредоносных программ, содержащихся в них.

Для реализации указанной возможности ОО анализирует тип каждого вложенного в сообщение электронной почты файла и проверяет, представлен ли данный тип во внутреннем списке запрещенных типов файлов.

Каждый тип вложенного в сообщение файла отождествляется в данном списке с одним из следующих уровней, определяющим каким образом должны обрабатываться вложения:

1. **Уровень 1.** Данный уровень присваивается файлам с расширениями *.bat, *.exe, *.vbs и *.js. Файлы данных типов блокируются ОО таким образом, что пользователи не могут просмотреть их содержимое и получить к ним доступ.

2. **Уровень 2.** К данному уровню относятся файлы всех остальных типов. В случае, если сообщение электронной почты включает в себя вложение, соответствующее уровню 2, ОО предоставляет пользователю возможность его сохранения на жестком диске. При этом сохранения файла на диске ОО блокирует все попытки его открытия или запуска. После сохранения вложения на жестком диске компьютера указанные выше ограничения объектом оценки снимаются.

При попытке пользователем отправить сообщение электронной почты, содержащее какое-либо вложение, ОО также выполняет проверку его типа. В случае, если тип вложенного файла соответствует уровню 1, т.е. он внесен в список запрещенных типов файлов, то ОО вводит на экран предупреждение о том, что получатели данного сообщения вероятно, не смогут открыть этот файл. При игнорировании предупреждения пользователем, сообщение электронной почты отправляется вместе с вложением. В противном случае, сообщение не отправляется.

Уполномоченный администратор имеет возможность определять перечень расширений файлов, включенных в список Уровня 1 или Уровня 2.

6.1.5.3 Уровни безопасности для макросов

Объект оценки обеспечивает возможность настройки уполномоченным администратором различных уровней безопасности для макросов, что позволяет улучшить управление ими и повысить безопасность во время их исполнения.

Объект оценки позволяет задавать следующий диапазон уровней безопасности для макросов:

1. **Очень высокая.** При использовании данного уровня безопасности разрешается запуск только макросов, установленных в надежных расположениях. Все остальные, подписанные и неподписанные макросы, отключаются.

2. **Высокая.** При использовании данного уровня безопасности разрешается запуск исключительно подписанных макросов из надежных источников. Неподписанные макросы автоматически отключаются ОО.

3. **Средняя.** При использовании данного уровня безопасности решение о запуске потенциально опасных макросов объектом оценки возлагается на пользователя их вызвавшего.

4. **Низкая.** При данном уровне безопасности разрешается запуск всех (подписанных и неподписанных) макросов. При этом ОО не выводит на экран никаких предупреждений. В данном режиме защита от потенциально опасных макросов полностью отсутствует.

По умолчанию объектом оценки для всех программных компонентов, входящих в его состав, устанавливается уровень безопасности для макросов, соответствующий значению «Очень высокая».

6.1.5.4 Контроль исполнения модулей и использования файлов, не имеющих цифровой подписи

Объектом оценки обеспечивается возможность поддержки списка надежных источников, что позволяет администратору реализовывать политику исполнения на компьютере исключительно тех исполняемых модулей и использования тех файлов, которые подписаны и получены от поставщиков из списка надежных источников. При этом ОО требует, чтобы цифровой подписью был подписан каждый исполняемый модуль. Цифровая подпись позволяет идентифицировать источник и обеспечивает безопасность выполнения кода.

В ОО администратор имеет возможность включать и отключать использование списка надежных источников. В случае, если использование надежных источников включено, любой устанавливаемый код (например, СОМ-надстройки, дополнительные программы, исполняемые файлы) в автоматическом режиме копируется или выполняется на компьютере исключительно при условии, что цифровая подпись данного кода принадлежит надежному источнику.

Сопоставление с ФТБ

Функции безопасности «Управление доступом к ОО» удовлетворяют следующим функциональным требованиям безопасности:

- FDP_ACC.1 (2) – ФБО обеспечивают управление доступом приложений и встроенного программного кода к адресной книге;
- FDP_ACF.1 (2) – ФБО определяют атрибуты управления доступом к адресной книге (в том числе, атрибут доступа к адресной книге), а также правила управления доступом к адресной книге;
- FDP_ACC.1 (3) – ФБО обеспечивают управление доступом пользователей ОО к файлам вложений электронной почты;
- FDP_ACF.1 (3) – ФБО определяют атрибуты управления доступом к вложениям электронной почты (в том числе, список запрещенных типов файлов вложений электронной почты и тип файла вложений электронной почты), а также правила управления доступом к вложениям электронной почты;
- FDP_ACC.1 (4) – ФБО обеспечивают управление доступом пользователей ОО к встроенным в документы программным кодам;
- FDP_ACF.1 (4) – ФБО определяют атрибуты управления доступом к встроенным программным кодам (в том числе, подпись), а также правила управления доступом к встроенным программным кодам;
- FDP_IFC.1 – ФБО обеспечивают фильтрацию почтовых сообщений;
- FDP_IFF.1 – ФБО определяют атрибуты фильтрации почтовых сообщений (в том числе, адрес электронной почты и наименование домена), а также правила фильтрации почтовых сообщений;
- FTA_TAB.2 (EXT) – ФБО обеспечивают отображение предупреждений пользователей относительно попыток выполнения ими действий, являющихся потенциально небезопасными.

6.2 Меры доверия к безопасности ОО

Для удовлетворения требований доверия к безопасности согласно ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), применены следующие меры доверия к безопасности ОО:

- управление конфигурацией;
- предоставление руководств;
- предоставление проектной документации;
- тестирование;
- оценка стойкости функций безопасности.

6.2.1 Управление конфигурацией

Меры управления конфигурацией, применяемые корпорацией Microsoft®, обеспечивают уникальную идентификацию версий ОО.

