ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-2— 2008

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 2

Функциональные требования безопасности

ISO/IEC 15408-2:2005
Information technology—Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements (IDT)

Издание официальное

БЗ 12—2007/464

Москва
Стандартинформ
2009

Федеральное агентство по техническому регулированию и метрологии

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным государственным учреждением «4 Центральный научно-исследовательский институт Министерства обороны России» (ФГУ «4 ЦНИИ Минобороны России»), Федеральным государственным унитарным предприятием «Научно-технический и сертификационный центр по комплексной защите информации» ФГУП Центр «Атомзащитаинформ», Федеральным государственным унитарным предприятием «Центральный научно-исследовательский институт управления, экономики и информации Росатома» (ФГУП «ЦНИИАТОМИНФОРМ») при участии экспертов Международной рабочей группы по Общим критериям на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 520-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15408-2:2005 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности» (ISO/IEC 15408-2:2005 «Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении N

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 15408-2—2002

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2009

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины, определения, обозначения и сокращения . . . 1
4 Краткий обзор . . . 1
4.1 Структура данной части ИСО/МЭК 15408 . . . 1
5 Парадигма функциональных требований . . . 2
6 Функциональные компоненты безопасности . . . 6
6.1 Краткий обзор . . . 6
6.2 Каталог компонентов . . . 10
7 Класс FAU. Аудит безопасности . . . 11
7.1 Автоматическая реакция аудита безопасности (FAU_ARP) . . . 11
7.2 Генерация данных аудита безопасности (FAU_GEN) . . . 12
7.3 Анализ аудита безопасности (FAU_SAA) . . . 13
7.4 Просмотр аудита безопасности (FAU_SAR) . . . 15
7.5 Выбор событий аудита безопасности (FAU_SEL) . . . 16
7.6 Хранение данных аудита безопасности (FAU_STG) . . . 17
8 Класс FCO. Связь . . . 18
8.1 Неотказуемость отправления (FCO_NRO) . . . 18
8.2 Неотказуемость получения (FCO_NRR) . . . 20
9 Класс FCS. Криптографическая поддержка . . . 21
9.1 Управление криптографическими ключами (FCS_CKM) . . . 21
9.2 Криптографические операции (FCS_COP) . . . 23
10 Класс FDP. Защита данных пользователя . . . 23
10.1 Политика управления доступом (FDP_ACC) . . . 25
10.2 Функции управления доступом (FDP_ACF) . . . 26
10.3 Аутентификация данных (FDP_DAU) . . . 27
10.4 Экспорт данных за пределы действия ФБО (FDP_ETC) . . . 28
10.5 Политика управления информационными потоками (FDP_IFC) . . . 29
10.6 Функции управления информационными потоками (FDP_IFF) . . . 30
10.7 Импорт данных из-за пределов действия ФБО (FDP_ITC) . . . 33
10.8 Передача в пределах ОО (FDP_ITT) . . . 35
10.9 Защита остаточной информации (FDP_RIP) . . . 36
10.10 Откат (FDP_ROL) . . . 37
10.11 Целостность хранимых данных (FDP_SDI . . . 38
10.12 Защита конфиденциальности данных пользователя при передаче между ФБО (FDP_UCT) . . . 39
10.13 Защита целостности данных пользователя при передаче между ФБО (FDP_UIT) . . . 40
11 Класс FIA. Идентификация и аутентификация . . . 41
11.1 Отказы аутентификации (FIA_AFL) . . . 42
11.2 Определение атрибутов пользователя (FIA_ATD) . . . 43
11.3 Спецификация секретов (FIA_SOS) . . . 43
11.4 Аутентификация пользователя (FIA_UAU) . . . 44
11.5 Идентификация пользователя (FIA_UID) . . . 47
11.6 Связывание пользователь-субъект (FIA_USB) . . . 48
12 Класс FMT. Управление безопасностью . . . 48
12.1 Управление отдельными функциями ФБО (FMT_MOF) . . . 49
12.2 Управление атрибутами безопасности (FMT_MSA) . . . 50
12.3 Управление данными ФБО (FMT_MTD) . . . 51
12.4 Отмена (FMT_REV) . . . 52
12.5 Срок действия атрибута безопасности (FMT_SAE) . . . 53
12.6 Спецификация функций управления (FMT_SMF) . . . 54
12.7 Роли управления безопасностью (FMT_SMR) . . . 54
13 Класс FPR. Приватность . . . 56
13.1 Анонимность (FPR_ANO) . . . 56
13.2 Псевдонимность (FPR_PSE) . . . 57
13.3 Невозможность ассоциации (FPR_UNL) . . . 58

14 Класс FPT. Защита ФБО . . . 60
14.1 Тестирование базовой абстрактной машины (FPT_AMT) . . . 62
14.2 Безопасность при сбое (FPT_FLS) . . . 62
14.3 Доступность экспортируемых данных ФБО (FPT_ITA) . . . 63
14.4 Конфиденциальность экспортируемых данных ФБО (FPT_ITC) . . . 63
14.5 Целостность экспортируемых данных ФБО (FPT_ITI) . . . 64
14.6 Передача данных ФБО в пределах ОО (FPT_ITT) . . . 65
14.7 Физическая защита ФБО (FPT_PHP) . . . 66
14.8 Надежное восстановление (FPT_RCV) . . . 68
14.9 Обнаружение повторного использования (FPT_RPL) . . . 69
14.10 Посредничество при обращениях (FPT_RVM) . . . 70
14.11 Разделение домена (FPT_SEP) . . . 71
14.12 Протокол синхронизации состояний (FPT_SSP) . . . 72
14.13 Метки времени (FPT_STM) . . . 73
14.14 Согласованность данных ФБО между ФБО (FPT_TDC) . . . 73
14.15 Согласованность данных ФБО при дублировании в пределах ОО (FPT_TRC) . . . 74
14.16 Самотестирование ФБО (FPT_TST) . . . 74
15 Класс FRU. Использование ресурсов . . . 75
15.1 Отказоустойчивость (FRU_FLT) . . . 76
15.2 Приоритет обслуживания (FRU_PRS) . . . 76
15.3 Распределение ресурсов (FRU_RSA) . . . 77
16 Класс FTA. Доступ к ОО . . . 78
16.1 Ограничение области выбираемых атрибутов (FTA_LSA) . . . 79
16.2 Ограничение на параллельные сеансы (FTA_MCS) . . . 79
16.3 Блокирование сеанса (FTA_SSL) . . . 80
16.4 Предупреждения перед предоставлением доступа к ОО (FTA_TAB) . . . 81
16.5 История доступа к ОО (FTA_TAH) . . . 82
16.6 Открытие сеанса с ОО (FTA_TSE) . . . 82
17 Класс FTP. Доверенный маршрут/канал . . . 83
17.1 Доверенный канал передачи между ФБО (FTP_ITC) . . . 83
17.2 Доверенный маршрут (FTP_TRP) . . . 84
Приложение А (обязательное) Замечания по применению функциональных требований безопасности . . . 86
А.1 Структура замечаний . . . 86
А.2 Таблицы зависимостей . . . 87
Приложение В (обязательное) Функциональные классы, семейства и компоненты . . . 92
Приложение С (обязательное) Аудит безопасности (FAU) . . . 93
С.1 Требования аудита в распределенной среде . . . 93
С.2 Автоматическая реакция аудита безопасности (FAU_ARP) . . . 93
С.3 Генерация данных аудита безопасности (FAU_GEN) . . . 93
С.4 Анализ аудита безопасности (FAU_SAA) . . . 96
С.5 Просмотр аудита безопасности (FAU_SAR) . . . 98
С.6 Выбор событий аудита безопасности (FAU_SEL) . . . 99
С.7 Хранение данных аудита безопасности (FAU_STG) . . . 100
Приложение D (обязательное) Связь (FCO) . . . 102
D.1 Неотказуемость отправления (FCO_NRO) . . . 102
D.2 Неотказуемость получения (FCO_NRR) . . . 103
Приложение Е (обязательное) Криптографическая поддержка (FCS) . . . 105
Е.1 Управление криптографическими ключами (FCS_CKM) . . . 105
Е.2 Криптографические операции (FCS_COP) . . . 107
Приложение F (обязательное) Защита данных пользователя (FDP) . . . 108
F.1 Политика управления доступом (FDP_ACC) . . . 109
F.2 Функции управления доступом (FDP_ACF) . . . 111
F.3 Аутентификация данных (FDP_DAU) . . . 113
F.4 Экспорт данных за пределы действия ФБО (FDP_ETC) . . . 113
F.5 Политика управления информационными потоками (FDP_IFC) . . . 114
F.6 Функции управления информационными потоками (FDP_IFF) . . . 115
F.7 Импорт данных из-за пределов действия ФБО (FDP_ITC) . . . 118
F.8 Передача в пределах ОО (FDP_ITT) . . . 120

F.9 Защита остаточной информации (FDP_RIP) . . . 121
F.10 Откат (FDP_ROL) . . . 122
F.11 Целостность хранимых данных (FDP_SDI) . . . 123
F.12 Защита конфиденциальности данных пользователя при передаче между ФБО (FDP_UCT) . . . 124
F.13 Защита целостности данных пользователя при передаче между ФБО (FDP_UIT) . . . 124
Приложение G (обязательное) Идентификация и аутентификация (FIA) . . . 126
G.1 Отказы аутентификации (FIA_AFL) . . . 127
G.2 Определение атрибутов пользователя (FIA_ATD) . . . 127
G.3 Спецификация секретов (FIA_SOS) . . . 128
G.4 Аутентификация пользователя (FIA_UAU) . . . 129
G.5 Идентификация пользователя (FIA_UID) . . . 130
G.6 Связывание пользователь-субъект (FIA_USB) . . . 131
Приложение H (обязательное) Управление безопасностью (FMT) . . . 132
H.1 Управление отдельными функциями ФБО (FMT_MOF) . . . 133
H.2 Управление атрибутами безопасности (FMT_MSA) . . . 133
H.3 Управление данными ФБО (FMT_MTD) . . . 134
H.4 Отмена (FMT_REV) . . . 135
H.5 Срок действия атрибутов безопасности (FMT_SAE) . . . 136
H.6 Спецификация функций управления (FMT_SMF) . . . 136
H.7 Роли управления безопасностью (FMT_SMR) . . . 136
Приложение I (обязательное) Приватность (FPR) . . . 138
I.1 Анонимность (FPR_ANO) . . . 138
I.2 Псевдонимность (FPR_PSE) . . . 140
I.3 Невозможность ассоциации (FPR_UNL) . . . 142
I.4 Скрытность (FPR_UNO) . . . 143
Приложение J (обязательное) Защита ФБО (FPT) . . . 146
J.1 Тестирование базовой абстрактной машины (FPT_AMT) . . . 146
J.2 Безопасность при сбое (FPT_FLS) . . . 148
J.3 Доступность экспортируемых данных ФБО (FPT_ITA) . . . 149
J.4 Конфиденциальность экспортируемых данных ФБО (FPT_ITC) . . . 149
J.5 Целостность экспортируемых данных ФБО (FPT_ITI) . . . 149
J.6 Передача данных ФБО в пределах ОО (FPT_ITT) . . . 150
J.7 Физическая защита ФБО (FPT_PHP) . . . 151
J.8 Надежное восстановление (FPT_RCV) . . . 152
J.9 Обнаружение повторного использования (FPT_RPL) . . . 154
J.10 Посредничество при обращениях (FPT_RVM) . . . 154
J.11 Разделение домена (FPT_SEP) . . . 155
J.12 Протокол синхронизации состояний (FPT_SSP) . . . 156
J.13 Метки времени (FPT_STM) . . . 157
J.14 Согласованность данных ФБО между ФБО (FPT_TDC) . . . 157
J.15 Согласованность данных ФБО при дублировании в пределах ОО (FPT_TRC) . . . 157
J.16 Самотестирование ФБО (FPT_TST) . . . 158
Приложение K (обязательное) Использование ресурсов (FRU) . . . 159
K.1 Отказоустойчивость (FRU_FLT) . . . 159
K.2 Приоритет обслуживания (FRU_PRS) . . . 160
K.3 Распределение ресурсов (FRU_RSA) . . . 160
Приложение L (обязательное) Доступ к ОО (FTA) . . . 162
L.1 Ограничение области выбираемых атрибутов (FTA_LSA) . . . 162
L.2 Ограничение на параллельные сеансы (FTA_MCS) . . . 163
L.3 Блокирование сеанса (FTA_SSL) . . . 163
L.4 Предупреждения перед предоставлением доступа к ОО (FTA_TAB) . . . 164
L.5 История доступа к ОО (FTA_TAH) . . . 164
L.6 Открытие сеанса с ОО (FTA_TSE) . . . 165
Приложение M (обязательное) Доверенный маршрут/канал (FTP) . . . 166
M.1 Доверенный канал передачи между ФБО (FTP_ITC) . . . 166
M.2 Доверенный маршрут (FTP_TRP) . . . 166
Приложение N (справочное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам . . . 167

Введение

Международный стандарт ИСО/МЭК 15408:2005 подготовлен Совместным техническим комитетом ИСО/МЭК СТК 1 «Информационные технологии», Подкомитет ПК 27 «Методы и средства обеспечения безопасности ИТ». Идентичный ИСО/МЭК 15408:2005 текст опубликован организациями—спонсорами проекта «Общие критерии» как «Общие критерии оценки безопасности информационных технологий», версия 2.3 (ОК, версия 2.3).

Второе издание ИСО/МЭК 15408:2005 отменяет и заменяет первое издание (ИСО/МЭК 15408:1999), которое подверглось технической переработке.

ИСО/МЭК 15408 под общим наименованием «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» состоит из следующих частей:

- часть 1. Введение и общая модель;
- часть 2. Функциональные требования безопасности;
- часть 3. Требования доверия к безопасности.

Если имеют в виду все три части стандарта, используют обозначение ИСО/МЭК 15408.

Функциональные компоненты безопасности, определенные в данной части ИСО/МЭК 15408, являются основой для выражения функциональных требований безопасности в профиле защиты (ПЗ) или задании по безопасности (ЗБ). Данные требования содержат описание желательного безопасного режима функционирования объекта оценки (ОО) или ИТ-среды ОО и предназначены для достижения целей безопасности, установленных в ПЗ или ЗБ. Данные требования содержат свойства безопасности, которые пользователи могут обнаружить при непосредственном взаимодействии с ИТ (то есть при входе и выходе) или при реакции ИТ на запросы.

Функциональные компоненты безопасности выражают требования безопасности, направленные на противостояние угрозам в предполагаемой среде эксплуатации ОО и/или охватывающие любую идентифицированную политику безопасности организации и предположения.

Аудитория для данной части ИСО/МЭК 15408 включает в себя потребителей, разработчиков и оценщиков безопасных ИТ-систем и продуктов. Дополнительная информация о потенциальных пользователях ИСО/МЭК 15408 и использовании ИСО/МЭК 15408 группами, которые включают в себя потенциальных пользователей, представлена в ИСО/МЭК 15408-1, раздел 4. Эти группы могут использовать данную часть ИСО/МЭК 15408 следующим образом:

a) потребители используют данную часть ИСО/МЭК 15408, выбирая компоненты, чтобы сформулировать функциональные требования для удовлетворения целей безопасности, приведенных в ПЗ или ЗБ. Более подробная информация о взаимосвязях требований безопасности и целей безопасности приведена в ИСО/МЭК 15408-1, подраздел 5.3;

b) разработчики, несущие ответственность за выполнение существующих или предполагаемых требований безопасности потребителя при разработке ОО, найдут в данной части ИСО/МЭК 15408 стандартизированный подход к пониманию указанных требований. Они используют содержание данной части ИСО/МЭК 15408 как основу для дальнейшего определения функций и механизмов безопасности ОО, которые соответствовали бы этим требованиям;

c) оценщики используют функциональные требования, определенные в данной части ИСО/МЭК 15408, для подтверждения того, что функциональные требования ОО, приведенные в ПЗ или ЗБ, соответствуют целям безопасности ИТ, а также для учета зависимостей данных требований и показа удовлетворения этих зависимостей. Оценщикам также следует использовать данную часть ИСО/МЭК 15408 при определении того, соответствует ли конкретный ОО предъявленным требованиям.

Федеральное агентство по техническому регулированию и метрологии

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 2

Функциональные требования безопасности

Information technology. Security techniques. Evaluation criteria for IT security.
Part 2. Security functional requirements

Дата введения — 2009—10—01

1 Область применения

Настоящий стандарт устанавливает структуру и содержание компонентов функциональных требований безопасности для оценки безопасности. Он также включает в себя каталог функциональных компонентов, отвечающих общим требованиям к функциональным возможностям безопасности многих продуктов и систем ИТ.

2 Нормативные ссылки

В настоящем стандарте использована ссылка на следующий международный стандарт:

ИСО/МЭК 15408-1:2005 Информационная технология — Методы и средства обеспечения безопасности — Критерии оценки безопасности информационных технологий — Часть 1: Введение и общая модель

3 Термины, определения, обозначения и сокращения

В настоящем стандарте применены термины, обозначения и сокращения по ИСО/МЭК 15408-1.

4 Краткий обзор

ИСО/МЭК 15408 и соответствующие функциональные требования безопасности, описанные ниже, не предназначены для окончательного решения всех задач безопасности ИТ. Скорее настоящий стандарт предлагает совокупность хорошо продуманных функциональных требований безопасности, которые могут применяться при создании доверенных продуктов или систем ИТ, отвечающих потребностям рынка. Эти функциональные требования безопасности представляют современный уровень спецификации требований и оценки.

В настоящий стандарт предполагалось включать только те функциональные требования безопасности, которые на момент издания стандарта были известны и одобрены его разработчиками.

Так как знания и потребности пользователей могут меняться, функциональные требования, представленные в настоящем стандарте, нуждаются в дальнейшем сопровождении. Предполагается, что некоторые разработчики ПЗ/ЗБ могут иметь потребности в безопасности, не охваченные компонентами функциональных требований, представленными в настоящем стандарте. В данном случае разработчик ПЗ/ЗБ может предпочесть использование нестандартных функциональных требований (так называемую «расширяемость») в соответствии с ИСО/МЭК 15408-1, приложения А и В.

4.1 Структура данной части ИСО/МЭК 15408

В разделе 5 приведено описание парадигмы, используемой в функциональных требованиях безопасности настоящего стандарта.

Издание официальное

Раздел 6 представляет собой каталог функциональных компонентов.

В разделах 7 — 17 приведено описание функциональных классов.

Приложение А содержит информацию для потенциальных пользователей функциональных компонентов, включая таблицы перекрестных ссылок зависимостей функциональных компонентов.

Приложения В — М содержат информацию для функциональных классов. Этот материал должен рассматриваться в качестве нормативных инструкций по применению соответствующих операций и выбору необходимой информации для аудита и документирования; использование глагола «следует» означает, что конкретная инструкция является предпочтительной, но и другие могут быть обоснованы. В случае, если приводят различные варианты, выбор остается за автором ПЗ/ЗБ.

ИСО/МЭК 15408-1 содержит следующую информацию, необходимую разработчикам ПЗ или ЗБ:

ИСО/МЭК 15408-1, раздел 2, определяет термины, используемые в ИСО/МЭК 15408;

ИСО/МЭК 15408-1, приложение А, определяет структуру профилей защиты;

ИСО/МЭК 15408-1, приложение В, определяет структуру заданий по безопасности;

библиография необходимых документов приведена в элементе «Библиография» ИСО/МЭК 15408-1.

5 Парадигма функциональных требований

В данном разделе приведена парадигма функциональных требований безопасности настоящего стандарта. Некоторые ключевые понятия парадигмы показаны на рисунках 1 и 2. Описаны и другие, не показанные на рисунках 1 и 2, ключевые понятия. Рассматриваемые ключевые понятия выделены полужирным курсивом. Определения терминов, приведенные в ИСО/МЭК 15408-1, раздел 2, в данном разделе не изменяются и не заменяются.

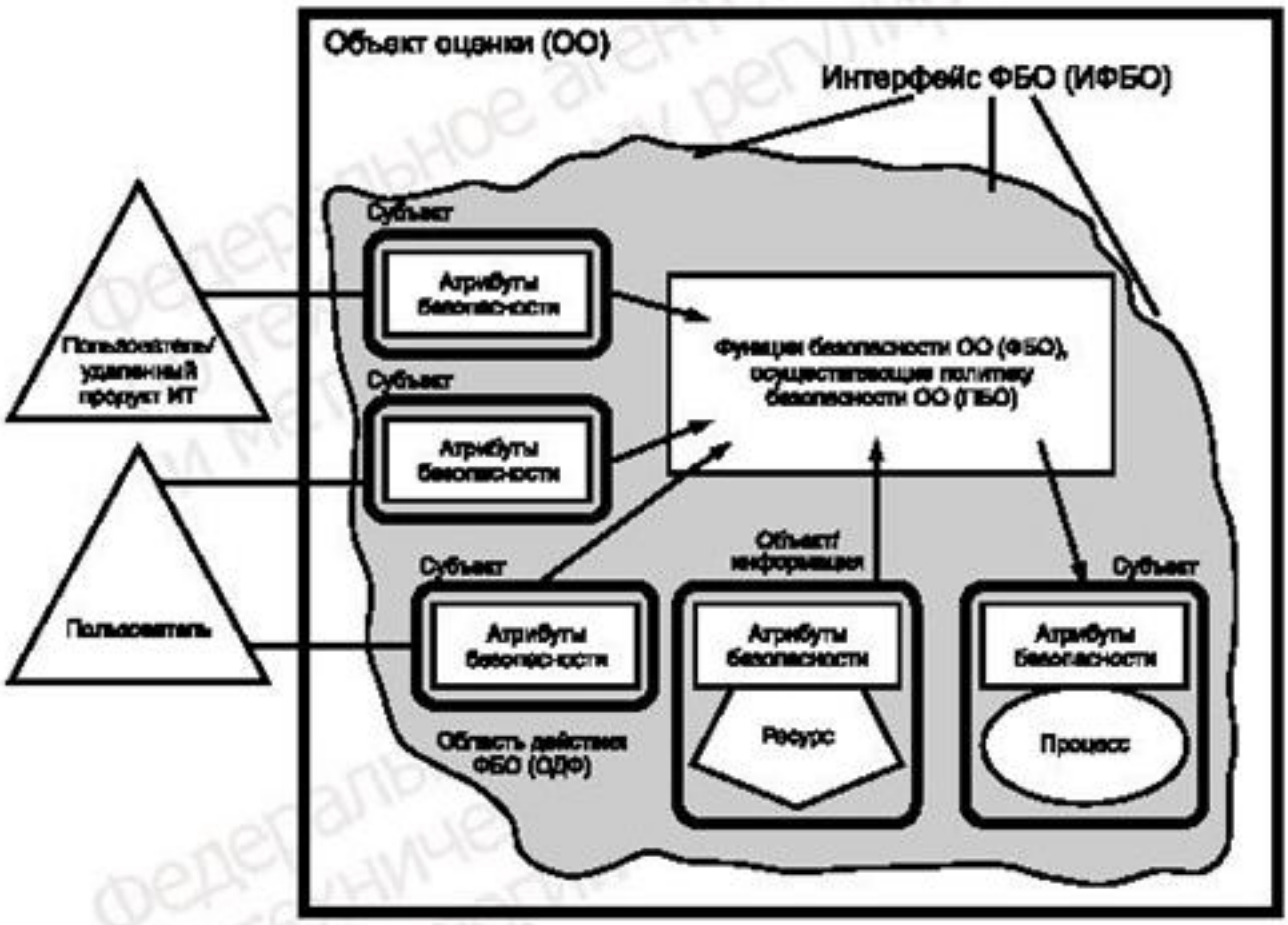

Рисунок 1 — Ключевые понятия функциональных требований безопасности (единый ОО)

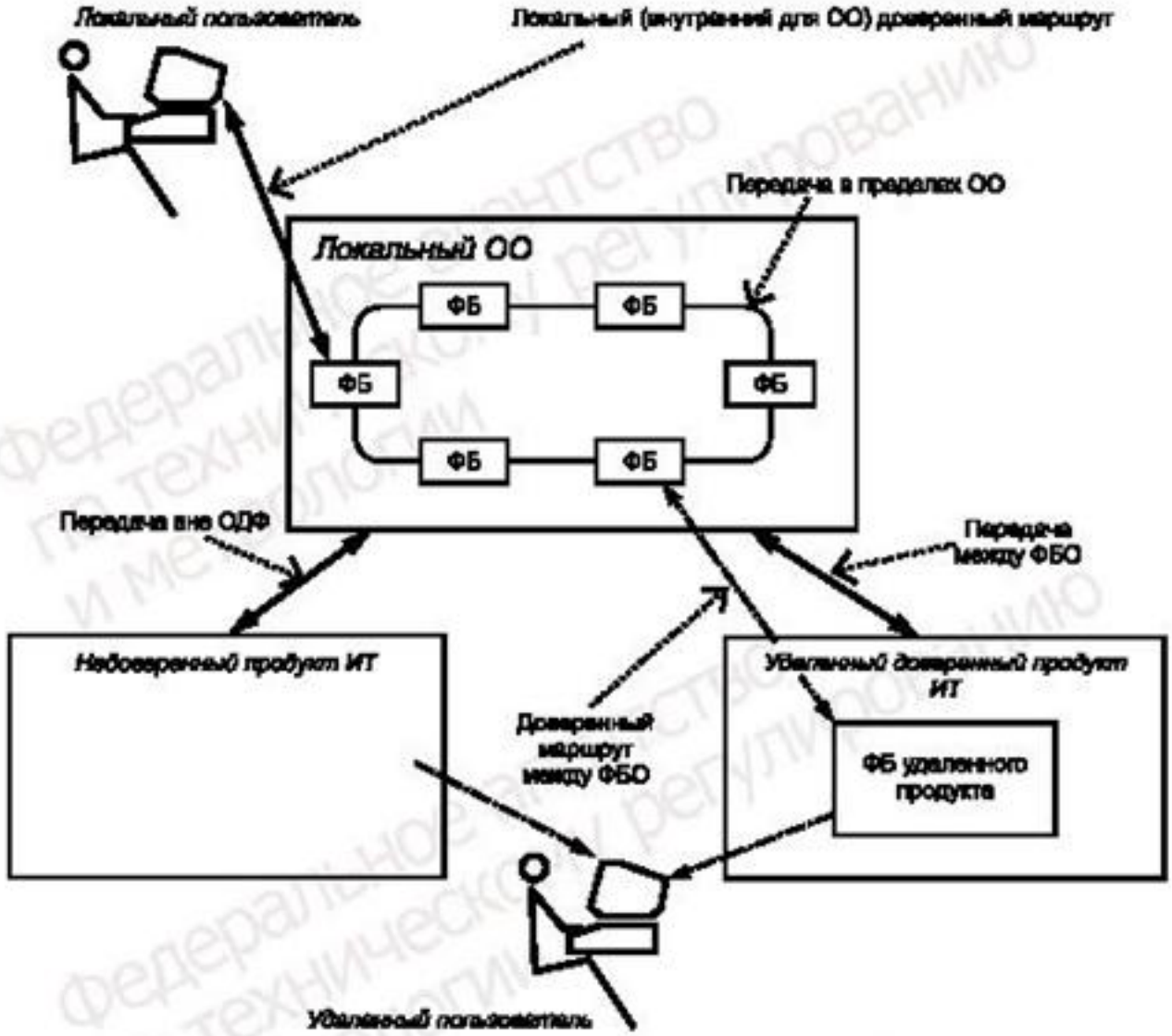

Рисунок 2 — Функции безопасности в распределенном ОО

Настоящий стандарт содержит каталог функциональных требований безопасности, которые могут быть предъявлены к ***объекту оценки (ОО)***. ОО — это продукт или система ИТ (вместе с руководствами администратора и пользователя), содержащие ресурсы типа электронных носителей данных (таких, как диски), периферийных устройств (таких, как принтеры) и вычислительных возможностей (таких, как процессорное время), которые могут использоваться для обработки и хранения информации и являются предметом оценки.