Корпорация Microsoft® осуществляет уникальную маркировку ОО, позволяющую отличать разные версии ОО. Это достигается маркированием упаковки, носителей. Кроме того, ОО может отображать свое название и номер версии при запуске программы или в ответ на запрос через графический интерфейс.

Корпорация Microsoft® использует многократную маркировку ОО – к названию и номеру версии добавляются номера пакетов исправлений и пакетов обновлений; при этом применяемые корпорацией Microsoft® меры управления конфигурацией обеспечивают согласованность меток вследствие непересечения областей значения меток.

Корпорация Microsoft® применяет меры управления конфигурацией, связывающие маркированные руководства, поставляемые в составе ОО, с данным ОО.

Сопоставление с ТДБ

Меры доверия, связанные с управлением конфигурацией, удовлетворяют следующему требованию доверия:

- ACM_CAP.1.

6.2.2 Представление руководств

Корпорация Microsoft® предоставляет руководства безопасной установки, генерации и запуска. В процедурах установки, генерации и запуска описаны шаги, необходимые для получения безопасной конфигурации ОО, описанной в ЗБ.

Корпорация Microsoft® предоставляет руководства администратора и пользователя, в которых описываются действия по выполнению функций безопасности ОО и приводятся предупреждения уполномоченным администраторам и пользователям о действиях, которые могут скомпрометировать безопасность ОО.

Сопоставление с ТДБ

Меры доверия, связанные с представлением руководств, удовлетворяют следующим требованиям доверия:

- ADO_IGS.1;
- AGD_ADM.1;
- AGD_USR.1.

6.2.3 Представление проектной документации

Проектная документация ОО, предоставляемая на оценку, включает функциональную спецификацию. Функциональная спецификация является неформальной.

В функциональной спецификации определены все внешние (то есть, видимые для пользователя или администратора) интерфейсы функций безопасности ОО, описаны режимы функционирования ОО на каждом внешнем интерфейсе, включая описание результатов, нештатных ситуаций и сообщений об ошибках.

Материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией направлены на отображения соответствия функций безопасности, представленных в функциональной спецификации, функциям безопасности, идентифицированным в краткой спецификации.

Сопоставление с ТДБ

Меры доверия, связанные с представлением проектной документации, удовлетворяют следующим требованиям доверия:

- ADV_FSP.1;
- ADV_RCR.1.

6.2.4 Тестирование

Корпорация Microsoft® предоставляет ОО, пригодный для тестирования, с соответствующей документацией, это позволяет провести независимое тестирование ФБО и сделать заключение, выполняются ли ФБО в соответствии со спецификациями.

Сопоставление с ТДБ

Меры доверия, связанные с тестированием, удовлетворяют требованию доверия:

- ATE_IND.1.

6.2.5 Оценка стойкости функций безопасности

Для механизма парольной защиты, являющегося вероятностным, предоставляется материал анализа стойкости функции безопасности (аутентификации). Анализ стойкости функции безопасности представлен в документе «Офисный программный комплекс Microsoft® Office. Профессиональный выпуск 2003. Русская версия. Свидетельство анализа стойкости функций безопасности ОО. Версия 1.0, 2005, MS.Office2003.СФБ».

Сопоставление с ТДБ

Меры доверия, связанные с оценкой стойкости функций безопасности, удовлетворяют следующему требованию доверия:

- AVA_SOF.1.

7 Утверждения о соответствии ПЗ

В данном разделе излагается утверждение о соответствии ОО конкретному профилю защиты и приводится обоснование этих утверждений.

7.1 Ссылка на ПЗ

Объект оценки соответствует профилю защиты ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты». Данное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

7.2 Конкретизация ПЗ

Все требования безопасности, сформулированные в ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005», включены в настоящее ЗБ. Некоторые из них были подвергнуты дальнейшей конкретизации.

Профиль защиты ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты» содержит ряд функциональных требований, операции над которыми при разработке ЗБ нуждались в завершении. Эти операции завершены в настоящем ЗБ в полном объеме (см. таблицу 7.1 – компоненты требований с пометкой «завершено»).

Кроме того, исходя из особенностей рассматриваемого ОО, по отношению к ряду функциональных требований, взятых из ПЗ, в настоящем ЗБ была применена операция уточнения (см. таблицу 7.1 – компоненты требований с пометкой «уточнено»).

Функциональные требования, операции над которыми были завершены, а также требования, уточненные в ЗБ относительно ПЗ, приведены в таблице 7.1.

Таблица 7.1 – Конкретизация функциональных требований по отношению к ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005»

Наименование требования	Изменение
Функциональные требования ОО	
FDP_ACC.1 (1)	завершено
FDP_ACF.1 (1)	завершено
FDP_ACC.1 (2)	завершено
FDP_ACF.1 (2)	завершено
FDP_ACC.1 (3)	завершено
FDP_ACF.1 (3)	завершено
FDP_ACC.1 (4)	завершено
FDP_ACF.1 (4)	завершено
FDP_IFF.1	завершено
FDP_UIT.1	завершено
FIA_ATD.1	завершено
FMT_MSA.1 (1)	завершено
FMT_MSA.1 (2)	завершено
FMT_MSA.1 (3)	завершено
FMT_MSA.1 (4)	завершено
FMT_MSA.1 (5)	завершено
FMT_MSA.1 (6)	завершено
FMT_MTD.1	завершено
FMT_SMR.1	завершено
FPT_RCV.3	завершено, уточнено
FPT_TDC.1	завершено, уточнено
FTA_TAB.2 (EXT)	завершено
FTP_ITC.1	завершено

Наименование требования	Изменение
Функциональные требования среды ИТ	
FIA_AFL.1	завершено
FIA_SOS.1	завершено

7.3 Дополнение ПЗ

В настоящее ЗБ включена следующая политика безопасности организации, не вошедшая в ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005»:

P.AccessDoc

Должен быть обеспечен доступ к защищаемым документам только уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям. Должна быть обеспечена возможность уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям ограничивать права доступа к защищаемым документам для других пользователей ОО и администраторов ОО, а также внешних пользователей.

В настоящее ЗБ включена следующая цель безопасности для ОО, не вошедшая в ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005»:

O.AccessDoc

Разграничение доступа к документам

ОО должен обеспечивать доступ к защищаемым документам только уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям. ОО должен обеспечивать возможность уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям ограничивать права доступа к защищаемым документам для других пользователей ОО и администраторов ОО, а также внешних пользователей.

В настоящее 3Б включены следующие функциональные требования безопасности ОО, не вошедшие в ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005»:

- FDP_ACC.1 (5) «Ограниченное управление доступом»;
- FDP_ACF.1 (5) «Управление доступом, основанное на атрибутах безопасности»;
- FDP_ACC.1 (6) «Ограниченное управление доступом»;
- FDP_ACF.1 (6) «Управление доступом, основанное на атрибутах безопасности»;
- FIA_UAU.2 (1) «Аутентификация до любых действий пользователя»;
- FIA_UAU.7 «Аутентификация с защищенной обратной связью»;
- FMT_MSA.3 (6) «Инициализация статических атрибутов»;
- FMT_MSA.1 (7) «Управление атрибутами безопасности»;
- FMT_MSA.3 (7) «Инициализация статических атрибутов»;
- FMT_MSA.1 (8) «Управление атрибутами безопасности».

8 Обоснование

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

8.1 Обоснование целей безопасности

8.1.1 Обоснование целей безопасности для ОО

В таблице 8.1 приведено отображение целей безопасности на угрозы и политику безопасности.

Таблица 8.1 – Отображение целей безопасности на угрозы и политику безопасности организации

	O.AccessData	O.AccessDoc	O.Establishment	O.AddressBook	O.Enclosure	O.Firmware	O.Filtration	O.Protect	O.Metadata	O.Recovery	O.Administration	O.Operation	O.Caution
T.UnauthAccess	X												
T.ModifStyle	X												
T.AccAddrBook				X									
T.AccEnclosure					X								
T.AccFirmware						X							
T.FiltrPostMessage							X						
T.ViolationConf								X					
T.ViolationInt								X					
T.AccMetadata									X				
T.LostData										X			
P.Reference			X										
P.Admin											X		
P.ConformOperation												X	
P.Caution													X
P.AccessDoc		X											

O.AccessData

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccess** и **T.ModifStyle**, так как обеспечивает доступ к защищаемым данным документов для ознакомления и модификации (в том числе и изменение формы представления документа, использование стилей, отличных от определенных в документе) только уполномоченным на это пользователям.

O.AccessData

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **P.AccessDoc**, так как обеспечивает доступ к защищаемым документам только уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям и возможность уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям ограничивать права доступа к защищаемым документам для других пользователей ОО и администраторов ОО, а также внешних пользователей.

O.Establishment

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **P.Reference**, так как предоставляет возможность установления полномочий на доступ к защищаемым данным документа пользователям, создающим документ, а также уполномоченным на это пользователям. Полномочия на доступ к защищаемым данным документа устанавливаются в соответствии с политикой безопасности, принятой в АС.

O.AddressBook

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.AccAddrBook**, так как предотвращает попытки доступа приложений и встроенного в документы программного кода к адресной книге несанкционированные администратором ОО.

O.Enclosure

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.AccEnclosure**, так как предотвращает попытки доступа пользователей ОО к запрещенным файлам вложений электронной почты.

O.Firmware

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.FiltrPostMessage**, так как предотвращает доступ и выполнение пользователями ОО неподписанного встроенного в документы программного кода.

O.Filtration

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.AccEnclosure**, так как обеспечивает фильтрацию почтовых сообщений, поступающих в ОО и/или выходящих из ОО.

O.Protect

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.ViolationConf** и **T.ViolationInt**, так как обеспечивает конфиденциальность, целостность и подлинность данных документов при перемещении документов внутри АС, а также при передаче документов внешним пользователям, обеспечивает возможность однозначного определения подлинности пользователя, осуществившего передачу документа.

O.Metadata

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.AccMetadata**, так как обеспечивает удаление метаданных в документах при запросе уполномоченных пользователей.

O.Recovery

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **T.LostData**, так как обеспечивает корректное восстановление функционирования ОО, а также возможность восстановления данных, которые формировались пользователем ОО

лично, либо группой пользователей с использованием среды совместной разработки, в случаях сбоев (отказов) ПО и аппаратных средств, в том числе сбоях источников электропитания.

O.Administration

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **P.Admin**, так как обеспечивает наличие надлежащих корректно функционирующих средств администрирования ОО доступных только уполномоченным администраторам ОО.

O.Operation

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **P.ConformOperation**, так как обеспечивает корректное и надлежащее функционирование ОО в среде функционирования (операционной системе) и согласованную интерпретацию данных, совместно используемых ОО и средой функционирования.

O.Caution

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **P.Caution**, так как обеспечивает предупреждение пользователей относительно попыток выполнения ими действий, являющихся потенциально небезопасными, согласно политике безопасности АС, а также при выполнении ОО блокирования действий оцененных ОО как небезопасные.

8.1.2 Обоснование целей безопасности для среды

В таблице 8.2 приведено отображение целей безопасности на угрозы и политику безопасности.