Оценка прежде всего подтверждает, что в отношении ресурсов ОО осуществляется определенная ***политика безопасности ОО (ПБО)***. ПБО определяет правила, по которым ОО управляет доступом к своим ресурсам и, таким образом, ко всей информации и сервисам, контролируемым ОО.

ПБО в свою очередь состоит из различных ***политик функций безопасности (ПФБ)***. Каждая ПФБ имеет свою область действия, определяющую субъекты, объекты и операции, на которые распространяется ПФБ. ПФБ реализуется ***функцией безопасности (ФБ)***, чьи механизмы осуществляют политику и предоставляют необходимые возможности.

Совокупность всех функций безопасности ОО, которые направлены на осуществление ПБО, определяется как ***функции безопасности объекта оценки (ФБО)***. ФБО объединяют функциональные возможности всех аппаратных, программных и программно-аппаратных средств ОО, на которые как непосредственно, так и косвенно возложено обеспечение безопасности.

Монитор обращений — это концепция абстрактной машины, которая осуществляет политику управления доступом ОО. ***Механизм проверки правомочности обращений*** — реализация концепции монитора обращений, обладающая следующими свойствами: защищенностью от проникновения, постоянной готовностью, простотой, достаточной для проведения исчерпывающего анализа и тестирования. ФБО могут состоять из механизма проверки правомочности обращений и/или других функций безопасности, необходимых для эксплуатации ОО.

ОО может быть единым продуктом, включающим в себя аппаратные, программно-аппаратные и программные средства.

В ином случае ОО может быть распределенным, состоящим из нескольких разделенных частей. Каждая часть ОО обеспечивает выполнение конкретного сервиса для ОО и взаимодействуют с другими частями ОО через ***внутренний канал связи***. Этот канал может быть всего лишь шиной процессора, а может являться внутренней сетью для ОО.

Если ОО состоит из нескольких частей, то каждая часть может иметь собственное подмножество ФБО, которое обменивается данными ФБО и пользователей через внутренние каналы связи с другими подмножествами ФБО. Это взаимодействие называется ***внутренней передачей ОО***. В этом случае части ФБО формируют объединенные ФБО, которые осуществляют ПБО для этого ОО.

Интерфейсы ОО могут быть локализованы в конкретном ОО или допускать взаимодействие с другими продуктами ИТ по ***внешним каналам связи***. Внешние взаимодействия с другими продуктами ИТ могут принимать две формы:

a) политика безопасности «удаленного доверенного продукта ИТ» и ПБО рассматриваемого ОО скоординированы и оценены в административном порядке. Обмен информацией в этом случае назван ***передачей между ФБО***, поскольку он осуществляется между ФБО различных доверенных продуктов;

b) удаленный продукт ИТ, обозначенный на рисунке 2 как «недоверенный продукт ИТ», не был оценен, поэтому его политика безопасности неизвестна. Обмен информацией в этом случае назван ***передачей за пределы области действия ФБО***, так как этот удаленный продукт ИТ не имеет ФБО (или характеристики его политики безопасности неизвестны).

Совокупность взаимодействий, которые могут происходить с ОО или в пределах ОО и подчинены правилам ПБО, относится к ***области действия функций безопасности (ОДФ)***. ОДФ включает в себя определенную совокупность взаимодействий в пределах ОО с использованием понятий «субъекты», «объекты» и «операции», но не обязательно охватывает все ресурсы ОО.

Совокупность интерфейсов как интерактивных (человеко-машинный интерфейс), так и программных (интерфейс программных приложений), через которые могут быть получены доступ к ресурсам при посредничестве ФБО или информация от ФБО, называется ***интерфейсом ФБО (ИФБО)***. ИФБО определяет границы возможностей функций ОО, которые предоставлены для осуществления ПБО.

Пользователей не включают в состав ОО, поэтому они находятся вне ОДФ. Однако пользователи взаимодействуют с ОО через ИФБО при запросе услуг, которые будут выполняться ОО. Существует два типа пользователей, учитываемых в функциональных требованиях безопасности настоящего стандарта: ***человек-пользователь*** и ***внешняя сущность ИТ***. Для человека-пользователя различают ***локального человека-пользователя***, взаимодействующего непосредственно с ОО через устройства ОО (такие, как рабочие станции), и ***удаленного человека-пользователя***, взаимодействующего с ОО через другой продукт ИТ.

Период взаимодействия между пользователем и ФБО называется ***сеансом пользователя***. Открытие сеансов пользователей может контролироваться на основе ряда условий, таких как аутентификация пользователя, время суток, метод доступа к ОО, число параллельных сеансов, разрешенных пользователю, и т. д.

В настоящем стандарте используется термин ***уполномоченный*** для обозначения пользователя, который обладает правами и/или привилегиями, необходимыми для выполнения операций. Поэтому термин ***уполномоченный пользователь*** указывает на то, что пользователю разрешается выполнять данную операцию в соответствии с ПБО.

Для выражения требований разделения административных обязанностей соответствующие функциональные компоненты безопасности (из семейства FMT_SMR), приведенные в настоящем стандарте, явно устанавливают обязательность административных ***ролей***. Роль — это заранее определенная совокупность правил, устанавливающих допустимые взаимодействия между пользователем и ОО. ОО может поддерживать определение произвольного числа ролей. Например, роли, связанные с операциями безопасности ОО, могут включать в себя роли «Администратор аудита» и «Администратор учета пользователей».

ОО содержит ресурсы, которые могут использоваться для обработки и хранения информации. Основной целью ФБО является полное и правильное осуществление ПБО для ресурсов и информации, которыми управляет ОО.

Ресурсы ОО могут иметь различную структуру и использоваться различными способами. Тем не менее, в настоящем стандарте проводится специальное разграничение, позволяющее специфицировать желательные свойства безопасности. Все сущности, которые могут быть созданы на основе ресурсов, характеризуются одним из двух способов. Сущности могут быть активными, то есть являться причиной действий, которые происходят в пределах ОО, и инициировать операции, выполняемые с информацией. Напротив, сущности могут быть пассивными, то есть являться источником или местом хранения информации.

Активные сущности названы ***субъектами***. В пределах ОО могут существовать несколько типов субъектов:

a) действующие от имени уполномоченного пользователя и подчиненные всем правилам ПБО (например процессы UNIX);

b) действующие как особый функциональный процесс, который может, в свою очередь, действовать от имени многих пользователей (например функции, которые характерны для архитектуры клиент/сервер);

c) действующие как часть собственно ОО (например доверенные процессы).

В настоящем стандарте рассматривается осуществление ПБО для субъектов перечисленных выше типов.

Пассивные сущности (то есть хранилища информации) названы ***объектами*** в функциональных требованиях безопасности настоящего стандарта. Объекты являются предметом операций, которые могут выполняться субъектами. В случае, если субъект (активная сущность) сам является предметом операции (например, при установлении связи между процессами), над субъектом могут производиться действия, как над объектом.

Объекты могут содержать ***информацию***. Это понятие требуется, чтобы специфицировать политики управления информационными потоками в соответствии с классом FDP.

Пользователи, субъекты, информация и объекты обладают определенными ***атрибутами***, которые содержат информацию, позволяющую ОО правильно функционировать. Некоторые атрибуты, такие как имена файлов, могут предназначаться только для информирования, в то время как другие, например, различные параметры управления доступом, — исключительно для осуществления ПБО. Эти последние обобщенно названы «***атрибутами безопасности***». В дальнейшем слово «атрибут» используется в настоящем стандарте как сокращение для словосочетания «атрибут безопасности» (если не оговорено иное). Вместе с тем, независимо от предназначения информации атрибута, могут потребоваться средства управления этим атрибутом в соответствии с ПБО.

В ОО содержатся данные пользователей и данные ФБО. Их взаимосвязь показана на рисунке 3. ***Данные пользователей*** — это информация, содержащаяся в ресурсах ОО, которая может применяться пользователями в соответствии с ПБО и не предназначена специально для ФБО. Например, содержание сообщения электронной почты является данными пользователя. ***Данные ФБО*** — это информация, используемая ФБО при осуществлении ПБО. Допускается воздействие пользователей на данные ФБО, если это предусмотрено ПБО. Примерами данных ФБО являются атрибуты безопасности, аутентификационные данные, списки управления доступом.

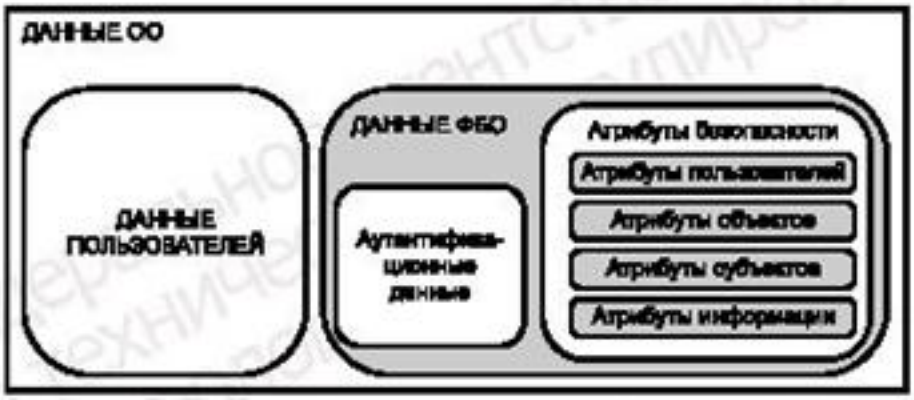

Рисунок 3 — Связь между данными пользователей и данными ФБО

Выделяются ПФБ, которые применяются при защите данных, такие как ***ПФБ управления доступом*** и ***ПФБ управления информационными потоками***. Действия механизмов, реализующих ПФБ управления доступом, основаны на атрибутах субъектов, объектов и операций в пределах области действия. Эти атрибуты используются в совокупности правил, управляющих операциями, которые субъектам разрешено выполнять на объектах.

Функционирование механизмов, реализующих ПФБ управления информационными потоками, основано на атрибутах субъектов и информации в пределах области действия и совокупности правил, по которым выполняются операции субъектов с информацией. Атрибуты информации, которые могут быть ассоциированы с атрибутами места хранения (или не ассоциированы с ними, например, в случае многоуровневой базы данных), остаются с информацией при ее перемещении.

Два специфических типа данных ФБО, рассматриваемых в настоящем стандарте, могут (но необязательно) совпадать. Это ***аутентификационные данные*** и ***секреты***.

Аутентификационные данные используют, чтобы верифицировать заявленный идентификатор пользователя, обращающегося к ОО за услугами. Самая распространенная форма аутентификационных данных — пароль, который необходимо хранить в секрете, чтобы механизм безопасности был эффективен. Однако в секрете необходимо хранить не все формы аутентификационных данных. Биометрические опознавательные устройства (например считыватели отпечатка пальца или сканеры сетчатки глаза) основываются не на предположении, что аутентификационные данные хранятся в секрете, а на том, что эти данные являются неотъемлемым свойством пользователя, которое невозможно подделать.

Термин «секрет», используемый в функциональных требованиях настоящего стандарта по отношению к аутентификационным данным, применим и к данным других типов, которые необходимо хранить в тайне при осуществлении определенной ПФБ. Например, стойкость механизма доверенного канала, в котором применена криптография для сохранения конфиденциальности передаваемой через канал информации, зависит от надежности способа сохранения в секрете криптографических ключей от несанкционированного раскрытия.

Следовательно, некоторые (но не все) аутентификационные данные необходимо хранить в секрете, и некоторые (но не все) секреты используют как аутентификационные данные. Взаимосвязь секретов и аутентификационных данных представлена на рисунке 4. На рисунке 4 указаны типы данных, которые часто относят к аутентификационным данным и секретам.

Рисунок 4 — Связь между понятиями «аутентификационные данные» и «секреты»

6 Функциональные компоненты безопасности

6.1 Краткий обзор

Данный раздел определяет содержание и форму представления функциональных требований настоящего стандарта и предоставляет руководство по организации требований для новых компонентов, включаемых в ЗБ. Функциональные требования объединены в классы, семейства и компоненты.

6.1.1 Структура класса

Структура функционального класса приведена на рисунке 5. Каждый функциональный класс содержит имя класса, представление класса и одно или несколько функциональных семейств.

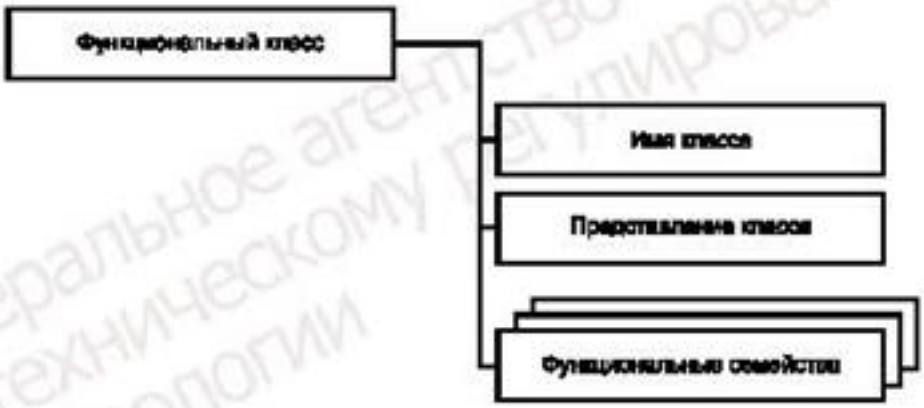

Рисунок 5 — Структура функционального класса

6.1.1.1 Имя класса

Имя класса содержит информацию, необходимую для идентификации функционального класса и отнесения его к определенной категории. Каждый функциональный класс имеет уникальное имя. Информация о категории предоставлена кратким именем, состоящим из трех букв латинского алфавита. Краткое имя класса используют при задании кратких имен семейств этого класса.

6.1.1.2 Представление класса

Представление класса обобщает участие семейств класса в достижении целей безопасности. Определение функциональных классов не отражает формальную таксономию в спецификации требований.

Представление класса содержит рисунок, показывающий все семейства этого класса и иерархию компонентов в каждом семействе, как указано в 6.2.

6.1.2 Структура семейства

Структура функционального семейства приведена на рисунке 6.

Рисунок 6 — Структура функционального семейства

6.1.2.1 Имя семейства

Имя семейства содержит описательную информацию, необходимую для идентификации и категорирования функционального семейства. Каждое функциональное семейство имеет уникальное имя. Информация о категории состоит из краткого имени, включающего в себя семь символов. Первые три символа идентичны краткому имени класса, далее следуют символ подчеркивания и краткое имя семейства в виде XXX_YYY. Уникальная краткая форма имени семейства предоставляет основное имя ссылки для компонентов.

6.1.2.2 Характеристика семейства

Характеристика семейства — это описание функционального семейства, в котором излагаются его цели безопасности и общее описание функциональных требований. Более детально они описаны ниже:

a) цели безопасности семейства характеризуют задачу безопасности, которая может быть решена с помощью компонентов этого семейства;

b) описание функциональных требований обобщает все требования, которые включены в компонент(ты). Описание ориентировано на разработчиков ПЗ, ЗБ и функциональных пакетов, которые хотели бы определить, соответствует ли семейство их конкретным требованиям.

6.1.2.3 Ранжирование компонентов

Функциональные семейства содержат один или несколько компонентов, каждый из которых может быть выбран для включения в ПЗ, ЗБ и функциональные пакеты. Цель ранжирования компонентов — предоставить пользователям информацию для выбора подходящего функционального компонента, если семейство идентифицировано пользователем как необходимая или полезная часть требований безопасности.

Далее перечисляются имеющиеся компоненты и приводится их обоснование. Детализация компонентов производится в описании каждого компонента.

Связи между компонентами в пределах функционального семейства могут быть иерархическими и неиерархическими. Компонент иерархичен (то есть расположен выше по иерархии) по отношению к другому компоненту, если предлагает большую безопасность.

Описания семейств содержат графическое представление иерархии компонентов, рассмотренное в 6.2.

6.1.2.4 Управление

Требования управления содержат информацию для разработчиков ПЗ/ЗБ, учитываемую при определении действий по управлению для данного компонента. Требования управления детализированы в компонентах класса «Управление безопасностью» (FMT).

Разработчик ПЗ/ЗБ может выбрать указанные требования управления или включить новые, не указанные в настоящем стандарте. В последнем случае следует представить необходимую информацию.

6.1.2.5 Аудит

Требования аудита содержат события, потенциально подвергаемые аудиту, для их отбора разработчиками ПЗ/ЗБ при условии включения в ПЗ/ЗБ требований из класса FAU «Аудит безопасности». Эти требования включают в себя события, относящиеся к безопасности, применительно к различным уровням детализации, поддерживаемым компонентами семейства FAU_GEN «Генерация данных аудита безопасности». Например, запись аудита какого-либо механизма безопасности может включать в себя на разных уровнях детализации действия, которые раскрываются в следующих терминах:

- минимальный — успешное использование механизма безопасности;
- базовый — любое использование механизма безопасности, а также информация о текущих значениях атрибутов безопасности;
- детализированный — любые изменения конфигурации механизма безопасности, включая параметры конфигурации до и после изменения.

Следует учесть, что категорирование событий, потенциально подвергаемых аудиту, всегда иерархично. Например, если выбрана базовая генерация данных аудита, то все события, идентифицированные как потенциально подвергаемые аудиту и поэтому входящие как в «минимальную», так и в «базовую» запись, следует включить в ПЗ/ЗБ с помощью соответствующей операции назначения, за исключением случая, когда событие более высокого уровня имеет более высокий уровень детализации, чем событие более низкого уровня, и может просто заменить его. Если необходима детализированная генерация данных аудита, то все идентифицированные события, потенциально подвергаемые аудиту (для минимального, базового и детализированного уровней), следует включить в ПЗ/ЗБ.

Правила управления аудитом более подробно объяснены в классе FAU «Аудит безопасности».

6.1.3 Структура компонента

Структура функционального компонента показана на рисунке 7.

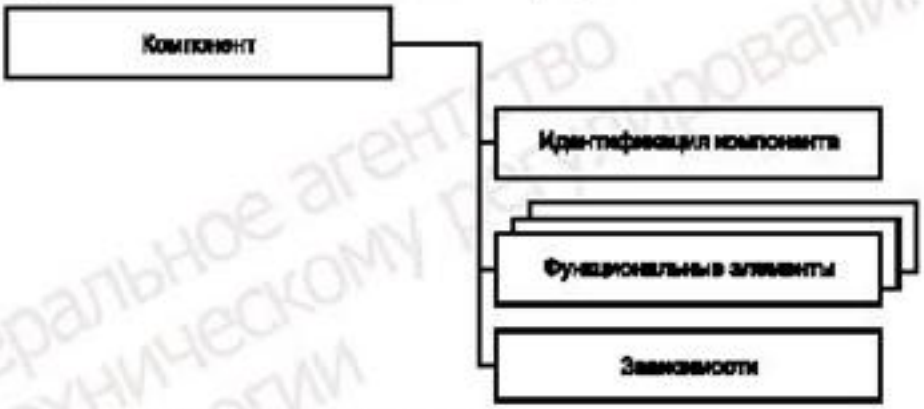

Рисунок 7 — Структура функционального компонента

6.1.3.1 Идентификация компонента

Идентификация компонента включает в себя описательную информацию, необходимую для идентификации, категорирования, записи и реализации перекрестных ссылок компонента. Для каждого функционального компонента представляются:

- *уникальное имя*, отражающее предназначение компонента;
- *краткое имя*, применяемое как основное имя ссылки для категорирования, записи и реализации перекрестных ссылок компонента и уникально отражающее класс и семейство, которым компонент принадлежит, а также номер компонента в семействе;
- *список иерархических связей*, содержащий имена других компонентов, для которых этот компонент иерархичен и вместо которых может использоваться при удовлетворении зависимостей от перечисленных компонентов.

6.1.3.2 Функциональные элементы

Каждый компонент включает в себя набор элементов. Каждый элемент определяется отдельно и является самодостаточным.

Функциональный элемент — это функциональное требование безопасности, дальнейшее разделение которого не меняет значимо результат оценки; является наименьшим функциональным требованием безопасности, идентифицируемым и признаваемым в ИСО/МЭК 15408.

При формировании ПЗ, ЗБ и/или пакетов не разрешается выбирать только часть элементов компонента. Для включения в ПЗ, ЗБ или пакет необходимо выбирать всю совокупность элементов компонента.

Вводится уникальная краткая форма имени функционального элемента. Например, имя FDP_IFF.4.2 читается следующим образом: F — функциональное требование, DP — класс «Защита данных пользователя», _IFF — семейство «Функции управления информационными потоками», .4 — четвертый компонент «Частичное устранение неразрешенных информационных потоков», .2 — второй элемент компонента.

6.1.3.3 Зависимости

Зависимости среди функциональных компонентов возникают, если компонент не самодостаточен и нуждается в функциональных возможностях другого компонента либо во взаимодействии с ним для поддержки собственного выполнения.

Каждый функциональный компонент содержит полный список зависимостей от других функциональных компонентов и компонентов доверия. Для некоторых компонентов указано, что зависимостей нет. Компоненты из списка могут, в свою очередь, иметь зависимости от других компонентов. Список, приведенный в компоненте, показывает прямые зависимости, то есть содержит ссылки только на функциональные компоненты, заведомо необходимые для обеспечения выполнения рассматриваемого компонента. Косвенные зависимости, определяемые собственными зависимостями компонентов из списка, показаны в приложении А. В некоторых случаях зависимость выбирают из нескольких предлагаемых функциональных компонентов, причем каждый из них достаточен для удовлетворения зависимости (см., например, FDP_UIT.1 «Целостность передаваемых данных»).

Список зависимостей идентифицирует минимум функциональных компонентов или компонентов доверия, необходимых для удовлетворения требований безопасности, ассоциированных с данным компонен-

том. Компоненты, которые иерархичны по отношению к компоненту из списка, также могут быть использованы для удовлетворения зависимости.

Зависимости между компонентами, указанные в настоящем стандарте, обязательны. Их необходимо удовлетворить в ПЗ/ЗБ. В некоторых, особых случаях эти зависимости удовлетворить невозможно. Разработчик ПЗ/ЗБ, обязательно обосновав, почему данная зависимость неприменима, может не включать соответствующий компонент в пакет, ПЗ или ЗБ.

6.2 Каталог компонентов

Расположение компонентов в настоящем стандарте не отражает какую-либо формальную таксономию.

Настоящий стандарт содержит классы, состоящие из семейств и компонентов, которые сгруппированы на основе общей функции и предназначения. Классы и семейства упорядочены в соответствии с латинским алфавитом. В начале каждого класса представлен рисунок, показывающий таксономию каждого класса, перечисляя семейства в каждом классе и компоненты в каждом семействе. На рисунке также представлена иерархия компонентов внутри каждого семейства.

В описании каждого функционального компонента приведены его зависимости от других компонентов.

Пример представления таксономии класса и иерархии компонентов в его семействах приведен на рисунке 8.