Таблица 8.2 – Отображение целей безопасности для среды на предположения безопасности и угрозы, которым противостоит среда

	OE.OSAuth	OE.Environment	OE.Security	OE.ProtectFileSystem	OE.LocateTOE	OE.NoEvilAdm	OE.RecoverySafeState	OE.ProtectResTSF
A.OSAuth	X							
A.Environment		X						
A.Security			X					
A.RecoverySafeState							X	
A.LocateTOE					X			
A.NoEvilAdm						X		
TE.UnauthAccessTOE	X							
TE.MasqAdmin&User	X							
TE.UnauthAccessTSF								X
TE.UnauthAccessData				X				

OE.OSAuth

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.OSAuth** и противостояния угрозам **TE.UnauthAccessTOE** и **TE.MasqAdmin&User**, так как обеспечивает осуществление аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов ОС, под управлением которой функционирует ОО.

OE.Environment

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Environment**, так как обеспечивает осуществление функционирования ОО в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.

OE.Security

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Security**, так как обеспечивает надлежащую безопасную настройку всех составляющих ОО компонентов и отсутствие в составе ОО таких компонентов, уровень безопасности которых (определяемый настройками администратора ОО) мог бы приводить к небезопасному использованию всего ОО в целом.

OE.ProtectFileSystem

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **TE.UnauthAccessData**, так как обеспечивает защиту данных ОО на уровне файлов файловой системы ОС от несанкционированного доступа.

OE.LocateTOE

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

OE.NoEvilAdm

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.NoEvilAdm**, так как обеспечивает благонадежность и компетентность персонала, ответственного за администрирование ОО, а также их деятельность в соответствии с документацией на ОО.

OE.RecoverySafeState

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.RecoverySafeState**, так как обеспечивает выполнение мероприятий, направленных на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

OE.ProtectResTSF

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **TE.UnauthAccessTSF**, так как обеспечивает защиту данных ФБО и ресурсов ОО, а также поддержку домена для функционирования ФБО.

8.2 Обоснование требований безопасности

8.2.1 Обоснование требований безопасности для ОО

8.2.1.1 Обоснование функциональных требований безопасности ОО

В таблице 8.3 представлено отображение функциональных требований безопасности на цели безопасности для ОО.

Таблица 8.3 – Отображение функциональных требований безопасности на цели безопасности

	O.AccessData	O.AccessDoc	O.Establishment	O.AddressBook	O.Enclosure	O.Firmware	O.Filtration	O.Protect	O.Metadata	O.Recovery	O.Administration	O.Operation	O.Caution
FDP_ACC.1 (1)	X												
FDP_ACF.1 (1)	X												
FDP_ACC.1 (2)				X									
FDP_ACF.1 (2)				X									
FDP_ACC.1 (3)					X								
FDP_ACF.1 (3)					X								
FDP_ACC.1 (4)						X							
FDP_ACF.1 (4)						X							
FDP_ACC.1 (5)		X											
FDP_ACF.1 (5)		X											
FDP_ACC.1 (6)		X											
FDP_ACF.1 (6)		X											
FDP_IFC.1							X						
FDP_IFF.1							X						
FDP_UCT.1								X					
FDP_UIT.1								X					
FDP_MDD.1 (EXT)									X				

	O.AccessData	O.AccessDoc	O.Establishment	O.AddressBook	O.Enclosure	O.Firmware	O.Filtration	O.Protect	O.Metadata	O.Recovery	O.Administration	O.Operation	O.Caution
FIA_ATD.1			X										
FIA_UAU.2 (1)		X											
FIA_UAU.7		X											
FIA_UID.2	X		X										
FMT_MSA.1 (1)			X										
FMT_MSA.1 (2)			X										
FMT_MSA.3 (1)			X										
FMT_MSA.1 (3)											X		
FMT_MSA.3 (2)											X		
FMT_MSA.1 (4)											X		
FMT_MSA.3 (3)											X		
FMT_MSA.1 (5)											X		
FMT_MSA.3 (4)											X		
FMT_MSA.1 (6)											X		
FMT_MSA.3 (5)											X		
FMT_MSA.1 (7)		X											
FMT_MSA.3 (6)		X											
FMT_MSA.1 (8)		X											
FMT_MSA.3 (7)		X											
FMT_MTD.1											X		
FMT_SMR.1			X								X		
FPT_AMT.1										X			
FPT_RCV.3										X			
FPT_TDC.1												X	
FPT_TST.1										X			

	O.AccessData	O.AccessDoc	O.Establishment	O.AddressBook	O.Enclosure	O.Firmware	O.Filtration	O.Protect	O.Metadata	O.Recovery	O.Administration	O.Operation	O.Caution
FTA_TAB.2 (EXT)													X
FTP_ITC.1								X					

FDP_ACC.1 (1) Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает управление доступом пользователей ОО и внешних пользователей к данным документов. Рассматриваемый компонент сопоставлен с целью **O.AccessData** и способствует ее достижению.

FDP_ACF.1 (1) Управление доступом, основанное на атрибутах безопасности

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FDP_ACC.1 (1) и определяет атрибуты управления доступом к данным (в том числе, идентификатор пользователя, введенный пароль при доступе к документу, идентификатор стиля; список доступа, список разрешенных стилей, пароль для доступа к документу на чтение, пароль для доступа к документу на изменение), а также правила управления доступом к данным. Рассматриваемый компонент сопоставлен с целью **O.AccessData** и способствует ее достижению.

FDP_ACC.1 (2) Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает управление доступом приложений и встроенного программного кода к адресной книге. Рассматриваемый компонент сопоставлен с целью **O.AddressBook** и способствует ее достижению.

FDP_ACF.1 (2) Управление доступом, основанное на атрибутах безопасности

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FDP_ACC.1 (2) и определяет атрибуты управления доступом к адресной книге (в том числе, атрибут доступа к адресной книге), а также правила управления доступом к

адресной книге. Рассматриваемый компонент сопоставлен с целью **O.AddressBook** и способствует ее достижению.