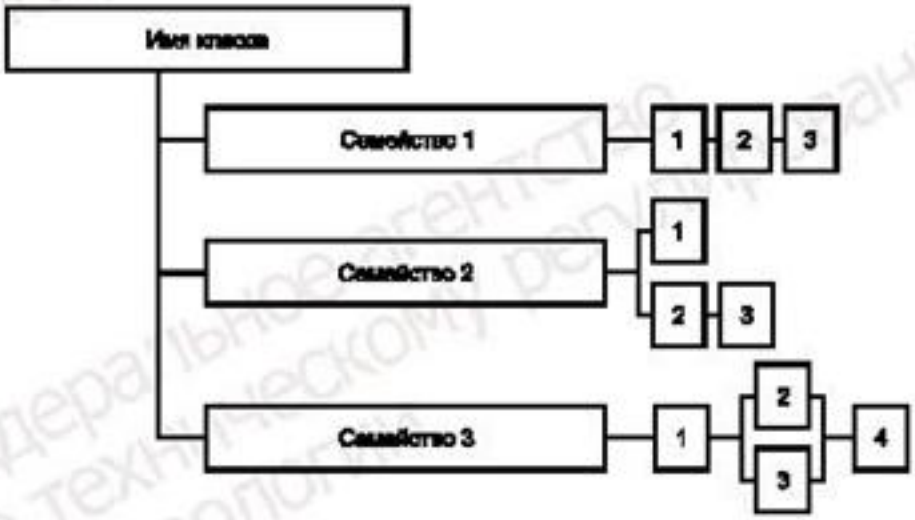

Рисунок 8 — Пример декомпозиции класса

В примере первое семейство содержит три иерархических компонента, где компоненты 2 и 3 могут быть применены для выполнения зависимостей вместо компонента 1. Компонент 3 иерархичен компоненту 2 и может применяться для выполнения зависимостей вместо компонента 2.

В семействе 2 имеются три компонента, не все из них иерархически связаны. Компоненты 1 и 2 не иерархичны другим компонентам. Компонент 3 иерархичен компоненту 2 и может применяться для удовлетворения зависимостей вместо компонента 2, но не вместо компонента 1.

В семействе 3 компоненты 2, 3 и 4 иерархичны компоненту 1. Компоненты 2 и 3 иерархичны компоненту 1, но несопоставимы по иерархии между собой. Компонент 4 иерархичен компонентам 2 и 3.

Такие рисунки дополняют текст описания семейств и упрощают идентификацию отношений их компонентов. Они не заменяют пункт «Иерархический для» в описании каждого компонента, который устанавливает обязательные утверждения иерархии для каждого компонента.

6.2.1 Выделение изменений в компоненте

Взаимосвязь компонентов в пределах семейства показана с использованием полужирного шрифта. Все новые требования в тексте компонентов выделены полужирным шрифтом. Для иерархически связанных компонентов требования выделены, если они расширены или модифицированы по сравнению с требованиями предыдущего компонента. Кроме того, любые новые или расширенные по сравнению с предыдущим компонентом разрешенные операции также выделены полужирным шрифтом.

7 Класс FAU. Аудит безопасности

Аудит безопасности включает в себя распознавание, запись, хранение и анализ информации, связанной с действиями, относящимися к безопасности (например, с действиями, контролируемыми ПБО). Записи аудита, получаемые в результате, могут быть проанализированы с тем, чтобы определить, какие действия, относящиеся к безопасности, происходили, и кто из пользователей за них отвечает.

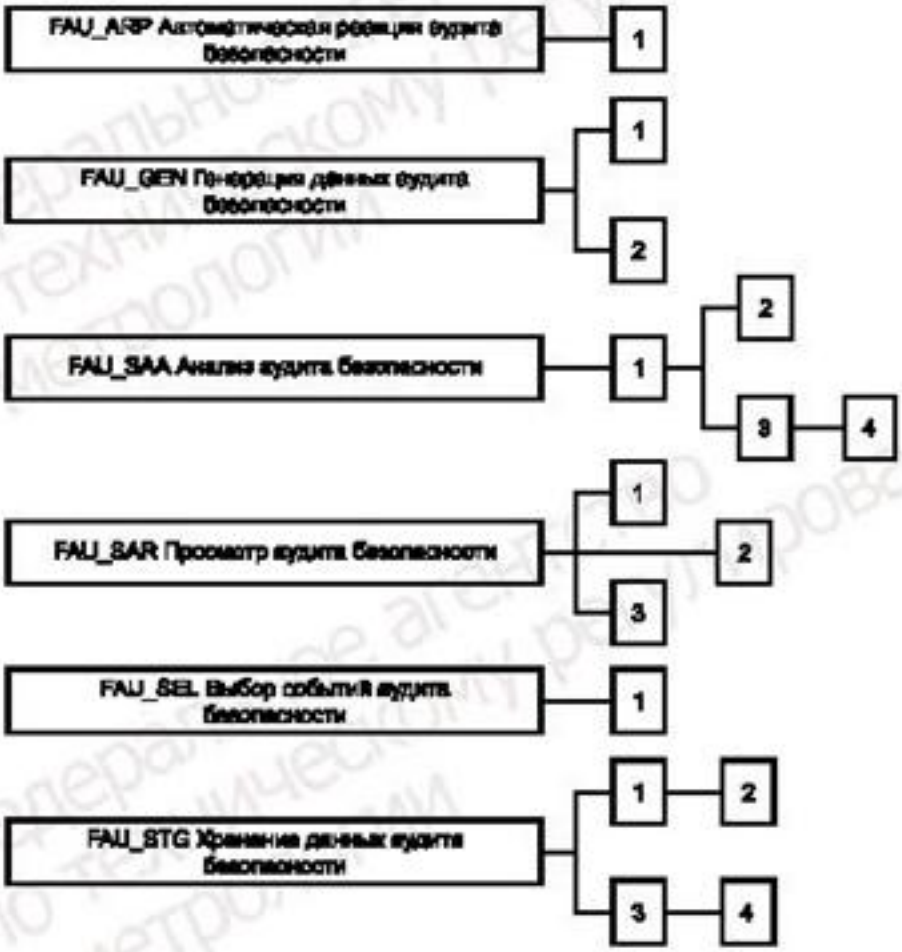

Рисунок 9 — Декомпозиция класса FAU «Аудит безопасности»

7.1 Автоматическая реакция аудита безопасности (FAU_ARP)

7.1.1 Характеристика семейства

Семейство FAU_ARP определяет реакцию на обнаружение событий, указывающих на возможное нарушение безопасности.

7.1.2 Ранжирование компонентов

Рисунок 10 — Ранжирование компонентов семейства FAU_ARP

В FAU_ARP.1 «Сигналы нарушения безопасности» ФБО должны предпринимать действия в случае обнаружения возможного нарушения безопасности.

7.1.3 Управление: FAU_ARP.1

Для функций управления из класса FMT могут рассматриваться следующие действия.

а) Управление действиями (добавление, удаление или модификация).

7.1.4 Аудит: FAU_ARP.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: действия, предпринимаемые в ответ на ожидаемые нарушения безопасности.

7.1.5 FAU_ARP.1 Сигналы нарушения безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_SAA.1 Анализ потенциального нарушения

7.1.5.1 FAU_ARP.1.1

ФБО должны предпринять [назначение: *список наименее разрушительных действий*] при обнаружении возможного нарушения безопасности.

7.2 Генерация данных аудита безопасности (FAU_GEN)

7.2.1 Характеристика семейства

Семейство FAU_GEN определяет требования к регистрации возникновения событий, относящихся к безопасности, которые подконтрольны ФБО. Данное семейство идентифицирует уровень аудита, перечисляет типы событий, которые потенциально должны подвергаться аудиту с использованием ФБО, и определяет минимальный объем связанной с аудитом информации, которую следует представлять в записях аудита различного типа.

7.2.2 Ранжирование компонентов

Рисунок 11 — Ранжирование компонентов семейства FAU_GEN

FAU_GEN.1 «Генерация данных аудита» определяет уровень событий, потенциально подвергаемых аудиту, и состав данных, которые должны быть зарегистрированы в каждой записи.

В FAU_GEN.2 «Ассоциация идентификатора пользователя» ФБО должны ассоциировать события, потенциально подвергаемые аудиту, и личные идентификаторы пользователей.

7.2.3 Управление: FAU_GEN.1, FAU_GEN.2

Действия по управлению не предусмотрены.

7.2.4 Аудит: FAU_GEN.1, FAU_GEN.2

Нет событий, для которых следует предусмотреть возможность аудита.

7.2.5 FAU_GEN.1 Генерация данных аудита

Иерархический для: нет подчиненных компонентов.

Зависимости: FPT_STM.1 Надежные метки времени

7.2.5.1 FAU_GEN.1.1

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

а) запуск и завершение выполнения функций аудита;

b) все события, потенциально подвергаемые аудиту, на [выбор (выбрать одно из): *минимальный, базовый, детализированный, неопределенный*] уровне аудита;

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

7.2.5.2 FAU_GEN.1.2

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

а) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);

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

7.2.6 FAU_GEN.2 Ассоциация идентификатора пользователя

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_GEN.1 Генерация данных аудита

FIA_UID.1 Выбор момента идентификации

7.2.6.1 FAU_GEN.2.1

ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.

7.3 Анализ аудита безопасности (FAU_SAA)

7.3.1 Характеристика семейства

Семейство FAU_SAA определяет требования для автоматизированных средств, которые анализируют показатели функционирования системы и данные аудита в целях поиска возможных или реальных нарушений безопасности. Этот анализ может использоваться для поддержки как обнаружения проникновения, так и автоматической реакции на ожидаемое нарушение безопасности.

Действия, предпринимаемые при обнаружении нарушений, могут быть при необходимости определены с использованием семейства FAU_ARP «Автоматическая реакция аудита безопасности».

7.3.2 Ранжирование компонентов

Рисунок 12 — Ранжирование компонентов семейства FAU_SAA

В FAU_SAA.1 «Анализ потенциального нарушения» требуется базовый порог обнаружения на основе установленного набора правил.

В FAU_SAA.2 «Выявление аномалии, основанное на профиле» ФБО поддерживают отдельные профили использования системы, где профиль представляет собой шаблоны предыстории использования, выполнявшиеся участниками целевой группы профиля. Целевая группа профиля может включать в себя одного или нескольких участников (например, отдельный пользователь; пользователи, совместно использующие общий идентификатор или общие учетные данные; пользователи, которым назначена одна роль; все пользователи системы или сетевого узла), которые взаимодействуют с ФБО. Каждому участнику целевой группы профиля назначается индивидуальный рейтинг подозрительной активности, который показывает, насколько текущие показатели действий участника соответствуют установленным шаблонам использования, представленным в профиле. Этот анализ может проводиться во время функционирования ОО или при анализе данных аудита в пакетном режиме.

В FAU_SAA.3 «Простая эвристика атаки» ФБО должны быть способны обнаружить возникновение характерных событий, которые свидетельствуют о значительной угрозе осуществлению ПБО. Этот поиск характерных событий может происходить в режиме реального времени или при анализе данных аудита в пакетном режиме.

В FAU_SAA.4 «Сложная эвристика атаки» ФБО должны быть способны задать и обнаружить многошаговые сценарии проникновения. Здесь ФБО способны сравнить события в системе (возможно, выполняемые несколькими участниками) с последовательностями событий, известными как полные сценарии проникновения. ФБО должны быть способны указать на обнаружение характерного события или последовательности событий, свидетельствующих о возможном нарушении ПБО.

7.3.3 Управление: FAU_SAA.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) сопровождение (добавление, модификация, удаление) правил из набора правил.

7.3.4 Управление: FAU_SAA.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) сопровождение (удаление, модификация, добавление) группы пользователей в целевой группе профиля.

7.3.5 Управление: FAU_SAA.3

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) сопровождение (удаление, модификация, добавление) подмножества событий системы.

7.3.6 Управление: FAU_SAA.4

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) сопровождение (удаление, модификация, добавление) подмножества событий системы;

b) сопровождение (удаление, модификация, добавление) набора последовательностей событий системы.

7.3.7 Аудит: FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: подключение и отключение любого из механизмов анализа;

b) минимальный: автоматические реакции, выполняемые инструментальными средствами.

7.3.8 FAU_SAA.1 Анализ потенциального нарушения

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_GEN.1 Генерация данных аудита

7.3.8.1 FAU_SAA.1.1

ФБО должны быть способны применять набор правил мониторинга событий, подвергающихся аудиту, и указывать на возможное нарушение ПБО, основываясь на этих правилах.

7.3.8.2 FAU_SAA.1.2

ФБО должны осуществлять следующие правила при мониторинге событий, подвергающихся аудиту:

a) накопление или объединение известных [назначение: *подмножество определенных событий, потенциально подвергаемых аудиту*], указывающих на возможное нарушение безопасности;

b) [назначение: *другие правила*].

7.3.9 FAU_SAA.2 Выявление аномалии, основанное на профиле

Иерархический для: FAU_SAA.1 Анализ потенциального нарушения

Зависимости: FIA_UID.1 Выбор момента идентификации

7.3.9.1 FAU_SAA.2.1

ФБО должны быть способны сопровождать профили использования системы, где каждый отдельный профиль представляет известные шаблоны предыстории использования, выполнявшиеся участниками [назначение: *спецификация целевой группы профиля*].

7.3.9.2 FAU_SAA.2.2

ФБО должны быть способны сопровождать рейтинг подозрительной активности для каждого пользователя, чьи действия отражены в профиле, где рейтинг подозрительной активности показывает степень несогласованности действий, выполняемых пользователем, с установленными шаблонами использования, представленными в профиле.

7.3.9.3 FAU_SAA.2.3

ФБО должны быть способны указывать на ожидаемое нарушение ПБО, когда рейтинг подозрительной активности пользователя превышает следующие пороговые условия [назначение: *условия, при которых ФБО сообщают об аномальных действиях*].

7.3.10 FAU_SAA.3 Простая эвристика атаки

Иерархический для: FAU_SAA.1 Анализ потенциального нарушения

Зависимости: нет зависимостей.

7.3.10.1 FAU_SAA.3.1

ФБО должны быть способны сопровождать внутреннее представление следующих характерных событий [назначение: *подмножество событий системы*], которые могут указывать на нарушение ПБО.

7.3.10.2 FAU_SAA.3.2

ФБО должны быть способны сравнивать характерные события с записью показателей функционирования системы, полученных при обработке [назначение: *информация, используемая для определения показателей функционирования системы*].

7.3.10.3 FAU_SAA.3.3

ФБО должны быть способны указывать на ожидаемое нарушение ПБО, когда событие системы соответствует характерному событию, указывающему на возможное нарушение ПБО.

7.3.11 FAU_SAA.4 Сложная эвристика атаки

Иерархический для: FAU_SAA.3 Простая эвристика атаки

Зависимости: нет зависимостей.

7.3.11.1 FAU_SAA.4.1

ФБО должны быть способны сопровождать внутреннее представление **следующих последовательностей событий известных сценариев проникновения [назначение: *список последовательностей событий системы, совпадение которых характерно для известных сценариев проникновения*]** и следующих характерных событий [назначение: *подмножество событий системы*], которые могут указывать на возможное нарушение ПБО.

7.3.11.2 FAU_SAA.4.2

ФБО должны быть способны сравнивать характерные события и **последовательности событий** с записью показателей функционирования системы, полученных при обработке [назначение: *информация, используемая для определения показателей функционирования системы*].

7.3.11.3 FAU_SAA.4.3

ФБО должны быть способны указывать на ожидаемое нарушение ПБО, когда **показатели функционирования системы** соответствуют характерному событию **или последовательности событий,** указывающим на возможное нарушение ПБО.

7.4 Просмотр аудита безопасности (FAU_SAR)

7.4.1 Характеристика семейства

Семейство FAU_SAR определяет требования к средствам аудита, к которым следует предоставить доступ уполномоченным пользователям для использования при просмотре данных аудита.

7.4.2 Ранжирование компонентов

Рисунок 13 — Ранжирование компонентов семейства FAU_SAR

FAU_SAR.1 «Просмотр аудита» предоставляет возможность читать информацию из записей аудита.

FAU_SAR.2 «Ограниченный просмотр аудита» содержит требование отсутствия доступа к информации кому-либо, кроме пользователей, указанных в FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 «Выборочный просмотр аудита» содержит требование отбора данных аудита средствами просмотра аудита на основе критериев просмотра.

7.4.3 Управление: FAU_SAR.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) поддержка (удаление, модификация, добавление) группы пользователей с правом доступа к чтению записей аудита.

7.4.4 Управление: FAU_SAR.2, FAU_SAR.3

Действия по управлению не предусмотрены.

7.4.5 Аудит: FAU_SAR.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) базовый: чтение информации из записей аудита.

7.4.6 Аудит: FAU_SAR.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) базовый: неуспешные попытки читать информацию из записей аудита.

7.4.7 Аудит: FAU_SAR.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) детализированный: параметры, используемые при просмотре.

7.4.8 FAU_SAR.1 Просмотр аудита

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_GEN.1 Генерация данных аудита

Компонент FAU_SAR.1 предоставит уполномоченным пользователям возможность получать и интерпретировать информацию. Для человека-пользователя эту информацию требуется представлять в понятном для него виде. Для внешней сущности ИТ информацию требуется представлять только в электронном виде.

7.4.8.1 FAU_SAR.1.1

ФБО должны предоставлять [назначение: *уполномоченные пользователи*] возможность читать [назначение: *список информации аудита*] из записей аудита.

7.4.8.2 FAU_SAR.1.2

ФБО должны предоставлять записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

7.4.9 FAU_SAR.2 Ограниченный просмотр аудита

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_SAR.1 Просмотр аудита

7.4.9.1 FAU_SAR.2.1

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

7.4.10 FAU_SAR.3 Выборочный просмотр аудита

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_SAR.1 Просмотр аудита

7.4.10.1 FAU_SAR.3.1

ФБО должны предоставлять возможность выполнять [выбор: *поиск, сортировка, упорядочение*] данных аудита, основанный на [назначение: *критерии с логическими отношениями*].

7.5 Выбор событий аудита безопасности (FAU_SEL)

7.5.1 Характеристика семейства

Семейство FAU_SEL определяет требования для отбора событий, которые будут подвергаться аудиту во время функционирования ОО, а также требования для включения или исключения событий из совокупности событий, подвергающихся аудиту.

7.5.2 Ранжирование компонентов

Рисунок 14 — Ранжирование компонентов семейства FAU_SEL

FAU_SEL.1 «Избирательный аудит» содержит требования возможности включения или исключения события из совокупности событий, подвергающихся аудиту, на основе атрибутов, определяемых разработчиком ПЗ/ЗБ.

7.5.3 Управление: FAU_SEL.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) сопровождение прав просмотра/модификации событий аудита.

7.5.4 Аудит: FAU_SEL.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: все модификации конфигурации аудита, происходящие во время сбора данных аудита.

7.5.5 FAU_SEL.1 Избирательный аудит

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_GEN.1 Генерация данных аудита

FMT_MTD.1 Управление данными ФБО

7.5.5.1 FAU_SEL.1.1

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

a) [выбор: *идентификатор объекта, идентификатор пользователя, идентификатор субъекта, идентификатор узла сети, тип события*];

b) [назначение: *список дополнительных атрибутов, на которых основана избирательность аудита*].

7.6 Хранение данных аудита безопасности (FAU_STG)

7.6.1 Характеристика семейства

Семейство FAU_STG определяет требования, при выполнении которых ФБО способны создавать и сопровождать журнал аудита безопасности.

7.6.2 Ранжирование компонентов

Рисунок 15 — Ранжирование компонентов семейства FAU_STG

В FAU_STG.1 «Защищенное хранение журнала аудита» содержатся требования защиты журнала аудита от несанкционированного удаления и/или модификации.

FAU_STG.2 «Гарантии доступности данных аудита» определяет гарантии того, что ФБО поддерживают имеющиеся данные аудита при возникновении нежелательной ситуации.

FAU_STG.3 «Действия в случае возможной потери данных аудита» определяет действия, которые необходимо предпринять, если превышен заданный порог заполнения журнала аудита.

FAU_STG.4 «Предотвращение потери данных аудита» определяет действия при переполнении журнала аудита.

7.6.3 Управление: FAU_STG.1

Действия по управлению не предусмотрены.

7.6.4 Управление: FAU_STG.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) сопровождение параметров, которые управляют возможностями хранения журнала аудита.

7.6.5 Управление: FAU_STG.3

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) отслеживание порога заполнения;

b) сопровождение (удаление, модификация, добавление) действий, которые нужно предпринять при возможном сбое хранения журнала аудита.

7.6.6 Управление: FAU_STG.4

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) сопровождение (удаление, модификация, добавление) действий, которые нужно предпринять при сбое хранения журнала аудита.

7.6.7 Аудит: FAU_STG.1, FAU_STG.2

Нет событий, для которых следует предусмотреть возможность аудита.

7.6.8 Аудит: FAU_STG.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: предпринимаемые действия после превышения порога заполнения.

7.6.9 Аудит: FAU_STG.4

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: предпринимаемые действия при сбое хранения журнала аудита.

7.6.10 FAU_STG.1 Защищенное хранение журнала аудита

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_GEN.1 Генерация данных аудита

7.6.10.1 FAU_STG.1.1

ФБО должны защищать хранимые записи аудита от несанкционированного удаления.

7.6.10.2 FAU_STG.1.2

ФБО должны быть способны [выбор (выбрать одно из): *предотвращать, выявлять*] несанкционированную модификацию хранимых записей аудита в журнале аудита.

7.6.11 FAU_STG.2 Гарантии доступности данных аудита

Иерархический для: FAU_STG.1 Защищенное хранение журнала аудита.

Зависимости: FAU_GEN.1 Генерация данных аудита

7.6.11.1 FAU_STG.2.1

ФБО должны защищать хранимые записи аудита от несанкционированного удаления.

7.6.11.2 FAU_STG.2.2

ФБО должны быть способны [выбор (выбрать одно из): *предотвращать, выявлять*] несанкционированную модификацию хранимых записей аудита в **журнале аудита**.

7.6.11.3 FAU_STG.2.3

ФБО должны обеспечивать поддержку [назначение: *показатель сохранности записей аудита*] при наступлении следующих событий: [выбор: *переполнение журнала аудита, сбой, атака*].

7.6.12 FAU_STG.3 Действия в случае возможной потери данных аудита

Иерархический для: нет подчиненных компонентов.

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита

7.6.12.1 FAU_STG.3.1

ФБО должны выполнять [назначение: *действия, которые нужно предпринимать в случае возможного сбоя хранения журнала аудита*], если журнал аудита превышает [назначение: *принятое ограничение*].

7.6.13 FAU_STG.4 Предотвращение потери данных аудита

Иерархический для: FAU_STG.3 Действия в случае возможной потери данных аудита

Зависимости: FAU_STG.1 Защищенное хранение журнала аудита

7.6.13.1 FAU_STG.4.1

ФБО должны [выбор (выбрать одно из): «*игнорировать события, подвергающиеся аудиту*», «*предотвращать события, подвергающиеся аудиту, исключая предпринимаемые уполномоченным пользователем со специальными правами*», «*записывать поверх самых старых хранимых записей аудита*» и [назначение: *другие действия, которые нужно предпринимать в случае возможного сбоя хранения журнала аудита*] при переполнении журнала аудита.

8 Класс FCO. Связь

Класс FCO содержит два семейства, связанные с уверенностью в идентичности сторон, участвующих в обмене данными: идентичностью отправителя переданной информации (доказательство отправления) и идентичностью получателя переданной информации (доказательство получения). Эти семейства обеспечивают то, что отправитель не сможет отрицать факт отправления сообщения, а получатель не сможет отрицать факт его получения.

Рисунок 16 — Декомпозиция класса FCO «Связь»

8.1 Неотказуемость отправления (FCO_NRO)

8.1.1 Характеристика семейства

Семейство FCO_NRO обеспечивает невозможность отрицания отправителем информации факта ее отправления. Семейство FCO_NRO содержит требование, чтобы ФБО обеспечили метод предоставления субъекту-получателю свидетельства отправления информации. Это свидетельство может быть затем верифицировано этим субъектом или другими субъектами.

8.1.2 Ранжирование компонентов

Рисунок 17 — Ранжирование компонентов семейства FCO_NRO

FCO_NRO.1 «Избирательное доказательство отправления» содержит требование, чтобы ФБО предоставили субъектам возможность запросить свидетельство отправления информации.

FCO_NRO.2 «Принудительное доказательство отправления» содержит требование, чтобы ФБО всегда генерировали свидетельство отправления передаваемой информации.

8.1.3 Управление: FCO_NRO.1, FCO_NRO.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление изменениями типов и полей информации, атрибутов отправителей информации и получателей свидетельств.

8.1.4 Аудит: FCO_NRO.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: идентификатор пользователя, который запросил генерацию свидетельства отправления;

b) минимальный: обращение к функции неотказуемости;

c) базовый: идентификация информации, получателя и копии предоставляемого свидетельства;

d) детализированный: идентификатор пользователя, который запросил верификацию свидетельства.

8.1.5 Аудит: FCO_NRO.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: обращение к функции неотказуемости;

b) базовый: идентификация информации, получателя и копии предоставляемого свидетельства;

c) детализированный: идентификатор пользователя, который запросил верификацию свидетельства.

8.1.6 FCO_NRO.1 Избирательное доказательство отправления

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UID.1 Выбор момента идентификации

8.1.6.1 FCO_NRO.1.1

ФБО должны быть способны генерировать свидетельство отправления передаваемой [назначение: *список типов информации*] при запросе [выбор: *отправитель, получатель, [назначение: список третьих лиц]*].

8.1.6.2 FCO_NRO.1.2

ФБО должны быть способны связывать [назначение: *список атрибутов*] отправителя информации и [назначение: *список информационных полей*] информации, к которой прилагается свидетельство.

8.1.6.3 FCO_NRO.1.3

ФБО должны предоставлять возможность верифицировать свидетельство отправления информации [выбор: *отправитель, получатель, [назначение: список третьих лиц]*] при установленных [назначение: *ограничения на свидетельство отправления*].

8.1.7 FCO_NRO.2 Принудительное доказательство отправления

Иерархический для: FCO_NRO.1 Избирательное доказательство отправления

Зависимости: FIA_UID.1 Выбор момента идентификации

8.1.7.1 FCO_NRO.2.1

ФБО должны **всегда осуществлять генерацию** свидетельства отправления передаваемой [назначение: *список типов информации*].

8.1.7.2 FCO_NRO.2.2

ФБО должны быть способны связывать [назначение: *список атрибутов*] отправителя информации и [назначение: *список информационных полей*] информации, к которой прилагается свидетельство.

8.1.7.3 FCO_NRO.2.3

ФБО должны предоставлять возможность верифицировать свидетельство отправления информации [выбор: *отправитель, получатель, [назначение: список третьих лиц]*] при установленных [назначение: *ограничения на свидетельство отправления*].

8.2 Неотказуемость получения (FCO_NRR)

8.2.1 Характеристика семейства

Неотказуемость получения обеспечивает невозможность отрицания получателем информации факта ее получения. Семейство FCO_NRR содержит требование, чтобы ФБО обеспечили метод предоставления субъекту-отправителю свидетельства получения информации. Это свидетельство может быть затем верифицировано этим субъектом или другими субъектами.

8.2.2 Ранжирование компонентов

Рисунок 18 — Ранжирование компонентов семейства FCO_NRR

FCO_NRR.1 «Избирательное доказательство получения» содержит требование, чтобы ФБО предоставили субъектам возможность запросить свидетельство получения информации.

FCO_NRR.2 «Принудительное доказательство получения» содержит требование, чтобы ФБО всегда генерировали свидетельство получения принятой информации.

8.2.3 Управление: FCO_NRR.1, FCO_NRR.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление изменениями типов и полей информации, атрибутов отправителей информации и других получателей свидетельств.

8.2.4 Аудит: FCO_NRR.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: идентификатор пользователя, который запросил генерацию свидетельства получения;

b) минимальный: обращение к функции неотказуемости;

c) базовый: идентификация информации, получателя и копии предоставляемого свидетельства;

d) детализированный: идентификатор пользователя, который запросил верификацию свидетельства.

8.2.5 Аудит: FCO_NRR.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: обращение к функции неотказуемости;

b) базовый: идентификация информации, получателя и копии предоставляемого свидетельства;

c) детализированный: идентификатор пользователя, который запросил верификацию свидетельства.

8.2.6 FCO_NRR.1 Избирательное доказательство получения

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UID.1 Выбор момента идентификации

8.2.6.1 FCO_NRR.1.1

ФБО должны быть способны генерировать свидетельство получения принятой [назначение: *список типов информации*] при запросе [выбор: *отправитель, получатель, [назначение: список третьих лиц]*].

8.2.6.2 FCO_NRR.1.2

ФБО должны быть способны связывать [назначение: *список атрибутов*] получателя информации и [назначение: *список информационных полей*] информации, к которой прилагается свидетельство.

8.2.6.3 FCO_NRR.1.3

ФБО должны предоставлять возможность верифицировать свидетельство получения информации [выбор: *отправитель, получатель, [назначение: список третьих лиц]*] при установленных [назначение: *ограничения на свидетельство отправления*].

8.2.7 FCO_NRR.2 Принудительное доказательство получения

Иерархический для: FCO_NRR.1 Избирательное доказательство получения

Зависимости: FIA_UID.1 Выбор момента идентификации

8.2.7.1 FCO_NRR.2.1

ФБО должны **осуществлять генерацию** свидетельства получения принятой [назначение: *список типов информации*].

8.2.7.2 FCO_NRR.2.2

ФБО должны быть способны связывать [назначение: *список атрибутов*] получателя информации и [назначение: *список информационных полей*] информации, к которой прилагается свидетельство.

8.2.7.3 FCO_NRR.2.3

ФБО должны предоставлять возможность верифицировать свидетельство получения информации [выбор: *отправитель, получатель, [назначение: список третьих лиц]*] при установленных [назначение: *ограничения на свидетельство отправления*].

9 Класс FCS. Криптографическая поддержка

ФБО могут использовать криптографические функциональные возможности для содействия достижению некоторых, наиболее важных целей безопасности. К ним относятся (но ими не ограничиваются) следующие цели: идентификация и аутентификация, неотказуемость, доверенный маршрут, доверенный канал, разделение данных. Класс FCS применяют, если ОО имеет криптографические функции, которые могут быть реализованы аппаратными, программно-аппаратными и/или программными средствами.

Класс FCS «Криптографическая поддержка» состоит из двух семейств: FCS_CKM «Управление криптографическими ключами» и FCS_COP «Криптографические операции». В семействе FCS_CKM «Управление криптографическими ключами» рассмотрены аспекты управления криптографическими ключами, тогда как в семействе FCS_COP «Криптографические операции» рассмотрено практическое применение этих криптографических ключей.

Рисунок 19 — Декомпозиция класса FCS «Криптографическая поддержка»

9.1 Управление криптографическими ключами (FCS_CKM)

9.1.1 Характеристика семейства

Криптографическими ключами необходимо управлять на протяжении всего их жизненного цикла. Семейство FCS_CKM предназначено для поддержки жизненного цикла и поэтому определяет требования к следующим действиям с криптографическими ключами: генерация, распределение, доступ к ним и их уничтожение. Это семейство следует использовать в случаях, если имеются функциональные требования управления криптографическими ключами.

9.1.2 Ранжирование компонентов

Рисунок 20 — Ранжирование компонентов семейства FCS_CKM

FCS_CKM.1 «Генерация криптографических ключей» содержит требования к их созданию согласно определенному алгоритму и длине ключа, которые могут основываться на соответствующем стандарте.

FCS_CKM.2 «Распределение криптографических ключей» содержит требование их распределения определенным методом, который может основываться на соответствующем стандарте.

FCS_CKM.3 «Доступ к криптографическим ключам» содержит требование осуществления доступа к ним согласно определенному методу, который может основываться на соответствующем стандарте.

FCS_CKM.4 «Уничтожение криптографических ключей» содержит требование их уничтожения согласно определенному методу, который может основываться на соответствующем стандарте.

9.1.3 Управление: FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление изменениями атрибутов криптографических ключей. Примерами атрибутов ключа являются: идентификатор пользователя, тип ключа (например, открытый, приватный, секретный), период действия ключа, а также возможное использование (например цифровая подпись, шифрование других ключей, согласование ключей, шифрование данных).

9.1.4 Аудит: FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешный или неуспешный результат действия;

b) базовый: атрибуты объекта и содержание объекта, за исключением любой чувствительной информации (например, секретных или приватных ключей).

9.1.5 FCS_CKM.1 Генерация криптографических ключей

Иерархический для: нет подчиненных компонентов.

Зависимости: [FCS_CKM.2 Распределение криптографических ключей или
FCS_COP.1 Криптографические операции]
FCS_CKM.4 Уничтожение криптографических ключей
FMT_MSA.2 Безопасные значения атрибутов безопасности

9.1.5.1 FCS_CKM.1.1

ФБО должны генерировать криптографические ключи в соответствии с определенным алгоритмом [назначение: *алгоритм генерации криптографических ключей*] и длиной [назначение: *длины криптографических ключей*], которые отвечают следующему: [назначение: *список стандартов*].

9.1.6 FCS_CKM.2 Распределение криптографических ключей

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ITC.1 Импорт данных пользователя без атрибутов безопасности или
FDP_ITC.2 Импорт данных пользователя с атрибутами безопасности, или
FCS_CKM.1 Генерация криптографических ключей]
FCS_CKM.4 Уничтожение криптографических ключей
FMT_MSA.2 Безопасные значения атрибутов безопасности

9.1.6.1 FCS_CKM.2.1

ФБО должны распределять криптографические ключи в соответствии с определенным методом [назначение: метод *распределения криптографических ключей*], который отвечает следующему: [назначение: *список стандартов*].

9.1.7 FCS_CKM.3 Доступ к криптографическим ключам

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ITC.1 Импорт данных пользователя без атрибутов безопасности или
FDP_ITC.2 Импорт данных пользователя с атрибутами безопасности, или
FCS_CKM.1 Генерация криптографических ключей]
FCS_CKM.4 Уничтожение криптографических ключей
FMT_MSA.2 Безопасные значения атрибутов безопасности

9.1.7.1 FCS_CKM.3.1

ФБО должны выполнять [назначение: *тип доступа к криптографическим ключам*] в соответствии с определенным методом доступа [назначение: *метод доступа к криптографическим ключам*], который отвечает следующему: [назначение: *список стандартов*].

9.1.8 FCS_CKM.4 Уничтожение криптографических ключей

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ITC.1 Импорт данных пользователя без атрибутов безопасности или
FDP_ITC.2 Импорт данных пользователя с атрибутами безопасности, или
FCS_CKM.1 Генерация криптографических ключей]
FMT_MSA.2 Безопасные значения атрибутов безопасности

9.1.8.1 FCS_CKM.4.1

ФБО должны уничтожать криптографические ключи в соответствии с определенным методом [назначение: *метод уничтожения криптографических ключей*], который отвечает следующему: [назначение: *список стандартов*].

9.2 Криптографические операции (FCS_COP)

9.2.1 Характеристика семейства

Для корректного осуществления криптографических операций их необходимо выполнять в соответствии с определенным алгоритмом и криптографическими ключами определенной длины. Данное семейство следует применять всякий раз, если необходимо выполнять криптографические операции.

К типичным криптографическим операциям относятся: зашифрование и/или расшифрование данных, генерация и/или верификация цифровых подписей, генерация криптографических контрольных сумм для обеспечения целостности и/или верификации контрольных сумм, хэширование (вычисление хэш-образа сообщения), зашифрование и/или расшифрование криптографических ключей, согласование криптографических ключей.

9.2.2 Ранжирование компонентов

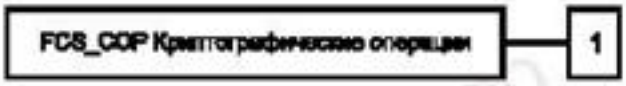

Рисунок 21 — Ранжирование компонентов семейства FCS_COP

FCS_COP.1 «Криптографические операции» содержит требования их выполнения по определенным алгоритмам с применением криптографических ключей определенной длины. Алгоритмы и длина криптографических ключей могут основываться на соответствующем стандарте.

9.2.3 Управление: FCS_COP.1

Действия по управлению не предусмотрены.

9.2.4 Аудит: FCS_COP.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешное или неуспешное завершение, а также тип криптографической операции;

b) базовый: любые применяемые криптографические режимы операций, атрибуты субъектов и объектов.

9.2.5 FCS_COP.1 Криптографические операции

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ITC.1 Импорт данных пользователя без атрибутов безопасности или
FDP_ITC.2 Импорт данных пользователя с атрибутами безопасности, или
FCS_CKM.1 Генерация криптографических ключей]
FCS_CKM.4 Уничтожение криптографических ключей
FMT_MSA.2 Безопасные значения атрибутов безопасности

9.2.5.1 FCS_COP.1.1

ФБО должны выполнять [назначение: *список криптографических операций*] в соответствии с определенными алгоритмами [назначение: *криптографические алгоритмы*] и длиной [назначение: *длины криптографических ключей*], которые отвечают следующему: [назначение: *список стандартов*].

10 Класс FDP. Защита данных пользователя

Класс FDP «Защита данных пользователя» содержит семейства, определяющие требования к функциям безопасности ОО и политикам функций безопасности ОО, связанным с защитой данных пользователя. Он разбит на четыре группы семейств, перечисленные ниже и применяемые к данным пользователя в

пределах ОО при их импорте, экспорте и хранении, а также к атрибутам безопасности, прямо связанным с данными пользователя:

a) политики функций безопасности для защиты данных пользователя:

1) FDP_ACC «Политика управления доступом»,

2) FDP_IFC «Политика управления информационными потоками».

Компоненты этих семейств позволяют разработчику ПЗ/ЗБ именовать политики функций безопасности для защиты данных пользователя и определять область действия этих политик, которые необходимо соотнести с целями безопасности. Предполагается, что имена этих политик будут использоваться повсеместно в тех функциональных компонентах, которые имеют операцию, запрашивающую назначение или выбор «ПФБ управления доступом» и/или «ПФБ управления информационными потоками». Правила, которые определяют функциональные возможности именованных ПФБ управления доступом и управления информационными потоками, будут установлены в семействах FDP_ACF «Функции управления доступом» и FDP_IFF «Функции управления информационными потоками» соответственно;

b) виды защиты данных пользователя:

1) FDP_ACF «Функции управления доступом»,

2) FDP_IFF «Функции управления информационными потоками»,

3) FDP_ITT «Передача в пределах ОО»,

4) FDP_RIP «Защита остаточной информации»,

5) FDP_ROL «Откат»,

6) FDP_SDI «Целостность хранимых данных»;

c) автономное хранение, импорт и экспорт данных:

1) FDP_DAU «Аутентификация данных»,

2) FDP_ETC «Экспорт данных за пределы действия ФБО»,

3) FDP_ITC «Импорт данных из-за пределов действия ФБО».

Компоненты этих семейств связаны с доверенной передачей данных в ОДФ или из ОДФ;

d) связь между ФБО:

1) FDP_UCT «Защита конфиденциальности данных пользователя при передаче между ФБО»,

2) FDP_UIT «Защита целостности данных пользователя при передаче между ФБО».

Компоненты этих семейств определяют взаимодействие между ФБО собственно ОО и другого доверенного продукта ИТ.

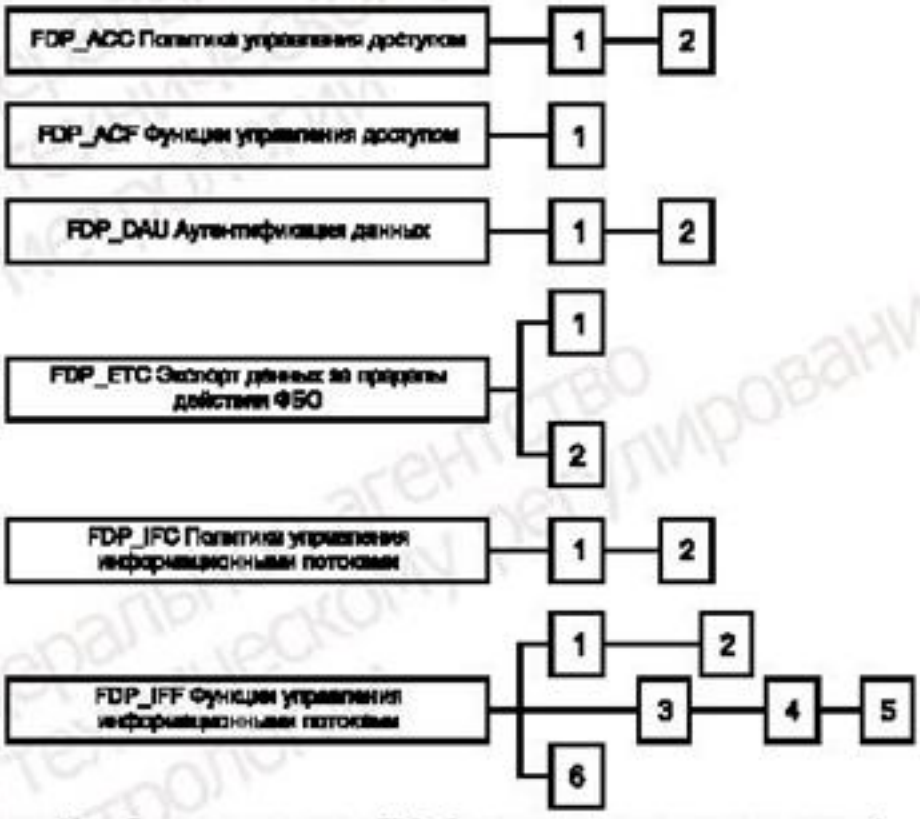

Рисунок 22 — Декомпозиция класса FDP «Защита данных пользователя», лист 1

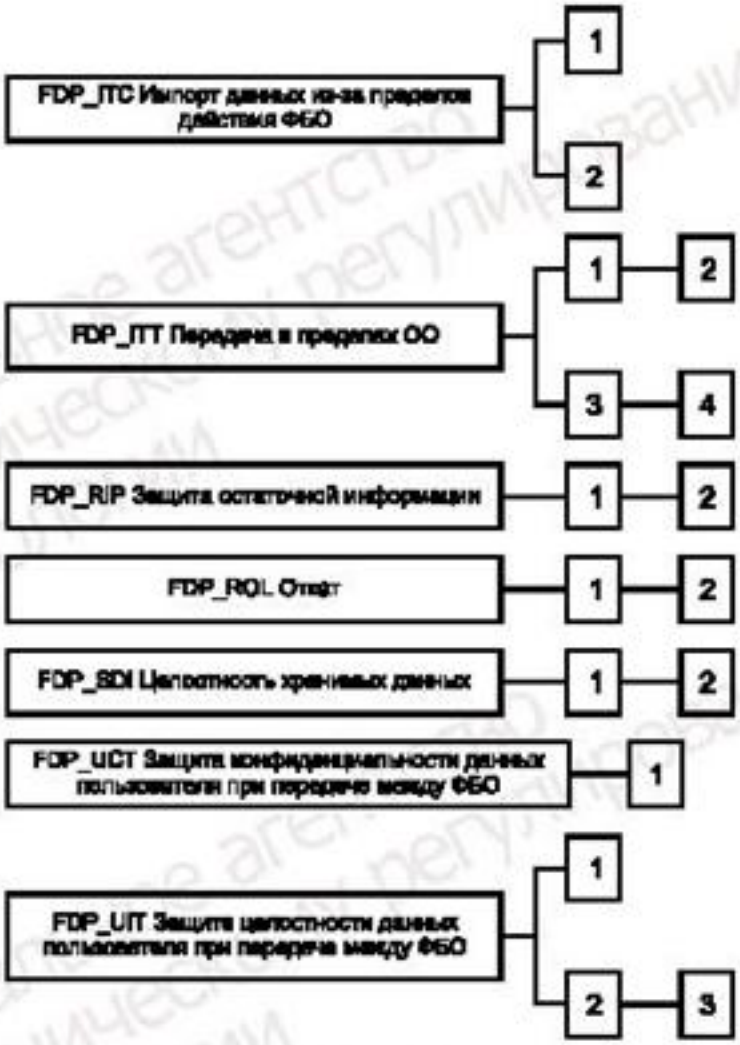

Рисунок 22, лист 2

10.1 Политика управления доступом (FDP_ACC)

10.1.1 Характеристика семейства

Семейство FDP_ACC идентифицирует ПФБ управления доступом, устанавливая им имена, и определяет области действия политик, образующих идентифицированную часть управления доступом ПБО. Области действия можно характеризовать тремя множествами: субъекты под управлением политики, объекты под управлением политики и операции управляемых субъектов на управляемых объектах, на которые распространяется политика. Общие критерии допускают существование нескольких политик, каждая из которых имеет уникальное имя. Это достигается посредством выполнения итераций компонентов рассматриваемого семейства по одному разу для каждой именованной политики управления доступом. Правила, определяющие функциональные возможности ПФБ управления доступом, будут установлены другими семействами, такими как FDP_ACF «Функции управления доступом» и FDP_SDI «Целостность хранимых данных». Предполагается, что имена ПФБ, идентифицированные в семействе FDP_ACC «Политика управления доступом», будут использоваться повсеместно в функциональных компонентах, которые имеют операцию, запрашивающую назначение или выбор «ПФБ управления доступом».

10.1.2 Ранжирование компонентов

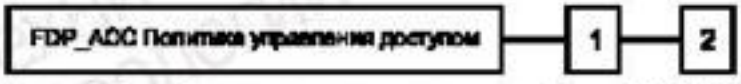

Рисунок 23 — Ранжирование компонентов семейства FDP_ACC

FDP_ACC.1 «Ограниченное управление доступом» содержит требование, чтобы каждая идентифицированная ПФБ управления доступом существовала для подмножества возможных операций на подмножестве объектов в ОО.

FDP_ACC.2 «Полное управление доступом» содержит требование, чтобы каждая идентифицированная ПФБ управления доступом охватывала все операции субъектов на объектах, управляемых этой ПФБ. Кроме этого, требуется, чтобы все объекты и операции в ОДФ были охвачены, по меньшей мере, одной идентифицированной ПФБ управления доступом.

10.1.3 Управление: FDP_ACC.1, FDP_ACC.2

Действия по управлению не предусмотрены.

10.1.4 Аудит: FDP_ACC.1, FDP_ACC.2

Нет событий, для которых следует предусмотреть возможность аудита.

10.1.5 FDP_ACC.1 Ограниченное управление доступом

Иерархический для: нет подчиненных компонентов.

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

10.1.5.1 FDP_ACC.1.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом*] для [назначение: *список субъектов, объектов и операций субъектов на объектах, на которые распространяется ПФБ*].

10.1.6 FDP_ACC.2 Полное управление доступом

Иерархический для: FDP_ACC.1 Ограниченное управление доступом

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

10.1.6.1 FDP_ACC.2.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом*] для [назначение: *список субъектов и объектов*] **и всех операций субъектов на объектах, на которые распространяется ПФБ.**

10.1.6.2 FDP_ACC.2.2

ФБО должны обеспечивать, чтобы на операции любого субъекта из ОДФ на любом объекте из ОДФ распространялась какая-либо ПФБ управления доступом.

10.2 Функции управления доступом (FDP_ACF)

10.2.1 Характеристика семейства

Семейство FDP_ACF описывает правила для конкретных функций, которые могут реализовать политики управления доступом, именованные в FDP_ACC. В FDP_ACC также определяется область действия этих политик.

10.2.2 Ранжирование компонентов

Рисунок 24 — Ранжирование компонентов семейства FDP_ACF

В этом семействе рассмотрены использование атрибутов безопасности и характеристики политик управления доступом. Предполагается, что компонент этого семейства будет использован, чтобы описать правила для функции, которая реализует ПФБ, ранее идентифицированную в FDP_ACC «Политика управления доступом». Разработчик ПЗ/ЗБ может также выполнять итерации этого компонента, если в ОО имеется несколько таких политик.

FDP_ACF.1 «Управление доступом, основанное на атрибутах безопасности» позволяет ФБО осуществить доступ, основанный на атрибутах и именованных группах атрибутов безопасности. Кроме того, ФБО могут иметь возможность явно разрешать или запрещать доступ к объекту, основываясь на атрибутах безопасности.

10.2.3 Управление: FDP_ACF.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление атрибутами, используемыми для явного разрешения или запрещения доступа.

10.2.4 Аудит: FDP_ACF.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешные запросы на выполнение операций на объекте, на который распространяется ПФБ;

b) базовый: все запросы на выполнение операций на объекте, на который распространяется ПФБ;

c) детализированный: специальные атрибуты безопасности, используемые при проверке правомерности доступа.

10.2.5 FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: FDP_ACC.1 Ограниченное управление доступом

FMT_MSA.3 Инициализация статических атрибутов

10.2.5.1 FDP_ACF.1.1

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

10.2.5.2 FDP_ACF.1.2

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

10.2.5.3 FDP_ACF.1.3

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

10.2.5.4 FDP_ACF.1.4

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

10.3 Аутентификация данных (FDP_DAU)

10.3.1 Характеристика семейства

Аутентификация данных позволяет сущности принять ответственность за подлинность информации (например, с использованием цифровой подписи). Семейство FDP_DAU содержит метод предоставления гарантии правильности специфического набора данных, который может быть впоследствии использован для верификации того, что содержание информации не было подделано или модифицировано мошенническим путем. В отличие от класса FAU «Аудит безопасности» данное семейство предназначено для применения скорее к статическим, чем к перемещаемым данным.

10.3.2 Ранжирование компонентов

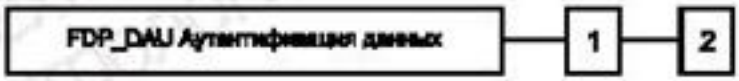

Рисунок 25 — Ранжирование компонентов семейства FDP_DAU

FDP_DAU.1 «Базовая аутентификация данных» содержит требование, чтобы ФБО были способны предоставить гарантию подлинности информации, содержащейся в объектах (например, документах).

FDP_DAU.2 «Аутентификация данных с идентификацией гаранта» содержит дополнительное требование, чтобы ФБО были способны установить идентификатор субъекта, который предоставил гарантию подлинности.

10.3.3 Управление: FDP_DAU.1, FDP_DAU.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) настройка в системе назначения или модификации объектов, для которых применяется аутентификация данных.

10.3.4 Аудит: FDP_DAU.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешная генерация свидетельства правильности;

b) базовый: неуспешная генерация свидетельства правильности;

c) детализированный: идентификатор субъекта, который запросил свидетельство.