FDP_ACC.1 (3) Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает управление доступом пользователей ОО к файлам вложений электронной почты. Рассматриваемый компонент сопоставлен с целью **O.Enclosure** и способствует ее достижению.

FDP_ACF.1 (3) Управление доступом, основанное на атрибутах безопасности

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FDP_ACC.1 (3) и определяет атрибуты управления доступом к вложениям электронной почты (в том числе, список запрещенных типов файлов вложений электронной почты и тип файла вложений электронной почты), а также правила управления доступом к вложениям электронной почты. Рассматриваемый компонент сопоставлен с целью **O.Enclosure** и способствует ее достижению.

FDP_ACC.1 (4) Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает управление доступом пользователей ОО к встроенным в документы программным кодам. Рассматриваемый компонент сопоставлен с целью **O.Firmware** и способствует ее достижению.

FDP_ACF.1 (4) Управление доступом, основанное на атрибутах безопасности

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FDP_ACC.1 (4) и определяет атрибуты управления доступом к встроенным программным кодам (в том числе, подпись), а также правила управления доступом к встроенным программным кодам. Рассматриваемый компонент сопоставлен с целью **O.Firmware** и способствует ее достижению.

FDP_ACC.1 (5) Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает управление доступом пользователей ОО и внешних пользователей к документам. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FDP_ACF.1 (5) Управление доступом, основанное на атрибутах безопасности

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FDP_ACC.1 (5) и определяет атрибуты управления доступом к документам, а также правила управления доступом к документам, используемые в политике управления доступом к документам. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FDP_ACC.1 (6) Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает управление доступом пользователей ОО к объектам БД. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FDP_ACF.1 (6) Управление доступом, основанное на атрибутах безопасности

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FDP_ACC.1 (6) и определяет атрибуты управления доступом к объектам БД, а также правила управления доступом к объектам БД, используемые в политике дискреционного управления доступом. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FDP_IFC.1 Ограниченное управление информационными потоками

Выполнение требований данного компонента обеспечивает фильтрацию почтовых сообщений. Рассматриваемый компонент сопоставлен с целью **O.Filtration** и способствует ее достижению.

FDP_IFF.1 Простые атрибуты безопасности

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FDP_IFC.1 и определяет атрибуты фильтрации почтовых сообщений (в том числе, адрес электронной почты и наименование домена), а также правила фильтрации почтовых сообщений. Рассматриваемый компонент сопоставлен с целью **O.Filtration** и способствует ее достижению.

FDP_UCT.1 Базовая конфиденциальность обмена данными

Выполнение требований данного компонента обеспечивает защиту данных пользователя от несанкционированного раскрытия при перемещении данных. Рассматриваемый компонент сопоставлен с целью **O.Protect** и способствует ее достижению.

FDP_UIT.1 Целостность передаваемых данных

Выполнение требований данного компонента обеспечивает защиту целостности данных пользователя при перемещении данных. Рассматриваемый компонент сопоставлен с целью **O.Protect** и способствует ее достижению.

FDP_MDD.1 (EXT) Удаление метаданных в документах

Выполнение требований данного компонента обеспечивает возможность удаления метаданных в документах по запросу пользователей, уполномоченных на изменение документа. Рассматриваемый компонент сопоставлен с целью **O.Metadata** и способствует ее достижению.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя атрибутов безопасности (в том числе, идентификатор пользователя и принадлежность к группе). Рассматриваемый компонент сопоставлен с целью **O.Establishment** и способствует ее достижению.

FIA_UAU.2 (1) Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает аутентификацию субъектов доступа к объектам БД до разрешения любого действия, выполняемого при

посредничестве ФБО от имени этого субъекта доступа. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FIA_UAU.7 Аутентификация с защищенной обратной связью

Выполнение требований данного компонента обеспечивает предоставление субъекту доступа к объектам БД возможности ввода аутентификационной информации в скрытом виде во время выполнения аутентификации. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** 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 целями **O.AccessData**, **O.Establishment** и способствует их достижению.

FMT_MSA.1 (1) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модификации атрибутов безопасности, используемых политикой управления доступом к данным, основанной на пароле, только пользователю, уполномоченному на изменение документа. Рассматриваемый компонент сопоставлен с целью **O.Establishment** и способствует ее достижению.

FMT_MSA.1 (2) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модификации ряда атрибутов безопасности (в том числе, списка доступа и списка разрешенных стилей), используемых политикой управления доступом к данным, основанной на пароле, только пользователю, уполномоченному на изменение дополнительных атрибутов безопасности данных документа. Рассматриваемый компонент сопоставлен с целью **O.Establishment** и способствует ее достижению.

FMT_MSA.3 (1) Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает установление разрешающих значений по умолчанию для атрибутов безопасности, используемых

политикой управления доступом к данным, основанной на пароле, определение альтернативных начальных значений для отмены значений по умолчанию при создании документа закрепляется за пользователем, владельцем документа. Рассматриваемый компонент сопоставлен с целью **O.Establishment** и способствует ее достижению.