10.3.5 Аудит: FDP_DAU.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешная генерация свидетельства правильности;

b) базовый: неуспешная генерация свидетельства правильности;

c) детализированный: идентификатор субъекта, который запросил свидетельство;

d) детализированный: идентификатор субъекта, который генерировал свидетельство.

10.3.6 FDP_DAU.1 Базовая аутентификация данных

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

10.3.6.1 FDP_DAU.1.1

ФБО должны предоставлять возможность генерировать свидетельство, которое может быть использовано как гарантия правильности [назначение: *список объектов или типов информации*].

10.3.6.2 FDP_DAU.1.2

ФБО должны предоставлять [назначение: список субъектов] возможность верифицировать свидетельство правильности указанной информации.

10.3.7 FDP_DAU.2 Аутентификация данных с идентификацией гаранта

Иерархический для: FDP_DAU.1 Базовая аутентификация данных

Зависимости: FIA_UID.1 Выбор момента идентификации

10.3.7.1 FDP_DAU.2.1

ФБО должны предоставлять возможность генерировать свидетельство, которое может быть использовано как гарантия правильности [назначение: *список объектов или типов информации*].

10.3.7.2 FDP_DAU.2.2

ФБО должны предоставлять [назначение: *список субъектов*] возможность верифицировать свидетельство правильности указанной информации и **идентификатор пользователя, который создал свидетельство.**

10.4 Экспорт данных за пределы действия ФБО (FDP_ETC)

10.4.1 Характеристика семейства

Семейство FDP_ETC определяет функции для экспорта данных пользователя из ОО так, чтобы их атрибуты безопасности и защита могли или полностью сохраняться или игнорироваться при экспорте этих данных. В семействе также рассматриваются ограничения на экспорт и ассоциация атрибутов безопасности с экспортируемыми данными пользователя.

10.4.2 Ранжирование компонентов

Рисунок 26 — Ранжирование компонентов семейства FDP_ETC

FDP_ETC.1 «Экспорт данных пользователя без атрибутов безопасности» содержит требование, чтобы ФБО осуществляли соответствующие ПФБ при экспорте данных пользователя за пределы действия ФБО. Данные пользователя, которые экспортируются этой функцией, не сопровождаются ассоциированными с ними атрибутами безопасности.

FDP_ETC.2 «Экспорт данных пользователя с атрибутами безопасности» содержит требование, чтобы ФБО осуществляли соответствующие ПФБ, используя функцию, которая точно и однозначно ассоциирует атрибуты безопасности с экспортируемыми данными пользователя.

10.4.3 Управление: FDP_ETC.1

Действия по управлению не предусмотрены.

10.4.4 Управление: FDP_ETC.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) изменение дополнительных правил управления экспортом информации пользователем с определенной ролью.

10.4.5 Аудит: FDP_ETC.1, FDP_ETC.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешный экспорт информации;

b) базовый: все попытки экспортировать информацию.

10.4.6 FDP_ETC.1 Экспорт данных пользователя без атрибутов безопасности

Иерархический для: нет подчиненных компонентов.

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

10.4.6.1 FDP_ETC.1.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*] при экспорте данных пользователя, контролируемом ПФБ, за пределы ОДФ.

10.4.6.2 FDP_ETC.1.2

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

10.4.7 FDP_ETC.2 Экспорт данных пользователя с атрибутами безопасности

Иерархический для: нет подчиненных компонентов.

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

10.4.7.1 FDP_ETC.2.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*] при экспорте данных пользователя, контролируемом ПФБ, за пределы ОДФ.

10.4.7.2 FDP_ETC.2.2

ФБО должны экспортировать данные пользователя с атрибутами безопасности, ассоциированными с данными пользователя.

10.4.7.3 FDP_ETC.2.3

ФБО должны обеспечивать, чтобы при экспорте за пределы ОДФ атрибуты безопасности однозначно ассоциировались с экспортируемыми данными пользователя.

10.4.7.4 FDP_ETC.2.4

ФБО должны осуществлять следующие правила при экспорте данных пользователя из ОДФ: [назначение: *дополнительные правила управления экспортом информации*].

10.5 Политика управления информационными потоками (FDP_IFC)

10.5.1 Характеристика семейства

Семейство FDP_IFC идентифицирует ПФБ управления информационными потоками, устанавливая им имена, и определяет области действия политик, образующих идентифицированную часть управления информационными потоками ПБО. Эти области действия можно характеризовать тремя множествами: субъекты под управлением политики, информация под управлением политики и операции перемещения управляемой информации к управляемым субъектам и от них, на которые распространяется политика. Общие критерии допускают существование нескольких политик, каждая из которых имеет уникальное имя. Это достигается посредством выполнения итераций компонентов рассматриваемого семейства по одному разу для каждой именованной политики управления информационными потоками. Правила, определяющие функциональные возможности ПФБ управления информационными потоками, будут установлены другими семействами, такими как FDP_IFF «Функции управления информационными потоками» и FDP_SDI «Целостность хранимых данных». Имена ПФБ управления информационными потоками, идентифицированные в семействе FDP_IFC, в дальнейшем будут использоваться повсеместно в тех функциональных компонентах, которые включают в себя операцию, запрашивающую назначение или выбор «ПФБ управления информационными потоками».

Механизм ФБО управляет информационными потоками в соответствии с ПФБ управления информационными потоками. Операции, которые изменяли бы атрибуты безопасности информации, в общем случае недопустимы, поскольку это было бы нарушением ПФБ управления информационными потоками. Однако, как исключение, такие операции могут быть разрешены в ПФБ управления информационными потоками, если это явно определено.

10.5.2 Ранжирование компонентов

Рисунок 27 — Ранжирование компонентов семейства FDP_IFC

FDP_IFC.1 «Ограниченное управление информационными потоками» содержит требование, чтобы каждая идентифицированная ПФБ управления информационными потоками выполнялась для подмножества возможных операций на подмножестве информационных потоков в ОО.

FDP_IFC.2 «Полное управление информационными потоками» содержит требование, чтобы каждая идентифицированная ПФБ управления информационными потоками охватывала все операции для субъектов и информацию под управлением этой ПФБ. Также требуется, чтобы все информационные потоки и операции в пределах ОДФ были охвачены хотя бы одной идентифицированной ПФБ управления информационными потоками. Совместно с компонентом FPT_RVM.1 это обеспечивает аспект «постоянная готовность» монитора обращений.

10.5.3 Управление: FDP_IFC.1, FDP_IFC.2

Действия по управлению не предусмотрены.

10.5.4 Аудит: FDP_IFC.1, FDP_IFC.2

Нет событий, для которых следует предусмотреть возможность аудита.

10.5.5 FDP_IFC.1 Ограниченное управление информационными потоками

Иерархический для: нет подчиненных компонентов.

Зависимости: FDP_IFF.1 Простые атрибуты безопасности

10.5.5.1 FDP_IFC.1.1

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

10.5.6 FDP_IFC.2 Полное управление информационными потоками

Иерархический для: FDP_IFC.1 Ограниченное управление информационными потоками

Зависимости: FDP_IFF.1 Простые атрибуты безопасности

10.5.6.1 FDP_IFC.2.1

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

10.5.6.2 FDP_IFC.2.2

ФБО должны обеспечивать, чтобы в пределах ОДФ на все операции перемещения управляемой информации к управляемым субъектам и от них распространялась какая-либо ПФБ управления информационными потоками.

10.6 Функции управления информационными потоками (FDP_IFF)

10.6.1 Характеристика семейства

Семейство FDP_IFF описывает правила для конкретных функций, которые могут реализовать ПФБ управления информационными потоками, именованные в FDP_IFC «Политика управления информационными потоками», где также определена область действия соответствующей политики. Семейство содержит два типа требований: первый связан с обычными информационными потоками, а второй — с неразрешенными информационными потоками (скрытыми каналами). Это разделение возникает, потому что проблема неразрешенных информационных потоков в некотором смысле противоречит остальным аспектам ПФБ управления информационными потоками. По существу, скрытые каналы дают возможность обходить ПФБ управления информационными потоками в нарушение политики. Таким образом, возникает потребность в специальных функциях, которые ограничивают либо предотвращают их возникновение.

10.6.2 Ранжирование компонентов

Рисунок 28 — Ранжирование компонентов семейства FDP_IFF

FDP_IFF.1 «Простые атрибуты безопасности» содержит требование наличия атрибутов безопасности информации и субъектов, которые выступают как инициаторы отправления или получатели этой информации. В нем также определяются правила, которые необходимо реализовать с использованием функции, и описано, как функция получает атрибуты безопасности.

FDP_IFF.2 «Иерархические атрибуты безопасности» расширяет требования предыдущего компонента, требуя, чтобы все ПФБ управления информационными потоками в ПБО использовали иерархические атрибуты безопасности, которые образуют некоторую структуру.

FDP_IFF.3 «Ограничение неразрешенных информационных потоков» содержит требование, чтобы ПФБ распространялась на неразрешенные информационные потоки, но не обязательно устраняла их.

FDP_IFF.4 «Частичное устранение неразрешенных информационных потоков» содержит требование, чтобы ПФБ обеспечила устранение некоторых, но не обязательно всех, неразрешенных информационных потоков.

FDP_IFF.5 «Полное устранение неразрешенных информационных потоков» содержит требование, чтобы ПФБ обеспечила устранение всех неразрешенных информационных потоков.

FDP_IFF.6 «Мониторинг неразрешенных информационных потоков» содержит требование, чтобы ПФБ отслеживала неразрешенные информационные потоки, максимальная интенсивность которых превышает заданное пороговое значение.

10.6.3 Управление: FDP_IFF.1, FDP_IFF.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление атрибутами, используемыми для явного разрешения и запрещения доступа.

10.6.4 Управление: FDP_IFF.3, FDP_IFF.4, FDP_IFF.5

Действия по управлению не предусмотрены.

10.6.5 Управление: FDP_IFF.6

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) включение или отключение функции мониторинга;

b) модификация максимальной интенсивности, которая отслеживается при мониторинге.

10.6.6 Аудит: FDP_IFF.1, FDP_IFF.2, FDP_IFF.5

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: разрешения на запрашиваемые информационные потоки;

b) базовый: все решения по запросам на информационные потоки;

c) детализированный: специфические атрибуты безопасности, используемые при принятии решений по осуществлению информационных потоков;

d) детализированный: некоторые специфические подмножества информации, передача которой обусловлена целями политики (например аудит материалов, для которых гриф секретности был понижен).

10.6.7 Аудит: FDP_IFF.3, FDP_IFF.4, FDP_IFF.6

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: разрешения на запрашиваемые информационные потоки;

b) базовый: все решения по запросам на информационные потоки;

c) базовый: использование выявленных скрытых каналов;

d) детализированный: специфические атрибуты безопасности, используемые при принятии решений по осуществлению информационных потоков;

e) детализированный: некоторые специфические подмножества информации, передача которой обусловлена целями политики (например аудит материалов, для которых гриф секретности был понижен);

f) детализированный: использование идентифицированных скрытых каналов, для которых оценка максимальной интенсивности превышает заданное пороговое значение.

10.6.8 FDP_IFF.1 Простые атрибуты безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: FDP_IFC.1 Ограниченное управление информационными потоками
FMT_MSA.3 Инициализация статических атрибутов

10.6.8.1 FDP_IFF.1.1

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

10.6.8.2 FDP_IFF.1.2

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

10.6.8.3 FDP_IFF.1.3

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

10.6.8.4 FDP_IFF.1.4

ФБО должны предоставлять следующее [назначение: *список дополнительных возможностей ПФБ*].

10.6.8.5 FDP_IFF.1.5

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

10.6.8.6 FDP_IFF.1.6

ФБО должны явно запрещать информационный поток, основываясь на следующих правилах: [назначение: *основанные на атрибутах безопасности правила, которые явно запрещают информационные потоки*].

10.6.9 FDP_IFF.2 Иерархические атрибуты безопасности

Иерархический для: FDP_IFF.1 Простые атрибуты безопасности

Зависимости: FDP_IFC.1 Ограниченное управление информационными потоками
FMT_MSA.3 Инициализация статических атрибутов

10.6.9.1 FDP_IFF.2.1

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

10.6.9.2 FDP_IFF.2.2

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

10.6.9.3 FDP_IFF.2.3

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

10.6.9.4 FDP_IFF.2.4

ФБО должны предоставлять следующее [назначение: *список дополнительных возможностей ПФБ*].

10.6.9.5 FDP_IFF.2.5

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

10.6.9.6 FDP_IFF.2.6

ФБО должны явно запрещать информационный поток, основываясь на следующих правилах: [назначение: *основанные на атрибутах безопасности правила, которые явно запрещают информационные потоки*].

10.6.9.7 FDP_IFF.2.7

ФБО должны осуществлять следующие отношения для любых двух допустимых атрибутов безопасности управления информационными потоками:

a) существует функция упорядочения, которая определяет для двух допустимых атрибутов безопасности, являются ли они равными, или один из них больше другого, или они несравнимы;

b) существует такая «наименьшая верхняя грань» в совокупности атрибутов безопасности, что для любых двух допустимых атрибутов безопасности найдется такой допустимый атрибут безопасности, который больше или равен двум допустимым атрибутам безопасности;

c) существует такая «наибольшая нижняя грань» в совокупности атрибутов безопасности, что для любых двух допустимых атрибутов безопасности найдется такой допустимый атрибут безопасности, который не больше этих двух допустимых атрибутов безопасности.

10.6.10 FDP_IFF.3 Ограничение неразрешенных информационных потоков

Иерархический для: нет подчиненных компонентов.

Зависимости: AVA_CCA.1 Анализ скрытых каналов

FDP_IFC.1 Ограниченное управление информационными потоками

10.6.10.1 FDP_IFF.3.1

ФБО должны осуществлять [назначение: ПФБ управления информационными потоками], чтобы ограничить интенсивность [назначение: *типы неразрешенных информационных потоков*] до [назначение: *максимальная интенсивность*].

10.6.11 FDP_IFF.4 Частичное устранение неразрешенных информационных потоков

Иерархический для: FDP_IFF.3 Ограничение неразрешенных информационных потоков

Зависимости: AVA_CCA.1 Анализ скрытых каналов

FDP_IFC.1 Ограниченное управление информационными потоками

10.6.11.1 FDP_IFF.4.1

ФБО должны осуществлять [назначение: *ПФБ управления информационными потоками*], чтобы ограничить интенсивность [назначение: *типы неразрешенных информационных потоков*] до [назначение: *максимальная интенсивность*].

10.6.11.2 FDP_IFF.4.2

ФБО должны предотвращать [назначение: *типы неразрешенных информационных потоков*].

10.6.12 FDP_IFF.5 Отсутствие неразрешенных информационных потоков

Иерархический для: FDP_IFF.4 Частичное устранение неразрешенных информационных потоков

Зависимости: AVA_CCA.3 Исчерпывающий анализ скрытых каналов

FDP_IFC.1 Ограниченное управление информационными потоками

10.6.12.1 FDP_IFF.5.1

ФБО должны обеспечивать, чтобы не существовало неразрешенных информационных потоков, способных нарушить [назначение: *имя ПФБ управления информационными потоками*].

10.6.13 FDP_IFF.6 Мониторинг неразрешенных информационных потоков

Иерархический для: нет подчиненных компонентов.

Зависимости: AVA_CCA.1 Анализ скрытых каналов

FDP_IFC.1 Ограниченное управление информационными потоками

10.6.13.1 FDP_IFF.6.1

ФБО должны осуществлять [назначение: *ПФБ управления информационными потоками*], чтобы отследить [назначение: *типы неразрешенных информационных потоков*], когда они превышают [назначение: *максимальная интенсивность*].

10.7 Импорт данных из-за пределов действия ФБО (FDP_ITC)

10.7.1 Характеристика семейства

Семейство FDP_ITC определяет механизмы для передачи данных пользователя в ОО так, чтобы эти данные имели соответствующие атрибуты безопасности и защиту. В семействе также рассматриваются ограничения на импорт и определение требуемых атрибутов безопасности, а также интерпретация атрибутов безопасности, ассоциированных с данными пользователя.

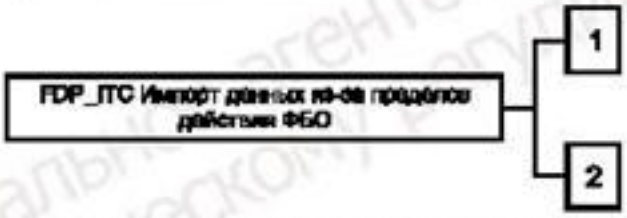

Рисунок 29 — Ранжирование компонентов семейства FDP_ITC

10.7.2 Ранжирование компонентов

Компонент FDP_ITC.1 «Импорт данных пользователя без атрибутов безопасности» содержит требования, чтобы атрибуты безопасности правильно представляли данные пользователя и поставлялись независимо от объекта.

Компонент FDP_ITC.2 «Импорт данных пользователя с атрибутами безопасности» содержит требования, чтобы атрибуты безопасности правильно представляли данные пользователя, а также точно и однозначно ассоциировались с данными пользователя, импортируемыми из-за пределов ОДФ.

10.7.3 Управление: FDP_ITC.1, FDP_ITC.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) модификация дополнительных правил управления, используемых для импорта.

10.7.4 Аудит: FDP_ITC.1, FDP_ITC.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: успешный импорт данных пользователя, включая любые атрибуты безопасности;

b) базовый: все попытки импортировать данные пользователя, включая любые атрибуты безопасности;

c) детализированный: спецификация атрибутов безопасности для импортируемых данных пользователя, выполненная уполномоченным пользователем.

10.7.5 FDP_ITC.1 Импорт данных пользователя без атрибутов безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
FMT_MSA.3 Инициализация статических атрибутов

10.7.5.1 FDP_ITC.1.1

ФБО должны осуществлять [назначение: *политики ФБ управления доступом и/или политики ФБ управления информационными потоками*] при импорте данных пользователя, контролируемом ПФБ, из-за пределов ОДФ.

10.7.5.2 FDP_ITC.1.2

ФБО должны игнорировать любые атрибуты безопасности, ассоциированные с данными пользователя, при импорте из-за пределов ОДФ.

10.7.5.3 FDP_ITC.1.3

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

10.7.6 FDP_ITC.2 Импорт данных пользователя с атрибутами безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
[FTP_ITC.1 Доверенный канал передачи между ФБО или
FTP_TRP.1 Доверенный маршрут]
FPT_TDC.1 Базовая согласованность данных ФБО между ФБО

10.7.6.1 FDP_ITC.2.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*] при импорте данных пользователя, контролируемом ПФБ, из-за пределов ОДФ.

10.7.6.2 FDP_ITC.2.2

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

10.7.6.3 FDP_ITC.2.3

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

10.7.6.4 FDP_ITC.2.4

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

10.7.6.5 FDP_ITC.2.5

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

10.8 Передача в пределах ОО (FDP_ITT)

10.8.1 Характеристика семейства

Семейство FDP_ITT содержит требования, связанные с защитой данных пользователя при их передаче между различными частями ОО по внутреннему каналу. Этим данное семейство отличается от семейств FDP_UCT «Защита конфиденциальности данных пользователя при передаче между ФБО» и FDP_UIT «Защита целостности данных пользователя при передаче между ФБО», которые обеспечивают защиту данных пользователя при их передаче между различными ФБО по внешнему каналу, а также от семейств FDP_ETC «Экспорт данных за пределы действия ФБО» и FDP_ITC «Импорт данных из-за пределов действия ФБО», которые связаны с передачей данных за пределы или из-за пределов действия ФБО.

10.8.2 Ранжирование компонентов

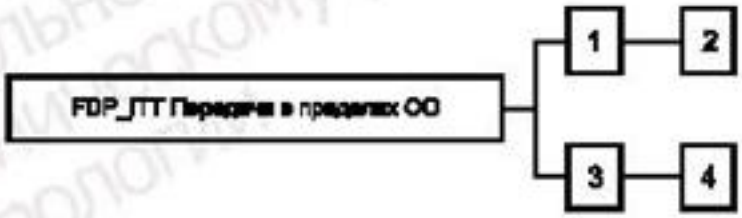

Рисунок 30 — Ранжирование компонентов семейства FDP_ITT

FDP_ITT.1 «Базовая защита внутренней передачи» содержит требование, чтобы данные пользователя были защищены при передаче между частями ОО.

FDP_ITT.2 «Разделение передачи по атрибутам» содержит в дополнение к первому компоненту требование разделения данных, основанного на значениях присущих ПФБ атрибутов.

FDP_ITT.3 «Мониторинг целостности» содержит требование, чтобы ФБ контролировала данные пользователя, передаваемые между частями ОО, на наличие идентифицированных ошибок целостности.

FDP_ITT.4 «Мониторинг целостности по атрибутам» расширяет третий компонент, разрешая дополнительную форму мониторинга целостности с разделением, использующим присущие ПФБ атрибуты.

10.8.3 Управление: FDP_ITT.1, FDP_ITT.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) если ФБО предоставляют несколько методов защиты данных пользователя во время передачи между физически разделенными частями ОО, то ФБО могут предусмотреть предопределенную роль с выбором метода, который будет использован.

10.8.4 Управление: FDP_ITT.3, FDP_ITT.4

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) возможность настройки спецификации действий, предпринимаемых после обнаружения ошибки целостности.

10.8.5 Аудит: FDP_ITT.1, FDP_ITT.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешные передачи данных пользователя с идентификацией используемого метода защиты;

b) базовый: все попытки передать данные пользователя с идентификацией используемого метода защиты и любых произошедших ошибок.

10.8.6 Аудит: FDP_ITT.3, FDP_ITT.4

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешные передачи данных пользователя с идентификацией используемого метода защиты целостности;

b) базовый: все попытки передать данные пользователя с идентификацией используемого метода защиты целостности и любых произошедших ошибок;

c) базовый: несанкционированные попытки изменить метод защиты целостности;

d) детализированный: действия, предпринимаемые после обнаружения ошибки целостности.

10.8.7 FDP_ITT.1 Базовая защита внутренней передачи

Иерархический для: нет подчиненных компонентов.

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

10.8.7.1 FDP_ITT.1.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], чтобы предотвращать [выбор: *раскрытие, модификация, недоступность*] данных пользователя при их передаче между физически разделенными частями ОО.

10.8.8 FDP_ITT.2 Разделение передачи по атрибутам

Иерархический для: FDP_ITT.1 Базовая защита внутренней передачи

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

10.8.8.1 FDP_ITT.2.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], чтобы предотвращать [выбор: *раскрытие, модификация, недоступность*] данных пользователя при их передаче между физически разделенными частями ОО.

10.8.8.2 FDP_ITT.2.2

ФБО должны разделять данные, контролируемые ПФБ, при их передаче между физически разделенными частями ОО, основываясь на значениях следующих атрибутов: [назначение: *атрибуты безопасности, которые требуют разделения данных*].

10.8.9 FDP_ITT.3 Мониторинг целостности

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
FDP_ITT.1 Базовая защита внутренней передачи

10.8.9.1 FDP_ITT.3.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], чтобы контролировать данные пользователя, передаваемые между физически разделенными частями ОО, на наличие следующих ошибок: [назначение: *ошибки целостности*].

10.8.9.2 FDP_ITT.3.2

При обнаружении ошибки целостности данных ФБО должны [назначение: *действия при ошибке целостности*].

10.8.10 FDP_ITT.4 Мониторинг целостности по атрибутам

Иерархический для: FDP_ITT.3 Мониторинг целостности

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
FDP_ITT.2 Разделение передачи по атрибутам

10.8.10.1 FDP_ITT.4.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], чтобы контролировать данные пользователя, передаваемые между физически разделенными частями ОО, на наличие следующих ошибок: [назначение: *ошибки целостности*], **основываясь на следующих атрибутах: [назначение: *атрибуты безопасности, которые требуют разделения каналов передачи*].**

10.8.10.2 FDP_ITT.4.2

При обнаружении ошибки целостности данных ФБО должны [назначение: *действия при ошибке целостности*].

10.9 Защита остаточной информации (FDP_RIP)

10.9.1 Характеристика семейства

Семейство FDP_RIP связано с необходимостью обеспечения последующей недоступности удаленной информации и отсутствия во вновь созданных объектах информации, которую не следует оставлять доступной. Это семейство содержит требования защиты информации, которая уже логически удалена или исключена из рассмотрения, но физически все еще может присутствовать в пределах ОО.

10.9.2 Ранжирование компонентов

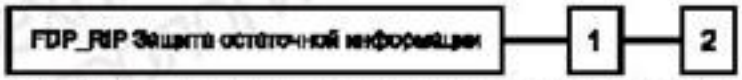

Рисунок 31 — Ранжирование компонентов семейства FDP_RIP

FDP_RIP.1 «Ограниченная защита остаточной информации» содержит требование, чтобы ФБО обеспечили недоступность содержания всей остаточной информации любых ресурсов для определенного подмножества объектов в ОДФ при распределении или освобождении ресурса.

FDP_RIP.2 «Полная защита остаточной информации» содержит требование, чтобы ФБО обеспечили недоступность содержания всей остаточной информации любых ресурсов для всех объектов при распределении или освобождении ресурса.

10.9.3 Управление: FDP_RIP.1, FDP_RIP.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) возможность настройки, когда выполнять защиту остаточной информации (то есть при распределении или освобождении) в пределах ОО.

10.9.4 Аудит: FDP_RIP.1, FDP_RIP.2

Нет событий, для которых следует предусмотреть возможность аудита.

10.9.5 FDP_RIP.1 Ограниченная защита остаточной информации

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

10.9.5.1 FDP_RIP.1.1

ФБО должны обеспечивать недоступность любого предыдущего информационного содержания ресурсов при [выбор: *распределение ресурса, освобождение ресурса*] для следующих объектов: [назначение: *список объектов*].

10.9.6 FDP_RIP.2 Полная защита остаточной информации

Иерархический для: FDP_RIP.1 Ограниченная защита остаточной информации

Зависимости: нет зависимостей.

10.9.6.1 FDP_RIP.2.1

ФБО должны обеспечивать недоступность любого предыдущего информационного содержания ресурсов при [выбор: *распределение ресурса, освобождение ресурса*] для **всех объектов**.

10.10 Откат (FDP_ROL)

10.10.1 Характеристика семейства

Операция отката включает в себя отмену последней операции или ряда операций, ограниченных некоторым пределом (например, периодом времени), и возврат к предшествующему известному состоянию. Откат предоставляет возможность отменить результаты операции или ряда операций, чтобы сохранить целостность данных пользователя.

10.10.2 Ранжирование компонентов

Рисунок 32 — Ранжирование компонентов семейства FDP_ROL

FDP_ROL.1 «Базовый откат» связан с необходимостью вернуть обратно или отменить ограниченное число операций в определенных пределах.

FDP_ROL.2 «Расширенный откат» связан с необходимостью вернуть обратно или отменить все операции в определенных пределах.

10.10.3 Управление: FDP_ROL.1, FDP_ROL.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) возможность настройки предела ограничений, до которого возможен откат в пределах ОО;

b) разрешение выполнять операцию отката только вполне определенным ролям.

10.10.4 Аудит: FDP_ROL.1, FDP_ROL.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: все успешные операции отката;

b) базовый: все попытки выполнить операции отката;

c) детализированный: все попытки выполнить операции отката с идентификацией типов операций, отмененных при откате.

10.10.5 FDP_ROL.1 Базовый откат

Иерархический для: нет подчиненных компонентов.

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

10.10.5.1 FDP_ROL.1.1

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

10.10.5.2 FDP_ROL.1.2

ФБО должны разрешать откат в пределах [назначение: *ограничение выполнения отката*].

10.10.6 FDP_ROL.2 Расширенный откат

Иерархический для: FDP_ROL.1 Базовый откат

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

10.10.6.1 FDP_ROL.2.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], чтобы разрешать откат **всех операций** на [назначение: *список объектов*].

10.10.6.2 FDP_ROL.2.2

ФБО должны разрешать откат в пределах [назначение: *ограничение выполнения отката*].

10.11 Целостность хранимых данных (FDP_SDI)

10.11.1 Характеристика семейства

Семейство FDP_SDI содержит требования, связанные с защитой данных пользователя во время их хранения в пределах ОДФ. Ошибки целостности могут воздействовать на данные пользователя, хранимые как в оперативной памяти, так и на запоминающих устройствах. Это семейство отличается от семейства FDP_ITT «Передача в пределах ОО», которое защищает данные пользователя от ошибок целостности во время их передачи в пределах ОО.

10.11.2 Ранжирование компонентов

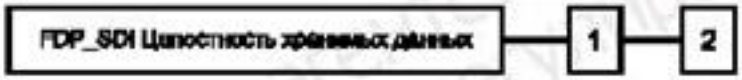

Рисунок 33 — Ранжирование компонентов семейства FDP_SDI

FDP_SDI.1 «Мониторинг целостности хранимых данных» содержит требование, чтобы ФБ контролировала данные пользователя, хранимые в пределах ОДФ, на наличие идентифицированных ошибок целостности.

FDP_SDI.2 «Мониторинг целостности хранимых данных и предпринимаемые действия» дополняет предыдущий компонент действиями, предпринимаемыми после обнаружения ошибок.

10.11.3 Управление: FDP_SDI.1

Действия по управлению не предусмотрены.

10.11.4 Управление: FDP_SDI.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) возможность настройки действий, предпринимаемых после обнаружения ошибки целостности.

10.11.5 Аудит: FDP_SDI.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешные попытки проверки целостности данных пользователя с индикацией результатов проверки;

b) базовый: все попытки проверки целостности данных пользователя с индикацией результатов проверки, если она была выполнена;

c) детализированный: тип обнаруженной ошибки целостности.

10.11.6 Аудит: FDP_SDI.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешные попытки проверки целостности данных пользователя с индикацией результатов проверки;

b) базовый: все попытки проверки целостности данных пользователя с индикацией результатов проверки, если она была выполнена;

c) детализированный: тип обнаруженной ошибки целостности;

d) детализированный: действия, предпринимаемые при обнаружении ошибки целостности.

10.11.7 FDP_SDI.1 Мониторинг целостности хранимых данных

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

10.11.7.1 FDP_SDI.1.1

ФБО должны контролировать данные пользователя, хранимые в пределах ОДФ, на наличие [назначение: *ошибки целостности*] для всех объектов, основываясь на следующих атрибутах: [назначение: *атрибуты данных пользователя*].

10.11.8 FDP_SDI.2 Мониторинг целостности хранимых данных и предпринимаемые действия

Иерархический для: FDP_SDI.1 Мониторинг целостности хранимых данных

Зависимости: нет зависимостей.

10.11.8.1 FDP_SDI.2.1

ФБО должны контролировать данные пользователя, хранимые в пределах ОДФ, на наличие [назначение: *ошибки целостности*] для всех объектов, основываясь на следующих атрибутах: [назначение: *атрибуты данных пользователя*].

10.11.8.2 FDP_SDI.2.2

При обнаружении ошибки целостности данных ФБО должны [назначение: *предпринимаемые действия*].

10.12 Защита конфиденциальности данных пользователя при передаче между ФБО (FDP_UCT)

10.12.1 Характеристика семейства

Семейство FDP_UCT определяет требования по обеспечению конфиденциальности данных пользователя при их передаче с использованием внешнего канала между различными ОО или пользователями различных ОО.

10.12.2 Ранжирование компонентов

Рисунок 34 — Ранжирование компонентов семейства FDP_UCT

Цель компонента FDP_UCT.1 «Базовая конфиденциальность обмена данными» состоит в предоставлении защиты от раскрытия данных пользователя во время их передачи.

10.12.3 Управление: FDP_UCT.1

Действия по управлению не предусмотрены.

10.12.4 Аудит: FDP_UCT.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: идентификатор любого пользователя или субъекта, использующего механизмы обмена данными;

b) базовый: идентификатор любого неуполномоченного пользователя или субъекта, делающего попытку использовать механизмы обмена данными;

c) базовый: ссылка на имена или другую информацию индексации, полезную при идентификации данных пользователя, которые были переданы или получены. Может включать в себя атрибуты безопасности, ассоциированные с информацией.

10.12.5 FDP_UCT.1 Базовая конфиденциальность обмена данными

Иерархический для: нет подчиненных компонентов.

Зависимости: [FTP_ITC.1 Доверенный канал передачи между ФБО или
FTP_TRP.1 Доверенный маршрут]
[FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]

10.12.5.1 FDP_UCT.1.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], предоставляющую возможность [выбор: *отправление, получение*] данных пользователя способом, защищенным от несанкционированного раскрытия.

10.13 Защита целостности данных пользователя при передаче между ФБО (FDP_UIT)

10.13.1 Характеристика семейства

Семейство FDP_UIT определяет требования по обеспечению целостности данных пользователя при их передаче между ФБО и другим доверенным продуктом ИТ, а также для их восстановления при обнаружении ошибок. Как минимум, данное семейство контролирует целостность данных пользователя на предмет модификации. Кроме того, семейство поддерживает различные способы исправления обнаруженных ошибок целостности.

10.13.2 Ранжирование компонентов

Рисунок 35 — Ранжирование компонентов семейства FDP_UIT

FDP_UIT.1 «Целостность передаваемых данных» связан с обнаружением модификации, удалений, вставок и повторения передаваемых данных пользователя.

FDP_UIT.2 «Восстановление переданных данных источником» связан с восстановлением исходных данных пользователя, полученных ФБО, с помощью источника — доверенного продукта ИТ.

FDP_UIT.3 «Восстановление переданных данных получателем» связан с самостоятельным восстановлением исходных данных пользователя, полученных ФБО, без какой-либо помощи источника — доверенного продукта ИТ.

10.13.3 Управление: FDP_UIT.1, FDP_UIT.2, FDP_UIT.3

Действия по управлению не предусмотрены.

10.13.4 Аудит: FDP_UIT.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: идентификатор любого пользователя или субъекта, использующего механизмы обмена данными;

b) базовый: идентификатор любого пользователя или субъекта, пытающегося использовать механизмы обмена данными пользователя, но не уполномоченного делать это таким образом;

c) базовый: ссылка на имена или другую информацию индексации, полезную при идентификации данных пользователя, которые были переданы или получены. Может включать в себя атрибуты безопасности, ассоциированные с данными пользователя;

d) базовый: любые идентифицированные попытки блокировать передачу данных пользователя;

e) детализированный: типы и/или результаты любых обнаруженных модификаций переданных данных пользователя.

10.13.5 Аудит: FDP_UIT.2, FDP_UIT.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: идентификатор любого пользователя или субъекта, использующего механизмы обмена данными;

b) минимальный: успешное восстановление после ошибок, включая тип обнаруженной ошибки;

c) базовый: идентификатор любого пользователя или субъекта, пытающегося использовать механизмы обмена данными пользователя, но не уполномоченного делать это таким образом;

d) базовый: ссылка на имена или другую информацию индексации, полезную при идентификации данных пользователя, которые были переданы или получены. Может включать в себя атрибуты безопасности, ассоциированные с данными пользователя;

e) базовый: любые идентифицированные попытки блокировать передачу данных пользователя;

f) детализированный: типы и/или результаты любых обнаруженных модификаций переданных данных пользователя.

10.13.6 FDP_UIT.1 Целостность передаваемых данных

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
[FTP_ITC.1 Доверенный канал передачи между ФБО или
FTP_TRP.1 Доверенный маршрут]

10.13.6.1 FDP_UIT.1.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], предоставляющую возможность [выбор: *отправление, получение*] данных пользователя способом, защищенным от следующих ошибок: [выбор: *модификация, удаление, вставка, повторение*].

10.13.6.2 FDP_UIT.1.2

ФБО должны быть способны определять после получения данных пользователя, произошли ли следующие ошибки: [выбор: *модификация, удаление, вставка, повторение*].

10.13.7 FDP_UIT.2 Восстановление переданных данных источником

Иерархический для: нет подчиненных компонентов.

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
FDP_UIT.1 Целостность передаваемых данных
FTP_ITC.1 Доверенный канал передачи между ФБО

10.13.7.1 FDP_UIT.2.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], предоставляющую возможность восстановления после [назначение: *список потенциально исправляемых ошибок*] с помощью источника — доверенного продукта ИТ.

10.13.8 FDP_UIT.3 Восстановление переданных данных получателем

Иерархический для: FDP_UIT.2 Восстановление переданных данных источником

Зависимости: [FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
FDP_UIT.1 Целостность передаваемых данных
FTP_ITC.1 Доверенный канал передачи между ФБО

10.13.8.1 FDP_UIT.3.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом и/или ПФБ управления информационными потоками*], предоставляющую возможность восстановления после [назначение: *список потенциально исправляемых ошибок*] **без какой-либо помощи источника — доверенного продукта ИТ**.

11 Класс FIA. Идентификация и аутентификация

Семейства класса FIA содержат требования к функциям установления и верификации заявленного идентификатора пользователя.

Идентификация и аутентификация требуются для обеспечения ассоциации пользователей с соответствующими атрибутами безопасности (такими как идентификатор, группы, роли, уровни безопасности или целостности).

Однозначная идентификация уполномоченных пользователей и правильная ассоциация атрибутов безопасности с пользователями и субъектами критичны для осуществления принятых политик безопасности. Семейства этого класса связаны с определением и верификацией идентификаторов пользователей, определением их полномочий на взаимодействие с ОО, а также с правильной ассоциацией атрибутов безопасности с каждым уполномоченным пользователем. Эффективность требований других классов (таких как «Защита данных пользователя», «Аудит безопасности») во многом зависит от правильно проведенных идентификации и аутентификации пользователей.

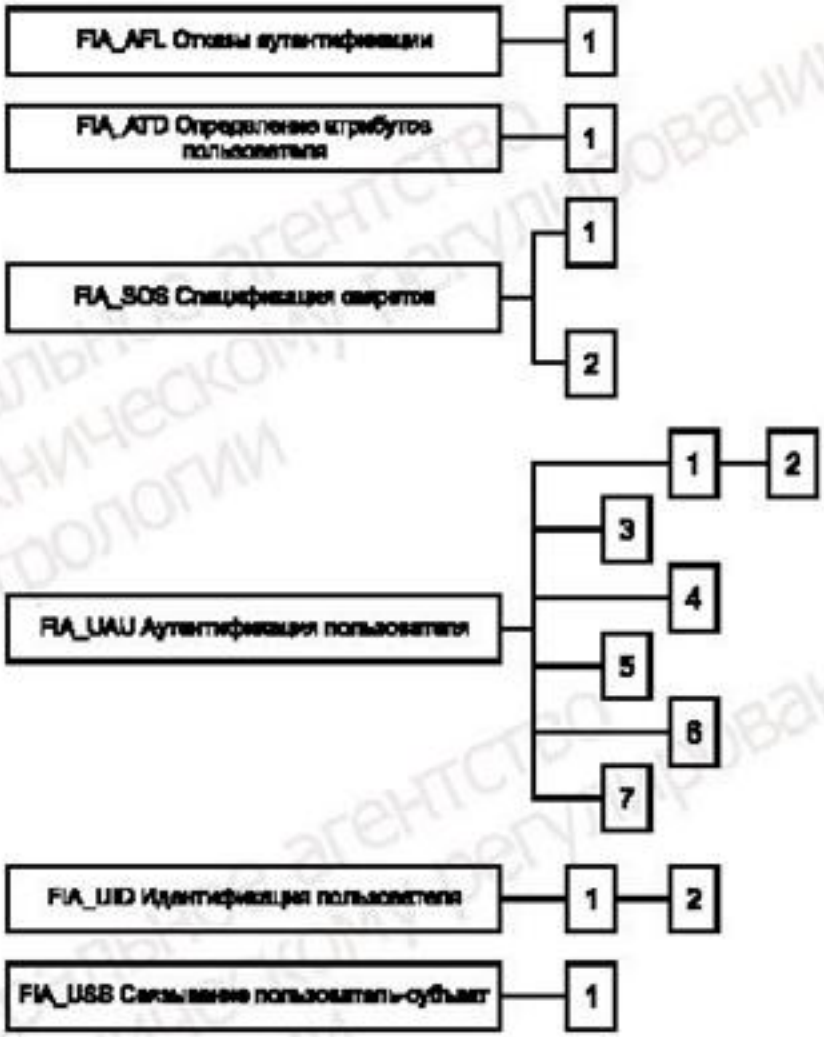

Рисунок 36 — Декомпозиция класса FIA «Идентификация и аутентификация»

11.1 Отказы аутентификации (FIA_AFL)

11.1.1 Характеристика семейства

Семейство FIA_AFL содержит требования к определению числа неуспешных попыток аутентификации и к действиям ФБО при превышении ограничений на неуспешные попытки аутентификации. Параметрами, определяющими возможное число попыток аутентификации, среди прочих могут быть число попыток и допустимый интервал времени.

11.1.2 Ранжирование компонентов

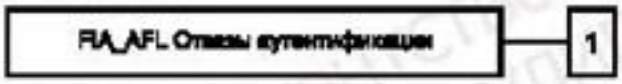

Рисунок 37 — Ранжирование компонентов семейства FIA_AFL

FIA_AFL.1 «Обработка отказов аутентификации» содержит требование, чтобы ФБО были способны прервать процесс открытия сеанса после определенного числа неуспешных попыток аутентификации пользователя. Также требуется, чтобы после прерывания процесса открытия сеанса ФБО были способны блокировать учетные данные пользователя или место входа (например, рабочую станцию), с которого выполнялись попытки, до наступления определенного администратором условия.

11.1.3 Управление: FIA_AFL.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление ограничениями для неуспешных попыток аутентификации;

b) управление действиями, предпринимаемыми при неуспешной аутентификации.

11.1.4 Аудит: FIA_AFL.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: достижение ограничения неуспешных попыток аутентификации и предпринятые действия (например блокирование терминала), а также, при необходимости, последующее восстановление нормального состояния (например деблокирование терминала).

11.1.5 FIA_AFL.1 Обработка отказов аутентификации

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UAU.1 Выбор момента аутентификации

11.1.5.1 FIA_AFL.1.1

ФБО должны обнаруживать, когда произойдет [выбор: *[назначение: положительное целое число], устанавливаемое администратором положительное целое число в пределах [назначение: диапазон допустимых значений]*] неуспешных попыток аутентификации, относящихся к [назначение: список событий аутентификации].

11.1.5.2 FIA_AFL.1.2

При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить [назначение: *список действий*].

11.2 Определение атрибутов пользователя (FIA_ATD)

11.2.1 Характеристика семейства

Все уполномоченные пользователи могут помимо идентификатора пользователя иметь другие атрибуты безопасности, применяемые при осуществлении ПБО. Семейство FIA_ATD определяет требования для ассоциации атрибутов безопасности с пользователями в соответствии с необходимостью поддержки ПБО.

11.2.2 Ранжирование компонентов

Рисунок 38 — Ранжирование компонентов семейства FIA_ATD

FIA_ATD.1 «Определение атрибутов пользователя» позволяет поддерживать атрибуты безопасности пользователя для каждого пользователя индивидуально.

11.2.3 Управление: FIA_ATD.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) уполномоченный администратор может быть способен определять дополнительные атрибуты безопасности для пользователей, если это указано в операции назначения.

11.2.4 Аудит: FIA_ATD.1

Нет событий, для которых следует предусмотреть возможность аудита.

11.2.5 FIA_ATD.1 Определение атрибутов пользователя

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

11.2.5.1 FIA_ATD.1.1

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

11.3 Спецификация секретов (FIA_SOS)

11.3.1 Характеристика семейства

Семейство FIA_SOS определяет требования к механизмам, которые реализуют определенную метрику качества для предоставляемых секретов и генерируют секреты, соответствующие определенной метрике.

11.3.2 Ранжирование компонентов

Рисунок 39 — Ранжирование компонентов семейства FIA_SOS

FIA_SOS.1 «Верификация секретов» содержит требование, чтобы ФБО верифицировали, отвечают ли секреты определенной метрике качества.

FIA_SOS.2 «Генерация секретов ФБО» содержит требование, чтобы ФБО были способны генерировать секреты, отвечающие определенной метрике качества.

11.3.3 Управление: FIA_SOS.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление метрикой, используемой для верификации секретов.

11.3.4 Управление: FIA_SOS.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление метрикой, используемой при генерации секретов.

11.3.5 Аудит: FIA_SOS.1, FIA_SOS.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: отклонение ФБО любого проверенного секрета;

b) базовый: отклонение или принятие ФБО любого проверенного секрета;

c) детализированный: идентификация любых изменений заданных метрик качества.

11.3.6 FIA_SOS.1 Верификация секретов

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

11.3.6.1 FIA_SOS.1.1

ФБО должны предоставлять механизм для верификации того, что секреты соответствуют [назначение: *определенная метрика качества*].

11.3.7 FIA_SOS.2 Генерация секретов ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

11.3.7.1 FIA_SOS.2.1

ФБО должны предоставлять механизм генерации секретов, соответствующих [назначение: *определенная метрика качества*].

11.3.7.2 FIA_SOS.2.2

ФБО должны быть способны использовать генерируемые ими секреты для [назначение: *список функций ФБО*].

11.4 Аутентификация пользователя (FIA_UAU)

11.4.1 Характеристика семейства

Семейство FIA_UAU определяет типы механизмов аутентификации пользователя, предоставляемые ФБО. Оно также определяет те атрибуты, на которых необходимо базировать механизмы аутентификации пользователя.

11.4.2 Ранжирование компонентов

Рисунок 40 — Ранжирование компонентов семейства FIA_UAU

FIA_UAU.1 «Выбор момента аутентификации» позволяет пользователю выполнить некоторые действия до аутентификации пользователя.

FIA_UAU.2 «Аутентификация до любых действий пользователя» содержит требование, чтобы пользователи были аутентифицированы прежде, чем ФБО даст им возможность предпринимать какие-либо действия.

FIA_UAU.3 «Аутентификация, защищенная от подделок» содержит требование, чтобы механизм аутентификации был способен выявить аутентификационные данные, которые были фальсифицированы или скопированы, и предотвратить их использование.

FIA_UAU.4 «Механизмы одноразовой аутентификации» содержит требование наличия механизма аутентификации, который оперирует аутентификационными данными одноразового использования.

FIA_UAU.5 «Сочетание механизмов аутентификации» содержит требование предоставления и применения различных механизмов аутентификации пользователей в особых случаях.

FIA_UAU.6 «Повторная аутентификация» содержит требование возможности определения событий, при которых необходима повторная аутентификация пользователя.

FIA_UAU.7 «Аутентификация с защищенной обратной связью» содержит требование, чтобы во время аутентификации пользователю предоставлялась строго ограниченная информация о ней.

11.4.3 Управление: FIA_UAU.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление аутентификационными данными администратором;

b) управление аутентификационными данными пользователем, ассоциированным с этими данными;

c) управление списком действий, которые могут быть предприняты до того, как пользователь аутентифицирован.

11.4.4 Управление: FIA_UAU.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление аутентификационными данными администратором;

b) управление аутентификационными данными пользователем, ассоциированным с этими данными.

11.4.5 Управление: FIA_UAU.3, FIA_UAU.4, FIA_UAU.7

Действия по управлению не предусмотрены.

11.4.6 Управление: FIA_UAU.5

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление механизмами аутентификации;

b) управление правилами аутентификации.

11.4.7 Управление: FIA_UAU.6

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление запросом на повторную аутентификацию, если для уполномоченного администратора предусмотрена возможность такого запроса.

11.4.8 Аудит: FIA_UAU.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: неуспешное использование механизма аутентификации;

b) базовый: все случаи использования механизма аутентификации;

c) детализированный: все действия при посредничестве ФБО до аутентификации пользователя.

11.4.9 Аудит: FIA_UAU.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: неуспешное использование механизма аутентификации;

b) базовый: все случаи использования механизма аутентификации.

11.4.10 Аудит: FIA_UAU.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: обнаружение фальсифицированных аутентификационных данных;

b) базовый: все безотлагательно предпринимаемые меры и результаты проверок на фальсифицированные данные.

11.4.11 Аудит: FIA_UAU.4

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: попытки повторного использования аутентификационных данных.

11.4.12 Аудит: FIA_UAU.5

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: итоговое решение по аутентификации;

b) базовый: результат действия каждого активизированного механизма вместе с итоговым решением.

11.4.13 Аудит: FIA_UAU.6

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: неуспешная повторная аутентификации;

b) базовый: все попытки повторной аутентификации.

11.4.14 Аудит: FIA_UAU.7

Нет событий, для которых следует предусмотреть возможность аудита.

11.4.15 FIA_UAU.1 Выбор момента аутентификации

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UID.1 Выбор момента идентификации

11.4.15.1 FIA_UAU.1.1

ФБО должны допускать выполнение [назначение: *список действий, выполняемых при посредничестве ФБО*] от имени пользователя, прежде чем пользователь аутентифицирован.

11.4.15.2 FIA_UAU.1.2

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

11.4.16 FIA_UAU.2 Аутентификация до любых действий пользователя

Иерархический для: FIA_UAU.1 Выбор момента аутентификации

Зависимости: FIA_UID.1 Выбор момента идентификации

11.4.16.1 FIA_UAU.2.1

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

11.4.17 FIA_UAU.3 Аутентификация, защищенная от подделок

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

11.4.17.1 FIA_UAU.3.1

ФБО должны [выбор: *обнаруживать, предотвращать*] применение любым пользователем ФБО аутентификационных данных, которые были подделаны.

11.4.17.2 FIA_UAU.3.2

ФБО должны [выбор: *обнаруживать, предотвращать*] применение любым пользователем ФБО аутентификационных данных, которые были скопированы у любого другого пользователя ФБО.

11.4.18 FIA_UAU.4 Механизмы одноразовой аутентификации

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

11.4.18.1 FIA_UAU.4.1

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

11.4.19 FIA_UAU.5 Сочетание механизмов аутентификации

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

11.4.19.1 FIA_UAU.5.1

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

11.4.19.2 FIA_UAU.5.2

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

11.4.20 FIA_UAU.6 Повторная аутентификация

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

11.4.20.1 FIA_UAU.6.1

ФБО должны повторно аутентифицировать пользователя при [назначение: *список условий, при которых требуется повторная аутентификация*].

11.4.21 FIA_UAU.7 Аутентификация с защищенной обратной связью

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UAU.1 Выбор момента аутентификации

11.4.21.1 FIA_UAU.7.1

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

11.5 Идентификация пользователя (FIA_UID)

11.5.1 Характеристика семейства

Семейство FIA_UID определяет условия, при которых от пользователей требуется идентифицировать себя до выполнения при посредничестве ФБО каких-либо других действий, требующих идентификации пользователя.

11.5.2 Ранжирование компонентов

Рисунок 41 — Ранжирование компонентов семейства FIA_UID

FIA_UID.1 «Выбор момента идентификации» позволяет пользователю выполнить некоторые действия перед своей идентификацией с использованием ФБО.