FMT_MSA.1 (3) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модификации атрибутов безопасности, используемых политикой управления доступом к адресной книге, только администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_MSA.3 (2) Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает установление ограничительных значений по умолчанию для атрибутов безопасности, используемых политикой управления доступом к адресной книге, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта или информации закрепляется за администратором ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_MSA.1 (4) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модификации атрибутов безопасности, используемых политикой управления доступом к вложениям электронной почты, только администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_MSA.3 (3) Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает установление ограничительных значений по умолчанию для атрибутов безопасности, используемых политикой управления доступом к вложениям электронной почты, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта или информации закрепляется за администратором ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_MSA.1 (5) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность установления и модификации атрибутов безопасности, используемых политикой управления встроенным программным кодом, только администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_MSA.3 (4) Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает установление ограничительных значений по умолчанию для атрибутов безопасности, используемых политикой управления встроенным программным кодом, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта или информации закрепляется за администратором ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_MSA.1 (6) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность установления и модификации атрибутов безопасности, используемых политикой фильтрации почтовых сообщений, только администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_MSA.3 (5) Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает установление разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой фильтрации почтовых сообщений, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта или информации закрепляется за администратором ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_MSA.1 (7) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модификации атрибутов безопасности, используемых политикой управления доступом к

документам, только пользователю, владельцу документа. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FMT_MSA.3 (6) Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает установление разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой управления доступом к документам, определение альтернативных начальных значений для отмены значений по умолчанию при создании документа закрепляется за пользователем, владельцем документа. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FMT_MSA.1 (8) Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модификации атрибутов безопасности, используемых политикой дискреционного управления доступом к объектам БД, только уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FMT_MSA.3 (7) Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает установление разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой дискреционного управления доступом к объектам БД, определение альтернативных начальных значений для отмены значений по умолчанию при создании объекта закрепляется за уполномоченным администратором ОО и пользователем ОО, являющимся владельцем объекта. Рассматриваемый компонент сопоставлен с целью **O.AccessDoc** и способствует ее достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента обеспечивает возможность выполнения определенных операций на данными ФБО, только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.Administration** и способствует ее достижению.

FMT_SMR.1 Роли безопасности

Данный компонент включен в ЗБ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту определенной роли. Рассматриваемый компонент сопоставлен с целями **O.Establishment** и **O.Administration** и способствует их достижению.

FPT_AMT.1 Тестирование абстрактной машины

Выполнение требований данного компонента обеспечивает тестирование правильности выполнения предположений безопасности, представленных базовой абстрактной машиной, периодически во время нормального функционирования. Рассматриваемый компонент сопоставлен с целью **O.Recovery** и способствует ее достижению.

FPT_RCV.3 Автоматическое восстановление без недопустимой потери

Выполнение требований данного компонента обеспечивает возвращение ОО в безопасное состояние после аварийных ситуаций и восстановления документов, с которыми пользователи осуществляли работу во время сбоя. Рассматриваемый компонент сопоставлен с целью **O.Recovery** и способствует ее достижению.

FPT_TDC.1 Базовая согласованность данных ФБО между ФБО

Выполнение требований данного компонента обеспечивает способность согласованно интерпретировать данные ФБО совместно используемые ОО и ОС. Рассматриваемый компонент сопоставлен с целью **O.Recovery** и способствует ее достижению.

FPT_TST.1 Тестирование ФБО

Выполнение требований данного компонента обеспечивает верификацию целостности кода ФБО. Рассматриваемый компонент сопоставлен с целью **O.Recovery** и способствует ее достижению.

FTA_TAB.2 (EXT) Предупреждающие сообщения

Выполнение требований данного компонента обеспечивает отображение предупреждений пользователей относительно попыток выполнения ими действий,

являющихся потенциально небезопасными. Рассматриваемый компонент сопоставлен с целью **O.Caution** и способствует ее достижению.

FTP_ITS.1 Доверенный канал передачи между ФБО

Выполнение требований данного компонента обеспечивает предоставление доверенного канала связи при перемещении документов внутри АС и между ОО и внешними пользователями. Рассматриваемый компонент сопоставлен с целью **O.Protect** и способствует ее достижению.

8.2.1.2 Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ЗБ соответствуют ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), и сформулированы, исходя из соответствия настоящего ЗБ профилю защиты ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005».

Выбор ОУД1 в качестве основы требований доверия в настоящем ЗБ является достаточным при определении допустимости использования ОО при обработке конфиденциальной информации.

8.2.2 Обоснование требований безопасности для среды ИТ

В таблице 8.4 представлено отображение функциональных требований безопасности среды ИТ на цели безопасности для среды.

Таблица 8.4 – Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	OE.OSAuth	OE.ProtectResTSF
FIA_AFL.1	X	
FIA_SOS.1	X	
FIA_UAU.2 (2)	X	

	OE.OSAuth	OE.ProtectResTSF
FPT_RVM.1		X
FPT_SEP.1		X

FIA_AFL.1 Обработка отказов аутентификации

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

FIA_UAU.2 (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 **OE.OSAuth** 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 **OE.ProtectResTSF** и способствует ее достижению.

FPT_SEP.1

Отделение домена ФБО

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

8.2.3 Обоснование зависимостей требований

В таблице 8.5 представлены результаты удовлетворения зависимостей функциональных требований. Все зависимости компонентов требований удовлетворены в настоящем ЗБ либо включением компонентов, определенных в части 2 ОК под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в части 2 ОК под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 8.5 является справочным и содержит компоненты, определенные в части 2 ОК в описании компонентов требований, приведенных в столбце 1 таблицы 8.5, под рубрикой «Зависимости».

Столбец 3 таблицы 8.5 показывает, какие компоненты требований были реально включены в настоящее ЗБ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 8.5. Компоненты требований в столбце 3 таблицы 8.5 либо совпадают с компонентами в столбце 2 таблицы 8.5, либо иерархичны по отношению к ним.