FIA_UID.2 «Идентификация до любых действий пользователя» содержит требование, чтобы пользователи идентифицировали себя прежде, чем ФБО позволят им предпринимать какие-либо действия.

11.5.3 Управление: FIA_UID.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление идентификаторами пользователей;

b) управление списком действий, если уполномоченный администратор может изменять действия, разрешенные до идентификации.

11.5.4 Управление: FIA_UID.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление идентификаторами пользователей.

11.5.5 Аудит: FIA_UID.1, FIA_UID.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: неуспешное использование механизма идентификации пользователя, включая представленный идентификатор пользователя;

b) базовый: все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя.

11.5.6 FIA_UID.1 Выбор момента идентификации

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

11.5.6.1 FIA_UID.1.1

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

11.5.6.2 FIA_UID.1.2

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

11.5.7 FIA_UID.2 Идентификация до любых действий пользователя

Иерархический для: FIA_UID.1 Выбор момента идентификации

Зависимости: нет зависимостей.

11.5.7.1 FIA_UID.2.1

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

11.6 Связывание пользователь-субъект (FIA_USB)

11.6.1 Характеристика семейства

Для работы с ОО аутентифицированный пользователь обычно активизирует какой-либо субъект. Атрибуты безопасности этого пользователя ассоциируются (полностью или частично) с этим субъектом. Семейство FIA_USB определяет требования по созданию и сопровождению ассоциации атрибутов безопасности пользователя с субъектом, действующим от имени пользователя.

11.6.2 Ранжирование компонентов

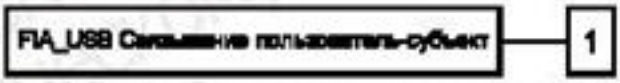

Рисунок 42 — Ранжирование компонентов семейства FIA_USB

FIA_USB.1 «Связывание пользователь-субъект» требует спецификации каких-либо правил, определяющих ассоциацию между атрибутами пользователя и атрибутами субъекта, в которые они отображаются.

11.6.3 Управление: FIA_USB.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) определение уполномоченным администратором атрибутов безопасности субъекта, задаваемых по умолчанию;

b) изменение уполномоченным администратором атрибутов безопасности субъекта.

11.6.4 Аудит: FIA_USB.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: неуспешное связывание атрибутов безопасности пользователя с субъектом (например, при создании субъекта);

b) базовый: успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом (например, успешное или неуспешное создание субъекта).

11.6.5 FIA_USB.1 Связывание пользователь-субъект

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_ATD.1 Определение атрибутов пользователя

11.6.5.1 FIA_USB.1.1

ФБО должны ассоциировать соответствующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя: [назначение: *список атрибутов безопасности пользователя*].

11.6.5.2 FIA_USB.1.2

ФБО должны осуществлять следующие правила исходной ассоциации атрибутов безопасности пользователей с субъектами, действующими от имени пользователей: [назначение: *правила исходной ассоциации атрибутов*].

11.6.5.3 FIA_USB.1.3

ФБО должны осуществлять следующие правила управления изменениями атрибутов безопасности пользователей, ассоциированными с субъектами, действующими от имени пользователей: [назначение: *правила изменения атрибутов*]

12 Класс FMT. Управление безопасностью

Класс FMT предназначен для спецификации управления некоторыми аспектами ФБО: атрибутами безопасности, данными и отдельными функциями. Могут быть установлены различные роли управления, а также определено их взаимодействие, например распределение обязанностей.

Класс FMT позволяет решать следующие задачи:

a) управление данными ФБО, которые включают в себя, например предупреждающие сообщения;

b) управление атрибутами безопасности, которые включают в себя, например списки управления доступом и перечни возможностей;

c) управление функциями из числа ФБО, которое включает в себя, например выбор функций, а также правил или условий, влияющих на режим выполнения ФБО;

d) определение ролей безопасности.

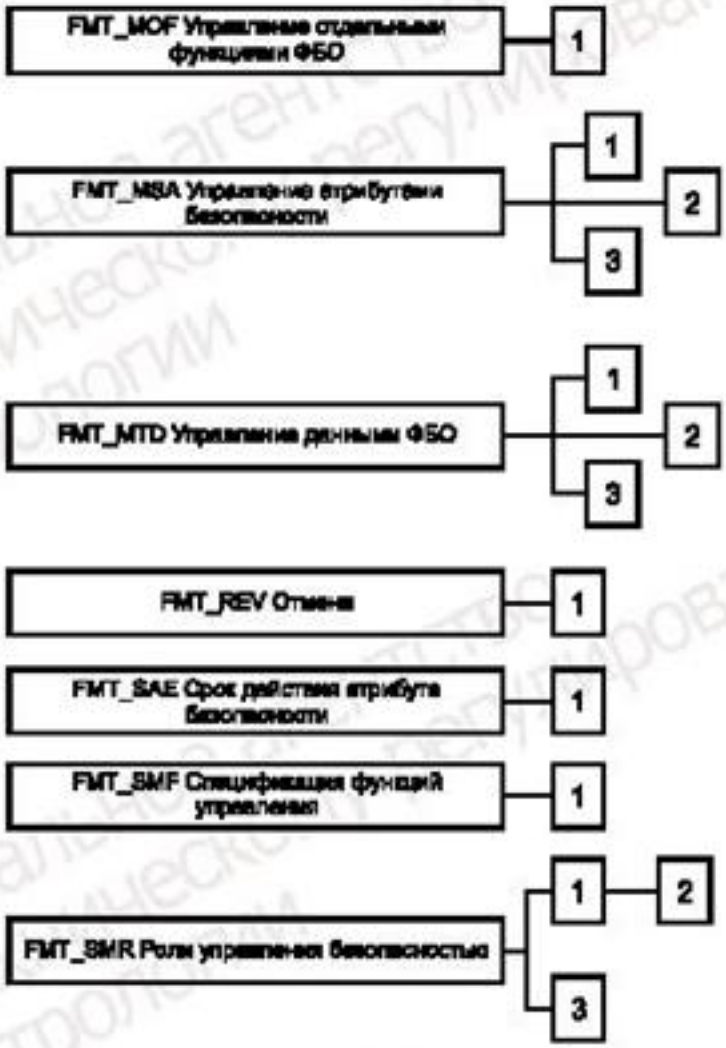

Рисунок 43 — Декомпозиция класса FMT «Управление безопасностью»

12.1 Управление отдельными функциями ФБО (FMT_MOF)

12.1.1 Характеристика семейства

Семейство FMT_MOF позволяет уполномоченным пользователям управлять функциями из числа ФБО. К ним относятся, например функции аудита и аутентификации.

12.1.2 Ранжирование компонентов

Рисунок 44 — Ранжирование компонентов семейства FMT_MOF

FMT_MOF.1 «Управление режимом выполнения функций безопасности» позволяет уполномоченным пользователям (ролям) управлять режимом выполнения функций из числа ФБО, использующих правила или предусматривающих определенные условия, которыми можно управлять.

12.1.3 Управление: FMT_MOF.1

Для функций управления из класса FMT может рассматриваться следующее действие:

a) управление группой ролей, которые могут взаимодействовать с функциями из числа ФБО.

12.1.4 Аудит: FMT_MOF.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: все модификации режима выполнения функций из числа ФБО.

12.1.5 FMT_MOF.1 Управление режимом выполнения функций безопасности

Иерархический для: нет подчиненных компонентов.

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

12.1.5.1 FMT_MOF.1.1

ФБО должны предоставлять возможность [выбор: *определять режим выполнения, отключать, подключать, модифицировать режим выполнения*] функций [назначение: *список функций*] только [назначение: *уполномоченные идентифицированные роли*].

12.2 Управление атрибутами безопасности (FMT_MSA)

12.2.1 Характеристика семейства

Семейство FMT_MSA позволяет уполномоченным пользователям управлять атрибутами безопасности. Такое управление может включать в себя возможности просмотра и модификации атрибутов безопасности.

12.2.2 Ранжирование компонентов

Рисунок 45 — Ранжирование компонентов семейства FMT_MSA

FMT_MSA.1 «Управление атрибутами безопасности» позволяет уполномоченным пользователям (ролям) управлять определенными атрибутами безопасности.

FMT_MSA.2 «Безопасные значения атрибутов безопасности» обеспечивает, чтобы значения, присвоенные атрибутам безопасности, были допустимы по безопасности.

FMT_MSA.3 «Инициализация статических атрибутов» обеспечивает, чтобы значения атрибутов безопасности по умолчанию являлись по сути разрешающими либо ограничительными.

12.2.3 Управление: FMT_MSA.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление группой ролей, которые могут оперировать атрибутами безопасности.

12.2.4 Управление: FMT_MSA.2

Действия по управлению не предусмотрены.

12.2.5 Управление: FMT_MSA.3

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление группой ролей, которые могут определять начальные значения;

b) управление установкой разрешающих или ограничительных значений по умолчанию для данной ПФБ управления доступом.

12.2.6 Аудит: FMT_MSA.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: все модификации значений атрибутов безопасности.

12.2.7 Аудит: FMT_MSA.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: все предлагаемые и отклоненные значения атрибутов безопасности;

b) детализированный: все предлагаемые и принятые безопасные значения атрибутов безопасности.

12.2.8 Аудит: FMT_MSA.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: модификации настройки по умолчанию разрешающих или ограничительных правил;

b) базовый: все модификации начальных значений атрибутов безопасности.

12.2.9 FMT_MSA.1 Управление атрибутами безопасности

Иерархический для: нет подчиненных компонентов.

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

12.2.9.1 FMT_MSA.1.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом, ПФБ управления информационными потоками*], предоставляющую возможность [выбор: *изменять значения по умолчанию, запрашивать, модифицировать, удалять* [назначение: *другие операции*] атрибуты безопасности [назначение: *список атрибутов безопасности*] только [назначение: *уполномоченные идентифицированные роли*].

12.2.10 FMT_MSA.2 Безопасные значения атрибутов безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: ADV_SPM.1 Неформальная модель политики безопасности ОО
[FDP_ACC.1 Ограниченное управление доступом или
FDP_IFC.1 Ограниченное управление информационными потоками]
FMT_MSA.1 Управление атрибутами безопасности
FMT_SMR.1 Роли безопасности

12.2.10.1 FMT_MSA.2.1

ФБО должны обеспечивать присвоение атрибутам безопасности только безопасных значений.

12.2.11 FMT_MSA.3 Инициализация статических атрибутов

Иерархический для: нет подчиненных компонентов.

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

12.2.11.1 FMT_MSA.3.1

ФБО должны осуществлять [назначение: *ПФБ управления доступом, ПФБ управления информационными потоками*], предусматривающую [выбор (выбрать одно из): *ограничительные, разрешающие, другие свойства*] значений по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ.

12.2.11.2 FMT_MSA.3.2

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

12.3 Управление данными ФБО (FMT_MTD)

12.3.1. Характеристика семейства

Семейство FMT_MTD позволяет уполномоченным пользователям (ролям) управлять данными ФБО. Примеры данных ФБО: информация аудита, текущее значение времени, конфигурация системы, другие параметры конфигурации ФБО.

12.3.2 Ранжирование компонентов

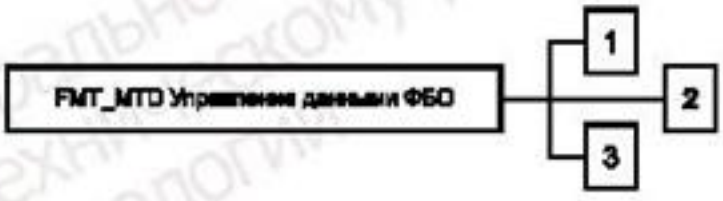

Рисунок 46 — Ранжирование компонентов семейства FMT_MTD

FMT_MTD.1 «Управление данными ФБО» позволяет уполномоченным пользователям управлять данными ФБО.

FMT_MTD.2 «Управление ограничениями данных ФБО» определяет действия, предпринимаемые при достижении или превышении ограничений данных ФБО.

FMT_MTD.3 «Безопасные данные ФБО» обеспечивает, чтобы значения, присвоенные данным ФБО, были допустимы по безопасности.

12.3.3 Управление: FMT_MTD.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление группой ролей, которые могут оперировать данными ФБО.

12.3.4 Управление: FMT_MTD.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление группой ролей, которые могут оперировать ограничениями данных ФБО.

12.3.5 Управление: FMT_MTD.3

Действия по управлению не предусмотрены.

12.3.6 Аудит: FMT_MTD.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) базовый: все модификации значений данных ФБО.

12.3.7 Аудит: FMT_MTD.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) базовый: все модификации ограничений данных ФБО;

b) базовый: все модификации действий, предпринимаемых при нарушениях ограничений.

12.3.8 Аудит: FMT_MTD.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: все отклоненные значения данных ФБО.

12.3.9 FMT_MTD.1 Управление данными ФБО

Иерархический для: нет подчиненных компонентов.

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

12.3.9.1 FMT_MTD.1.1

ФБО должны предоставлять возможность [выбор: *изменение значений по умолчанию, запрос, модификация, удаление, очистка,* [назначение: *другие операции*]] следующих данных [назначение: *список данных ФБО*] только [назначение: *уполномоченные идентифицированные роли*].

12.3.10 FMT_MTD.2 Управление ограничениями данных ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: FMT_MTD.1 Управление данными ФБО
FMT_SMR.1 Роли безопасности

12.3.10.1 FMT_MTD.2.1

ФБО должны предоставлять возможность определения ограничений для [назначение: *список данных ФБО*] только [назначение: *уполномоченные идентифицированные роли*].

12.3.10.2 FMT_MTD.2.2

ФБО должны предпринимать следующие действия при достижении или превышении данными ФБО установленных выше ограничений: [назначение: *предпринимаемые действия*].

12.3.11 FMT_MTD.3 Безопасные данные ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: ADV_SPM.1 Неформальная модель политики безопасности ОО
FMT_MTD.1 Управление данными ФБО

12.3.11.1 FMT_MTD.3.1

ФБО должны обеспечивать присвоение данным ФБО только безопасных значений.

12.4 Отмена (FMT_REV)

12.4.1 Характеристика семейства

Семейство FMT_REV связано с отменой атрибутов безопасности различных сущностей в пределах ОО.

12.4.2 Ранжирование компонентов

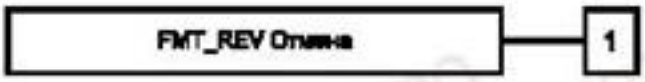

Рисунок 47 — Ранжирование компонентов семейства FMT_REV

FMT_REV.1 «Отмена» предусматривает отмену атрибутов безопасности, осуществляемую в некоторый момент времени.

12.4.3 Управление: FMT_REV.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление группой ролей, которые могут вызывать отмену атрибутов безопасности;

b) управление списками пользователей, субъектов, объектов и других ресурсов, для которых возможна отмена;

c) управление правилами отмены.

12.4.4 Аудит: FMT_REV.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: неуспешная отмена атрибутов безопасности;

b) базовый: все попытки отменить атрибуты безопасности.

12.4.5 FMT_REV.1 Отмена

Иерархический для: нет подчиненных компонентов.

Зависимости: FMT_SMR.1 Роли безопасности

12.4.5.1 FMT_REV.1.1

ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с [выбор: *пользователи, субъекты, объекты, [назначение: другие дополнительные ресурсы]*], в пределах ОДФ только [назначение: *уполномоченные идентифицированные роли*].

12.4.5.2 FMT_REV.1.2

ФБО должны осуществлять правила [назначение: правила отмены].

12.5 Срок действия атрибута безопасности (FMT_SAE)

12.5.1 Характеристика семейства

Семейство FMT_SAE связано с возможностью установления срока действия атрибутов безопасности.

12.5.2 Ранжирование компонентов

Рисунок 48 — Ранжирование компонентов семейства FMT_SAE

FMT_SAE.1 «Ограниченная по времени авторизация» предоставляет возможность уполномоченному пользователю устанавливать срок действия определенных атрибутов безопасности.

12.5.3 Управление: FMT_SAE.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление списком атрибутов безопасности с назначенным сроком действия;

b) предпринимаемые по истечении назначенного срока действия.

12.5.4 Аудит: FMT_SAE.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: назначение срока действия для атрибута;

b) базовый: действия, предпринятые по истечении назначенного срока.

12.5.5 FMT_SAE.1 Ограниченная по времени авторизация

Иерархический для: нет подчиненных компонентов.

Зависимости: FMT_SMR.1 Роли безопасности
FPT_STM.1 Надежные метки времени

12.5.5.1 FMT_SAE.1.1

ФБО должны предоставлять возможность назначать срок действия для [назначение: *список атрибутов безопасности, для которых предусмотрено установление срока действия*] только [назначение: *идентифицированные уполномоченные роли*].

12.5.5.2 FMT_SAE.1.2

Для каждого из этих атрибутов безопасности ФБО должны быть способны к [назначение: *список действий, предпринимаемых для каждого атрибута безопасности*] по истечении его срока действия.

12.6 Спецификация функций управления (FMT_SMF)

12.6.1 Характеристика семейства

Семейство FMT_SMF позволяет специфицировать функции управления, предоставляемые ОО. Функции управления предоставляют ИФБО, который позволяет администраторам определять параметры управления функционированием ОО в части аспектов, относящихся к безопасности, например атрибуты защиты данных, атрибуты защиты ОО, атрибуты аудита, атрибуты идентификации и аутентификации. Функции управления также включают в себя функции, выполняемые операторами для обеспечения непрерывной работы ОО, такие как резервирование и восстановление. Данное семейство используется совместно с другими компонентами из класса FMT «Управление безопасностью»: компонент из этого семейства предусматривает наличие функций управления, а другие семейства из класса FMT «Управление безопасностью» накладывают ограничения на возможность использования этих функций управления.

12.6.2 Ранжирование компонентов

Рисунок 49 — Ранжирование компонентов семейства FMT_SMF

FMT_SMF.1 «Спецификация функций управления» требует, чтобы ФБО предоставляли конкретные функции управления.

12.6.3 Управление FMT_SMF.1

Действия по управлению не предусмотрены.

12.6.4 Аудит FMT_SMF.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: Использование функций управления.

12.6.5 FMT_SMF.1 Спецификация функций управления

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

12.6.5.1 FMT_SMF.1.1

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

12.7 Роли управления безопасностью (FMT_SMR)

12.7.1 Характеристика семейства

Семейство FMT_SMR предназначено для управления назначением различных ролей пользователям. Возможности этих ролей по управлению безопасностью описаны в других семействах этого класса.

12.7.2 Ранжирование компонентов

Рисунок 50 — Ранжирование компонентов семейства FMT_SMR

FMT_SMR.1 «Роли безопасности» определяет роли, относящиеся к безопасности и распознаваемые ФБО.

FMT_SMR.2 «Ограничения на роли безопасности» определяет, что в дополнение к определению ролей имеются правила, управляющие отношениями между ролями.

FMT_SMR.3 «Принятие ролей» содержит требование, чтобы принятие роли производилось только через явный запрос к ФБО.

12.7.3 Управление: FMT_SMR.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление группой пользователей — исполнителей роли.

12.7.4 Управление: FMT_SMR.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление группой пользователей — исполнителей роли;

b) управление условиями, которым должны удовлетворять роли.

12.7.5 Управление: FMT_SMR.3

Действия по управлению не предусмотрены.

12.7.6 Аудит: FMT_SMR.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: модификация группы пользователей — исполнителей роли;

b) детализированный: каждое использование прав, предоставленных ролью.

12.7.7 Аудит: FMT_SMR.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: модификация в группе пользователей — исполнителей роли;

b) минимальный: неуспешные попытки использовать роль вследствие ограничений, накладываемых на роли;

c) детализированный: каждое использование прав, предоставленных ролью.

12.7.8 Аудит: FMT_SMR.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: конкретные запросы на принятие роли.

12.7.9 FMT_SMR.1 Роли безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UID.1 Выбор момента идентификации

12.7.9.1 FMT_SMR.1.1

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

12.7.9.2 FMT_SMR.1.2

ФБО должны быть способны ассоциировать пользователей с ролями.

12.7.10 FMT_SMR.2 Ограничения на роли безопасности

Иерархический для: FMT_SMR.1 Роли безопасности

Зависимости: FIA_UID.1 Выбор момента идентификации

12.7.10.1 FMT_SMR.2.1

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

12.7.10.2 FMT_SMR.2.2

ФБО должны быть способны ассоциировать пользователей с ролями.

12.7.10.3 FMT_SMR.2.3

ФБО должны обеспечивать, чтобы условия [назначение: *условия для различных ролей*] удовлетворялись.

12.7.11 FMT_SMR.3 Принятие ролей

Иерархический для: нет подчиненных компонентов.

Зависимости: FMT_SMR.1 Роли безопасности

12.7.11.1 FMT_SMR.3.1

ФБО должны требовать явный запрос для принятия следующих ролей [назначение: *список ролей*].

13 Класс FPR. Приватность

Класс FPR содержит требования приватности. Эти требования предоставляют пользователю защиту от раскрытия его идентификатора и злоупотребления этим другими пользователями.

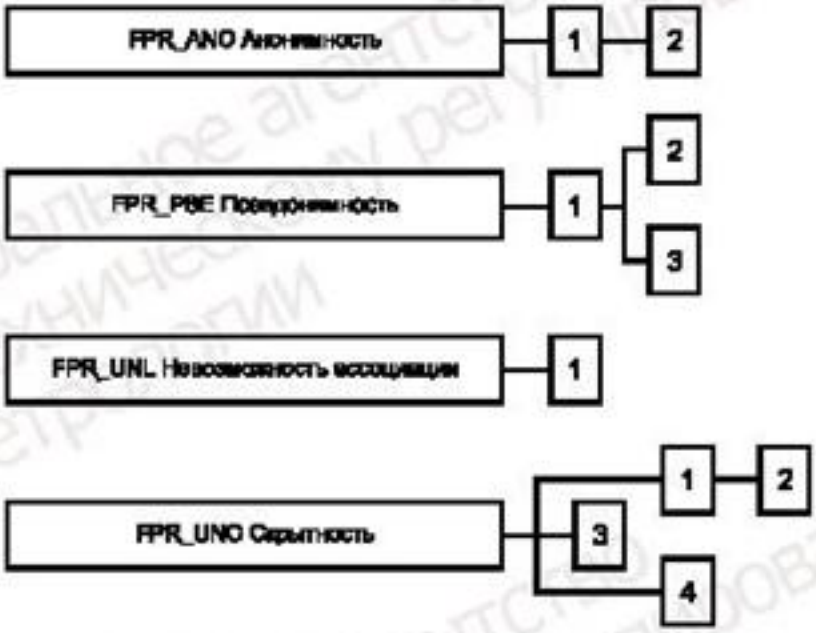

Рисунок 51 — Декомпозиция класса FPR «Приватность»

13.1 Анонимность (FPR_ANO)

13.1.1 Характеристика семейства

Семейство FPR_ANO обеспечивает пользователю возможность использовать ресурс или услугу ОО без раскрытия своего идентификатора. Требования семейства предоставляют защиту идентификатора пользователя. Семейство не предназначено для защиты идентификаторов субъектов.

13.1.2 Ранжирование компонентов

Рисунок 52 — Ранжирование компонентов семейства FPR_ANO

FPR_ANO.1 «Анонимность» содержит требование, чтобы другие пользователи или субъекты не могли определить идентификатор пользователя, связанного с субъектом или операцией.

FPR_ANO.2 «Анонимность без запроса информации» расширяет требования FPR_ANO.1 «Анонимность», обеспечивая, чтобы ФБО не запрашивали идентификатор пользователя.

13.1.3 Управление: FPR_ANO.1, FPR_ANO.2

Действия по управлению не предусмотрены.

13.1.4 Аудит: FPR_ANO.1, FPR_ANO.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: обращение к механизму анонимности.

13.1.5 FPR_ANO.1 Анонимность

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

13.1.5.1 FPR_ANO.1.1

ФБО должны обеспечивать, чтобы [назначение: *совокупность пользователей и/или субъектов*] была не способна определить подлинное имя пользователя, связанного с [назначение: *список субъектов и/или операций, и/или объектов*].

13.1.6 FPR_ANO.2 Анонимность без запроса информации

Иерархический для: FPR_ANO.1 Анонимность

Зависимости: нет зависимостей.

13.1.6.1 FPR_ANO.2.1

ФБО должны обеспечивать, чтобы [назначение: *совокупность пользователей и/или субъектов*] была не способна определить подлинное имя пользователя, связанного с [назначение: *список субъектов и/или операций, и/или объектов*].

13.1.6.2 FPR_ANO.2.2

ФБО должны предоставлять [назначение: *список услуг*] для [назначение: *список субъектов*] без запроса какой-либо ссылки на подлинное имя пользователя.

13.2 Псевдонимность (FPR_PSE)

13.2.1 Характеристика семейства

Семейство FPR_PSE обеспечивает пользователю возможность использовать ресурс или услугу без раскрытия своего идентификатора, оставаясь в то же время ответственным за это использование.

13.2.2 Ранжирование компонентов

Рисунок 53 — Ранжирование компонентов семейства FPR_PSE

FPR_PSE.1 «Псевдонимность» содержит требование, чтобы некоторая совокупность пользователей и/или субъектов была не способна определить идентификатор пользователя, связанного с субъектом или операцией, но в то же время этот пользователь оставался ответственным за свои действия.

FPR_PSE.2 «Обратимая псевдонимность» содержит требование, чтобы ФБО предоставили возможность определить первоначальный идентификатор пользователя, основываясь на представленном псевдониме.

FPR_PSE.3 «Альтернативная псевдонимность» содержит требование, чтобы при создании псевдонима для идентификатора пользователя ФБО следовали определенным правилам.

13.2.3 Управление: FPR_PSE.1, FPR_PSE.2, FPR_PSE.3

Действия по управлению не предусмотрены.

13.2.4 Аудит: FPR_PSE.1, FPR_PSE.2, FPR_PSE.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: идентификатор субъекта/пользователя, который потребовал раскрытия идентификатора пользователя.

13.2.5 FPR_PSE.1 Псевдонимность

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

13.2.5.1 FPR_PSE.1.1

ФБО должны обеспечивать, чтобы [назначение: *совокупность пользователей и/или субъектов*] была не способна определять подлинное имя пользователя, связанного с [назначение: *список субъектов и/или операций, и/или объектов*].

13.2.5.2 FPR_PSE.1.2

ФБО должны быть способны предоставлять [назначение: *число псевдонимов*] псевдонимов подлинного имени пользователя для [назначение: *список субъектов*].

13.2.5.3 FPR_PSE.1.3

ФБО должны быть способны [выбор (выбрать одно из): *определять псевдоним пользователя, принимать псевдоним от пользователя*] и верифицировать его соответствие [назначение: *метрика псевдонимов*].

13.2.6 FPR_PSE.2 Обратимая псевдонимность

Иерархический для: FPR_PSE.1 Псевдонимность

Зависимости: FIA_UID.1 Выбор момента идентификации

13.2.6.1 FPR_PSE.2.1

ФБО должны обеспечивать, чтобы [назначение: *совокупность пользователей и/или субъектов*] была не способна определять подлинное имя пользователя, связанное с [назначение: *список субъектов и/или операций, и/или объектов*].

13.2.6.2 FPR_PSE.2.2

ФБО должны быть способны предоставлять [назначение: *число псевдонимов*] псевдонимов подлинного имени пользователя для [назначение: *список субъектов*].

13.2.6.3 FPR_PSE.2.3

ФБО должны быть способны [выбор (выбрать одно из): *определять псевдоним пользователя, принимать псевдоним от пользователя*] и верифицировать его соответствие [назначение: *метрика псевдонимов*].

13.2.6.4 FPR_PSE.2.4

ФБО должны предоставлять [выбор: *уполномоченный пользователь*, [*назначение: список доверенных субъектов]*] возможность определять идентификатор пользователя по представленному псевдониму только при выполнении [назначение: *список условий*].

13.2.7 FPR_PSE.3 Альтернативная псевдонимность

Иерархический для: FPR_PSE.1 Псевдонимность

Зависимости: нет зависимостей.

13.2.7.1 FPR_PSE.3.1

ФБО должны обеспечивать, чтобы [назначение: *совокупность пользователей и/или субъектов*] была не способна определять подлинное имя пользователя, связанное с [назначение: *список субъектов и/или операций, и/или объектов*].

13.2.7.2 FPR_PSE.3.2

ФБО должны быть способны предоставлять [назначение: *число псевдонимов*] псевдонимов подлинного имени пользователя для [назначение: *список субъектов*].

13.2.7.3 FPR_PSE.3.3

ФБО должны быть способны [выбор (выбрать одно из): *определять псевдоним пользователя, принимать псевдоним от пользователя*] и верифицировать его соответствие [назначение: *метрика псевдонимов*].

13.2.7.4 FPR_PSE.3.4

ФБО должны предоставлять псевдоним для подлинного имени пользователя, который должен быть идентичен псевдониму, предоставленному ранее, при следующих условиях [назначение: *список условий*]; в противном случае предоставляемый псевдоним должен быть не связан с предоставленными ранее псевдонимами.

13.3 Невозможность ассоциации (FPR_UNL)

13.3.1 Характеристика семейства

Семейство FPR_UNL обеспечивает пользователю возможность неоднократно использовать ресурсы или услуги, не давая в то же время никому возможности связать вместе их использование.

Рисунок 54 — Ранжирование компонентов семейства FPR_UNL

13.3.2 Ранжирование компонентов

FPR_UNL.1 «Невозможность ассоциации» содержит требование, чтобы пользователи и/или субъекты были не способны определить, инициированы ли определенные операции в системе одним и тем же пользователем.

13.3.3 Управление: FPR_UNL.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление функцией предотвращения ассоциации.

13.3.4 Аудит: FPR_UNL.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: обращение к механизму предотвращения ассоциации.

13.3.5 FPR_UNL.1 Невозможность ассоциации

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

13.3.5.1 FPR_UNL.1.1

ФБО должны обеспечивать, чтобы [назначение: *совокупность пользователей и/или субъектов*] была не способна определять, что [назначение: *список операций*] [выбор: *были инициированы одним и тем же пользователем, связаны следующим образом [назначение: список соотношений]*].

13.4 Скрытность (FPR_UNO)

13.4.1 Характеристика семейства

Семейство FPR_UNO обеспечивает возможность пользователю использовать ресурс или услугу без предоставления кому-либо, в особенности третьей стороне, информации об использовании данного ресурса или данной услуги.

13.4.2 Ранжирование компонентов

Рисунок 55 — Ранжирование компонентов семейства FPR_UNO

FPR_UNO.1 «Скрытность» содержит требование, чтобы пользователи и/или субъекты не могли определить, выполняется ли операция.

FPR_UNO.2 «Распределение информации, влияющее на скрытность» содержит требование, чтобы ФБО предоставили специальные механизмы для предотвращения концентрации информации, связанной с приватностью, в пределах ОО. Такая концентрация могла бы повлиять на обеспечение скрытности при нарушениях безопасности.

FPR_UNO.3 «Скрытность без запроса информации» содержит требование, чтобы ФБО не пытались получить информацию, связанную с приватностью, что может использоваться для нарушения скрытности.

FPR_UNO.4 «Открытость для уполномоченного пользователя» содержит требование, чтобы ФБО предоставили одному или нескольким уполномоченным пользователям возможность наблюдать за использованием ресурсов и/или услуг.

13.4.3 Управление: FPR_UNO.1, FPR_UNO.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление режимом выполнения функции скрытности.

13.4.4 Управление: FPR_UNO.3

Действия по управлению не предусмотрены.

13.4.5 Управление: FPR_UNO.4

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление совокупностью уполномоченных пользователей, которые способны определить, выполнялись ли операции.

13.4.6 Аудит: FPR_UNO.1, FPR_UNO.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: обращение к механизму скрытности.

13.4.7 Аудит: FPR_UNO.3

Нет событий, для которых следует предусмотреть возможность аудита.

13.4.8 Аудит: FPR_UNO.4

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: наблюдение за использованием ресурса или услуги пользователем или субъектом.

13.4.9 FPR_UNO.1 Скрытность

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

13.4.9.1 FPR_UNO.1.1

ФБО должны обеспечивать, чтобы [назначение: *совокупность пользователей и/или субъектов*] была не способна наблюдать следующие операции [назначение: *список операций*] на [назначение: *список объектов*], выполняемые [назначение: *совокупность защищаемых пользователей и/или субъектов*].

13.4.10 FPR_UNO.2 Распределение информации, влияющее на скрытность

Иерархический для: FPR_UNO.1 Скрытность

Зависимости: нет зависимостей

13.4.10.1 FPR_UNO.2.1

ФБО должны обеспечивать, чтобы [назначение: *совокупность пользователей и/или субъектов*] была не способна наблюдать следующие операции [назначение: *список операций*] на [назначение: *список объектов*], выполняемые [назначение: *совокупность защищаемых пользователей и/или субъектов*].

13.4.10.2 FPR_UNO.2.2

ФБО должны распределять [назначение: *информация, связанная со скрытностью*] среди различных частей ОО так, чтобы во время существования информации выполнялись следующие условия: [назначение: *список условий*].

13.4.11 FPR_UNO.3 Скрытность без запроса информации

Иерархический для: нет подчиненных компонентов.

Зависимости: FPR_UNO.1 Скрытность

13.4.11.1 FPR_UNO.3.1

ФБО должны предоставлять [назначение: *список услуг*] для [назначение: *список субъектов*] без запроса каких-либо ссылок на [назначение: *информация, связанная с приватностью*].

13.4.12 FPR_UNO.4 Открытость для уполномоченного пользователя

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей

13.4.12.1 FPR_UNO.4.1

ФБО должны предоставлять [назначение: *совокупность уполномоченных пользователей*] возможность наблюдать за использованием [назначение: *список ресурсов и/или услуг*].

14 Класс FPT. Защита ФБО

Класс FPT содержит семейства функциональных требований, связанных с целостностью и управлением механизмами, реализованными в ФБО (не завися при этом от особенностей ПБО), а также с целостностью данных ФБО (не завися от специфического содержания данных ПБО). В некотором смысле, компоненты семейств этого класса дублируют компоненты из класса FDP и могут даже использовать одни и те же механизмы. Однако класс FDP «Защита данных пользователя» сфокусирован на защите данных пользователя, в то время как класс FPT «Защита ФБО» — на защите данных ФБО. Фактически, компоненты из класса FPT необходимы для обеспечения требований невозможности нарушения и обхода политик ФБ данного ОО.

В рамках данного класса выделяют три важные составные части ФБО:

1) *абстрактная машина ФБО*, то есть виртуальная или физическая машина, на которой выполняется оцениваемая реализация ФБО;

2) *реализация ФБО*, которая выполняется на абстрактной машине и реализует механизмы, осуществляющие ПБО;

3) *данные ФБО*, которые являются административными базами данных, управляющими осуществлением ПБО.

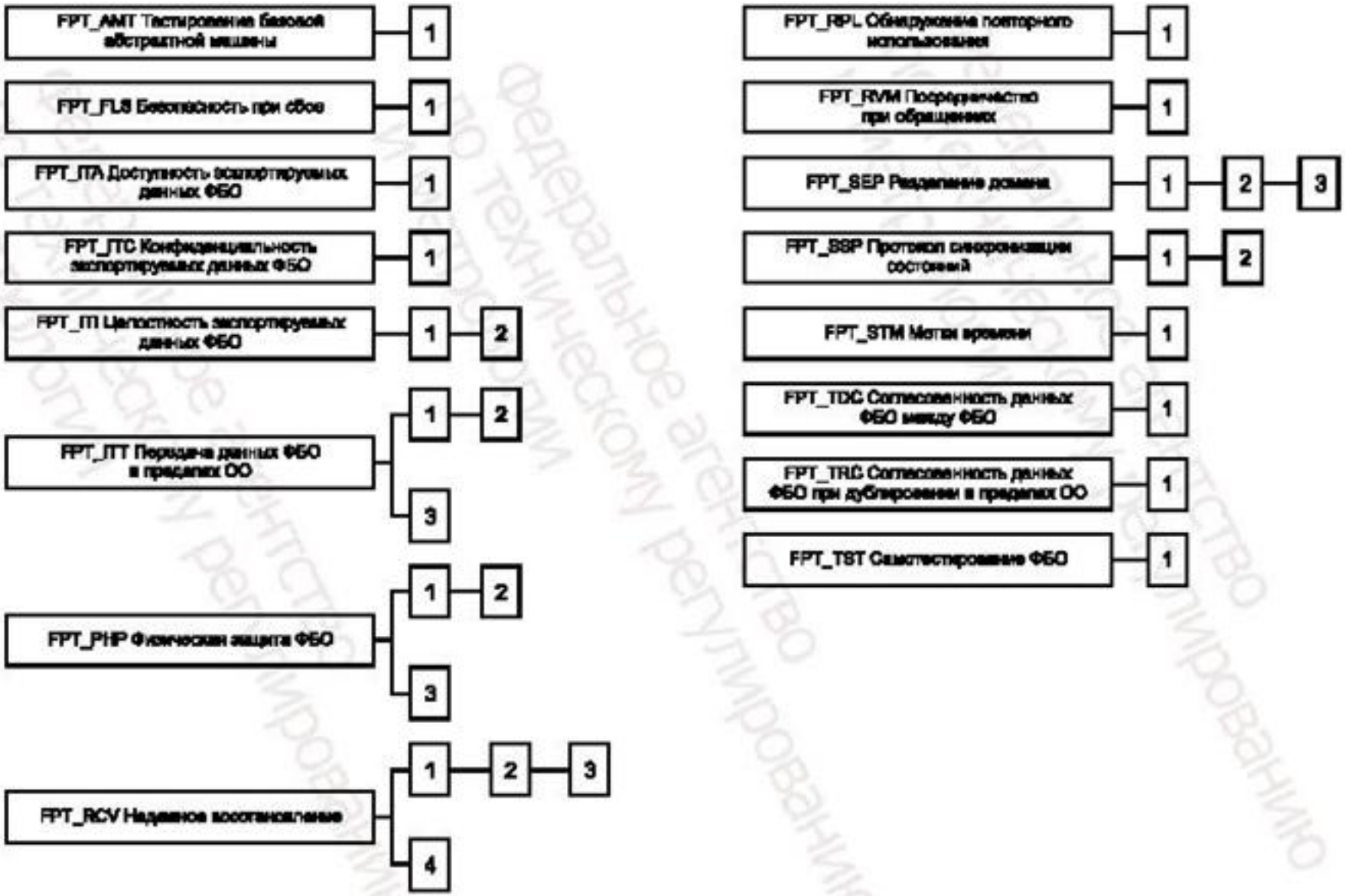

Рисунок 56 — Декомпозиция класса FPT «Защита ФБО»

Федеральное агентство по техническому регулированию и метрологии

14.1 Тестирование базовой абстрактной машины (FPT_AMT)

14.1.1 Характеристика семейства

Семейство FPT_AMT определяет требования к выполнению тестирования ФБО, демонстрирующего предположения безопасности относительно базовой абстрактной машины, на которую полагаются ФБО. «Абстрактная» машина может быть как платформой аппаратных/программно-аппаратных средств, так и некоторым известным и прошедшим оценку сочетанием аппаратных/программных средств, действующим как виртуальная машина.

14.1.2 Ранжирование компонентов

Рисунок 57 — Ранжирование компонентов семейства FPT_AMT

FPT_AMT.1 «Тестирование абстрактной машины» предоставляет возможность проверки базовой абстрактной машины.

14.1.3 Управление: FPT_AMT.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление условиями, при которых происходит тестирование абстрактной машины, например, при первоначальном запуске, с постоянным интервалом, при заданных условиях;

b) управление временным интервалом (при необходимости).

14.1.4 Аудит: FPT_AMT.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: выполнение тестирования базовой машины и результаты тестирования.

14.1.5 FPT_AMT.1 Тестирование абстрактной машины

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.1.5.1 FPT_AMT.1.1

ФБО должны выполнять пакет тестовых программ [выбор: *при первоначальном запуске, периодически во время нормального функционирования, по запросу уполномоченного пользователя, [назначение: другие условия]*] для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая является базовой для ФБО.

14.2 Безопасность при сбое (FPT_FLS)

14.2.1 Характеристика семейства

Требования семейства FPT_FLS обеспечивают возможность сохранения политики безопасности ОО при идентифицированых типах сбоев ФБО.

14.2.2 Ранжирование компонентов

Рисунок 58 — Ранжирование компонентов семейства FPT_FLS

Это семейство состоит из одного компонента, FPT_FLS.1 «Сбой с сохранением безопасного состояния», содержащего требование, чтобы ФБО сохраняли безопасное состояние при идентифицированных сбоях.

14.2.3 Управление: FPT_FLS.1

Действия по управлению не предусмотрены.

14.2.4 Аудит: FPT_FLS.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: сбой ФБО.

14.2.5 FPT_FLS.1 Сбой с сохранением безопасного состояния

Иерархический для: нет подчиненных компонентов.

Зависимости: ADV_SPM.1 Неформальная модель политики безопасности ОО

14.2.5.1 FPT_FLS.1.1

ФБО должны сохранять безопасное состояние при следующих типах сбоев: [назначение: *список типов сбоев ФБО*].

14.3 Доступность экспортируемых данных ФБО (FPT_ITA)

14.3.1 Характеристика семейства

Семейство FPT_ITA определяет правила предотвращения потери доступности данных ФБО, передаваемых между ФБО и удаленным доверенным продуктом ИТ. Это могут быть, например, критичные данные ФБО, такие как пароли, ключи, данные аудита или выполняемый код ФБО.

14.3.2 Ранжирование компонентов

Рисунок 59 — Ранжирование компонентов семейства FPT_ITA

Это семейство состоит из одного компонента FPT_ITA.1 «Доступность экспортируемых данных ФБО в пределах заданной метрики», содержащего требование, чтобы ФБО обеспечили с заданной вероятностью доступность данных ФБО, предоставляемых удаленному доверенному продукту ИТ.

14.3.3 Управление: FPT_ITA.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление списком типов данных ФБО, которые должны быть доступны удаленному доверенному продукту ИТ.

14.3.4 Аудит: FPT_ITA.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: отсутствие данных ФБО, когда они запрошены ОО.

14.3.5 FPT_ITA.1 Доступность экспортируемых данных ФБО в пределах заданной метрики

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.3.5.1 FPT_ITA.1.1

ФБО должны обеспечивать доступность [назначение: *список типов данных ФБО*] для удаленного доверенного продукта ИТ в пределах [назначение: *заданная метрика доступности*] при выполнении следующих условий [назначение: *условия обеспечения доступности*].

14.4 Конфиденциальность экспортируемых данных ФБО (FPT_ITC)

14.4.1 Характеристика семейства

Семейство FPT_ITC определяет правила защиты данных ФБО от несанкционированного раскрытия при передаче между ФБО и удаленным доверенным продуктом ИТ. Это могут быть, например, критичные данные ФБО, такие как пароли, ключи, данные аудита или выполняемый код ФБО.

14.4.2 Ранжирование компонентов

Рисунок 60 — Ранжирование компонентов семейства FPT_ITC

Это семейство состоит из одного компонента FPT_ITC.1 «Конфиденциальность экспортируемых данных ФБО при передаче», содержащего требование, чтобы ФБО обеспечили защиту данных, передаваемых между ФБО и удаленным доверенным продуктом ИТ, от раскрытия при передаче.

14.4.3 Управление: FPT_ITC.1

Действия по управлению не предусмотрены.

14.4.4 Аудит: FPT_ITC.1

Нет событий, для которых следует предусмотреть возможность аудита.

14.4.5 FPT_ITC.1 Конфиденциальность экспортируемых данных ФБО при передаче

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.4.5.1 FPT_ITC.1.1

ФБО должны защищать все данные ФБО, передаваемые от ФБО к удаленному доверенному продукту ИТ, от несанкционированного раскрытия при передаче.

14.5 Целостность экспортируемых данных ФБО (FPT_ITI)

14.5.1 Характеристика семейства

Семейство FPT_ITI определяет правила защиты данных ФБО от несанкционированной модификации при передаче между ФБО и удаленным доверенным продуктом ИТ. Это могут быть, например, критичные данные ФБО, такие как пароли, ключи, данные аудита или выполняемый код ФБО.

14.5.2 Ранжирование компонентов

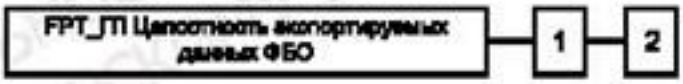

Рисунок 61 — Ранжирование компонентов семейства FPT_ITI

FPT_ITI.1 «Обнаружение модификации экспортируемых данных ФБО» позволяет обнаружить модификацию данных ФБО при передаче между ФБО и удаленным доверенным продуктом ИТ при допущении, что последнему известен используемый механизм передачи.

FPT_ITI.2 «Обнаружение и исправление модификации экспортируемых данных ФБО» позволяет удаленному доверенному продукту ИТ не только обнаружить модификацию, но и восстановить данные ФБО, модифицированные при передаче от ФБО, при допущении, что последнему известен используемый механизм передачи.

14.5.3 Управление: FPT_ITI.1

Действия по управлению не предусмотрены.

14.5.4 Управление: FPT_ITI.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление типами данных ФБО, которые ФБО следует пытаться исправить, если они модифицированы при передаче;

b) управление типами действий, которые ФБО могут предпринять, если данные ФБО модифицированы при передаче.

14.5.5 Аудит: FPT_ITI.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: обнаружение модификации передаваемых данных ФБО;

b) базовый: действия, предпринятые при обнаружении модификации передаваемых данных ФБО.

14.5.6 Аудит: FPT_ITI.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: обнаружение модификации передаваемых данных ФБО;

b) базовый: действия, предпринятые при обнаружении модификации передаваемых данных ФБО;

c) базовый: использование механизма восстановления.

14.5.7 FPT_ITI.1 Обнаружение модификации экспортируемых данных ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.5.7.1 FPT_ITI.1.1

ФБО должны предоставлять возможность обнаруживать модификацию любых данных ФБО при передаче между ФБО и удаленным доверенным продуктом ИТ в пределах следующей метрики: [назначение: *метрика модификации*].

14.5.7.2 FPT_ITI.1.2

ФБО должны предоставлять возможность верифицировать целостность всех данных ФБО при их передаче между ФБО и удаленным доверенным продуктом ИТ и выполнять [назначение: *предпринимаемые действия*], если модификация обнаружена.

14.5.8 FPT_ITI.2 Обнаружение и исправление модификации экспортируемых данных ФБО

Иерархический для: FPT_ITI.1 Обнаружение модификации экспортируемых данных ФБО

Зависимости: нет зависимостей.

14.5.8.1 FPT_ITI.2.1

ФБО должны предоставлять возможность обнаруживать модификацию любых данных ФБО при передаче между ФБО и удаленным доверенным продуктом ИТ в пределах следующей метрики: [назначение: *метрика модификации*].

14.5.8.2 FPT_ITI.2.2

ФБО должны предоставлять возможность верифицировать целостность всех данных ФБО при их передаче между ФБО и удаленным доверенным продуктом ИТ и выполнять [назначение: *предпринимаемые действия*], если модификация обнаружена.

14.5.8.3 FPT_ITI.2.3

ФБО должны предоставлять возможность исправлять [назначение: *тип модификации*] все данные ФБО, передаваемые между ФБО и удаленным доверенным продуктом ИТ.

14.6 Передача данных ФБО в пределах ОО (FPT_ITT)

14.6.1 Характеристика семейства

Семейство FPT_ITT содержит требования защиты данных ФБО при их передаче между разделенными частями ОО по внутреннему каналу.

14.6.2 Ранжирование компонентов

Рисунок 62 — Ранжирование компонентов семейства FPT_ITT

FPT_ITT.1 «Базовая защита внутренней передачи данных ФБО» содержит требование, чтобы данные ФБО были защищены при их передаче между разделенными частями ОО.

FPT_ITT.2 «Разделение данных ФБО при передаче» содержит требование, чтобы при передаче ФБО отделяли данные пользователей от данных ФБО.

FPT_ITT.3 «Мониторинг целостности данных ФБО» содержит требование, чтобы данные ФБО, передаваемые между разделенными частями ОО, контролировались на идентифицированные ошибки целостности.

14.6.3 Управление: FPT_ITT.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление типами модификации, от которых ФБО следует защищать передаваемые данные;

b) управление механизмом, используемым для обеспечения защиты данных при передаче между различными частями ФБО.

14.6.4 Управление: FPT_ITT.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление типами модификации, от которых ФБО следует защищать передаваемые данные;

b) управление механизмом, используемым для обеспечения защиты данных при передаче между различными частями ФБО;

c) управление механизмом разделения данных.

14.6.5 Управление: FPT_ITT.3

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление типами модификации, от которых ФБО следует защищать передаваемые данные;

b) управление механизмом, используемым для обеспечения защиты данных при передаче между различными частями ФБО;

c) управление типами модификации данных ФБО, которые ФБО следует пытаться обнаружить;

d) управление действиями, предпринимаемыми после обнаружения модификации.

14.6.6 Аудит: FPT_ITT.1, FPT_ITT.2

Нет событий, для которых следует предусмотреть возможность аудита.

14.6.7 Аудит: FPT_ITT.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: обнаружение модификации данных ФБО;

b) базовый: действия, предпринятые после обнаружения ошибок целостности.

14.6.8 FPT_ITT.1 Базовая защита внутренней передачи данных ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.6.8.1 FPT_ITT.1.1

ФБО должны защищать свои данные от [выбор: *раскрытие, модификация*] при их передаче между разделенными частями ОО.

14.6.9 FPT_ITT.2 Разделение данных ФБО при передаче

Иерархический для: FPT_ITT.1 Базовая защита внутренней передачи данных ФБО.

Зависимости: нет зависимостей.

14.6.9.1 FPT_ITT.2.1

ФБО должны защищать свои данные от [выбор: *раскрытие, модификация*] при их передаче между разделенными частями ОО.

14.6.9.2 FPT_ITT.2.2

ФБО должны отделять данные пользователя от данных ФБО при их передаче между разделенными частями ОО.

14.6.10 FPT_ITT.3 Мониторинг целостности данных ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: FPT_ITT.1 Базовая защита внутренней передачи данных ФБО

14.6.10.1 FPT_ITT.3.1

ФБО должны быть способны обнаруживать [выбор: *модификация данных, подмена данных, перестановка данных, удаление данных,* [назначение: *другие ошибки целостности*] в данных ФБО, передаваемых между разделенными частями ОО.

14.6.10.2 FPT_ITT.3.2

При обнаружении ошибки целостности данных ФБО должны предпринимать следующие действия: [назначение: *выполняемые действия*].

14.7 Физическая защита ФБО (FPT_PHP)

14.7.1 Характеристика семейства

Компоненты семейства FPT_PHP дают возможность ограничивать физический доступ к ФБО, а также реагировать на