Таблица 8.5 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
Зависимости функциональных требований ОО		
FDP_ACC.1 (1)	FDP_ACF.1	FDP_ACF.1 (1)
FDP_ACF.1 (1)	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1 (1), FMT_MSA.3 (1)
FDP_ACC.1 (2)	FDP_ACF.1	FDP_ACF.1 (2)
FDP_ACF.1 (2)	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1 (2), FMT_MSA.3 (2)
FDP_ACC.1 (3)	FDP_ACF.1	FDP_ACF.1 (3)
FDP_ACF.1 (3)	FDP_ACC.1,	FDP_ACC.1 (3),

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
	FMT_MSA.3	FMT_MSA.3 (3)
FDP_ACC.1 (4)	FDP_ACF.1	FDP_ACF.1 (4)
FDP_ACF.1 (4)	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1 (4), FMT_MSA.3 (4)
FDP_ACC.1 (5)	FDP_ACF.1	FDP_ACF.1 (5)
FDP_ACF.1 (5)	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1 (5), FMT_MSA.3 (6)
FDP_ACC.1 (6)	FDP_ACF.1	FDP_ACF.1 (6)
FDP_ACF.1 (6)	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1 (6), FMT_MSA.3 (7)
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1, FMT_MSA.3 (5)
FDP_UCT.1	[FTP_ITC.1 или FTP_TRP.1], [FDP_ACC.1 или FDP_IFC.1]	FTP_ITC.1, FDP_ACC.1 (1)
FDP_UIT.1	[FDP_ACC.1 или FDP_IFC.1], [FTP_ITC.1 или FTP_TRP.1]	FDP_ACC.1 (1), FTP_ITC.1
FIA_UAU.2 (1)	FIA_UID.1	FIA_UID.2
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 (1)
FMT_MSA.1 (1)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1 (1), FMT_SMR.1
FMT_MSA.1 (2)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1 (1), FMT_SMR.1

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
FMT_MSA.3 (1)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_SMR.1
FMT_MSA.1 (3)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1 (2), FMT_SMR.1
FMT_MSA.3 (2)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (3), FMT_SMR.1
FMT_MSA.1 (4)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1 (3), FMT_SMR.1
FMT_MSA.3 (3)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (4), FMT_SMR.1
FMT_MSA.1 (5)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1 (4), FMT_SMR.1
FMT_MSA.3 (4)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (5), FMT_SMR.1
FMT_MSA.1 (6)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1 (4), FMT_SMR.1
FMT_MSA.3 (5)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (6), FMT_SMR.1
FMT_MSA.1 (7)	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1 (5), FMT_SMR.1
FMT_MSA.3 (6)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (7), FMT_SMR.1
FMT_MSA.1 (8)	[FDP_ACC.1 или FDP_IFC.1],	FDP_ACC.1 (6), FMT_SMR.1

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
	FMT_SMR.1	
FMT_MSA.3 (7)	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1 (8), FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RCV.3	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
Зависимости функциональных требований среды ИТ		
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (2)
FIA_UAU.2 (2)	FIA_UID.1	FIA_UID.2

Включение в ЗБ компонента FPT_RCV.3 требует для удовлетворения зависимостей включения компонента ADV_SPM.1, однако разработчиком в руководствах ОО достаточно предоставить четкое определение безопасного состояния ФБО, при котором ФБО не противоречивы и продолжают корректное осуществление ПБО и объяснение, почему такое состояние можно считать безопасным, при выполнении этого требования зависимость компонента FPT_RCV.1 от компонента ADV_SPM.1 можно не учитывать.

Усиление ОУД1 компонентом AVA_SOF.1 (Оценка стойкости функции безопасности) требует включения в ЗБ для удовлетворения зависимостей компонента требований доверия к безопасности – ADV_HLD.1 (Описательный проект верхнего уровня). Это включение вызвано тем, что оценщику может потребоваться информация из проекта верхнего уровня для анализа того, как работают несколько разных механизмов для обеспечения функции безопасности «Аутентификация». Минимальный уровень такой информации предоставляется через зависимость ADV_HLD. Но, так как функция безопасности «Аутентификация» в рассматриваемом ОО обеспечивается одним

механизмом – «механизмом пароля», информацию об этом механизме достаточно подробно изложить в ЗБ, функциональной спецификации и руководствах, и зависимостью ADV_HLD.1 (Описательный проект верхнего уровня) можно пренебречь.

8.3 Обоснование краткой спецификации ОО

Обоснование краткой спецификации ОО представлено таблицей 8.6 и таблицей 8.7.

Таблица 8.6 – Отображение функциональных требований безопасности на функции безопасности

	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Управление доступом к ОО
FDP_ACC.1 (1)	X				
FDP_ACF.1 (1)	X				
FDP_ACC.1 (2)					X
FDP_ACF.1 (2)					X
FDP_ACC.1 (3)					X
FDP_ACF.1 (3)					X
FDP_ACC.1 (4)					X
FDP_ACF.1 (4)					X
FDP_ACC.1 (5)	X				
FDP_ACF.1 (5)	X				
FDP_ACC.1 (6)	X				
FDP_ACF.1 (6)	X				
FDP_IFC.1					X

	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Управление доступом к ОО
FDP_IFF.1					X
FDP_UCT.1	X				
FDP_UIT.1	X				
FDP_MDD.1 (EXT)	X				
FIA_ATD.1		X			
FIA_UAU.2 (1)		X			
FIA_UAU.7		X			
FIA_UID.2		X			
FMT_MSA.1 (1)			X		
FMT_MSA.1 (2)			X		
FMT_MSA.3 (1)			X		
FMT_MSA.1 (3)			X		
FMT_MSA.3 (2)			X		
FMT_MSA.1 (4)			X		
FMT_MSA.3 (3)			X		
FMT_MSA.1 (5)			X		
FMT_MSA.3 (4)			X		
FMT_MSA.1 (6)			X		
FMT_MSA.3 (5)			X		
FMT_MSA.1 (7)			X		
FMT_MSA.3 (6)			X		

	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Управление доступом к ОО
FMT_MSA.1 (8)			X		
FMT_MSA.3 (7)			X		
FMT_MTD.1			X		
FMT_SMR.1			X		
FPT_AMT.1				X	
FPT_RCV.3				X	
FPT_TDC.1				X	
FPT_TST.1				X	
FTA_TAB.2 (EXT)					X
FTP_ITC.1	X				

Таблица 8.7 – Отображение требований доверия на меры безопасности

	Управление конфигурацией	Предоставление руководств	Предоставление проектной документации	Тестирование	Оценка стойкости функций безопасности
ACM_CAP.1	X				
ADO_IGS.1		X			
ADV_FSP.1			X		
ADV_RCR.1			X		
AGD_ADM.1		X			
AGD_USR.1		X			
ATE_IND.1				X	
AVA_SOF.1					X

8.4 Обоснование требований к стойкости функций безопасности

Термин «стойкость функции» определен в части 1 ОК как характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного режима при прямой атаке на лежащие в ее основе механизмы безопасности. В части 1 ОК определено три уровня стойкости функции: базовая СФБ, средняя СФБ и высокая СФБ. В настоящем ЗБ выбран уровень стойкости функции – средняя СФБ. Средняя СФБ – это уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения. Выбор СФБ в ЗБ определялся, исходя из возможностей ОО и обеспечения соответствия ОО профилю защиты ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005». Выбор средней СФБ в качестве минимального уровня стойкости функций безопасности является

достаточным при определении допустимости использования ОО при обработке конфиденциальной информации.

8.5 Обоснование утверждений о соответствии ПЗ

Объект оценки соответствует ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005». Данное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

8.5.1 Обоснование конкретизации требований безопасности ИТ

Все требования безопасности, сформулированные в ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты», включены в настоящее ЗБ. Некоторые из них были подвергнуты дальнейшей конкретизации.

Профиль защиты ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005» содержит ряд функциональных требований, операции над которыми при разработке ЗБ нуждались в завершении. Операции подобных требований завершены в настоящем ЗБ в полном объеме.

Исходя из особенностей рассматриваемого ОО, по отношению к ряду функциональных требований, взятых из ПЗ, в настоящем ЗБ была применена операция уточнения.

FPT_RCV.3 – уточнено относительно ПЗ в связи с особенностями ОО – возможностью возврата безопасного состояния ОО в случае сбоев (отказов) программного и аппаратного обеспечения ОО.

FPT_TDC.1 – уточнено относительно ПЗ в связи с особенностями ОО – использованием в качестве ИТ среды функционирования ОС.

8.5.2 Обоснование добавления политик безопасности организации

В настоящее ЗБ включена следующая политика безопасности организации, не вошедшая в ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005»:

P.AccessDoc – включена в связи с возможностью ОО, связанной с обеспечением доступа к защищаемым документам только уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям, а также обеспечением возможности уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям ограничивать права доступа к защищаемым документам для других пользователей ОО и администраторов ОО, а также внешних пользователей.

8.5.3 Обоснование добавления целей безопасности для ОО

В настоящее ЗБ включена следующая цель безопасности для ОО, не вошедшая в ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005»:

O.AccessDoc – ОО должен обеспечивать доступ к защищаемым документам только уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям. ОО должен обеспечивать возможность уполномоченным на это пользователям ОО, администраторам ОО и внешним пользователям ограничивать права доступа к защищаемым документам для других пользователей ОО и администраторов ОО, а также внешних пользователей.

Включение данной цели безопасности для ОО связано с добавлением в ЗБ политики безопасности организации **P.AccessDoc** и необходимостью ее реализации.

8.5.4 Обоснование добавления требований безопасности ИТ

В настоящее ЗБ включены следующие функциональные требования безопасности ОО, не вошедшие в ПЗ ОПК.ПЗ «Безопасность информационных технологий. Офисные программные комплексы. Профиль защиты. Версия 1.0, 2005»:

Компонент функциональных требований безопасности FDP_ACC.1 (5) – включен в связи с возможностью ОО реализовывать политику управления доступом к документам.

Компонент функциональных требований безопасности FDP_ACF.1 (5) – включен в связи с возможностью ОО осуществлять управление доступом к документам по определенным правилам, с использованием определенных атрибутов и в соответствии с политикой управления доступом к документам.

Компонент функциональных требований безопасности FDP_ACC.1 (6) – включен в связи с возможностью ОО реализовывать политику дискреционного управления доступом к объектам БД.

Компонент функциональных требований безопасности FDP_ACF.1 (6) – включен в связи с возможностью ОО осуществлять дискреционное управление доступом к объектам БД по определенным правилам, с использованием определенных атрибутов и в соответствии с политикой дискреционного управления доступом.

Компонент функциональных требований безопасности FIA_UAU.2 (1) – включен в связи с возможностью ОО осуществлять аутентификацию субъектов доступа к объектам БД.

Компонент функциональных требований безопасности FIA_UAU.7 – включен в связи с возможностью ОО осуществлять ввод аутентификационных данных при доступе к объектам БД в скрытом виде.

Компонент функциональных требований безопасности FMT_MSA.3 (6) – включен в связи с возможностью ОО, связанной с установлением разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой управления доступом к документам.

Компонент функциональных требований безопасности FMT_MSA.1 (7) – включен в связи с возможностью ОО, связанной с модификацией атрибутов безопасности, используемых политикой управления доступом к документам только пользователем, владельцем документа.

Компонент функциональных требований безопасности FMT_MSA.3 (7) – включен в связи с возможностью ОО, связанной с установлением разрешающих значений по умолчанию для атрибутов безопасности, используемых политикой дискреционного управления доступом к объектам БД.

Компонент функциональных требований безопасности FMT_MSA.1 (8) – включен в связи с возможностью ОО, связанной с модификацией атрибутов безопасности, используемых политикой дискреционного управления доступом к объектам БД только уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта.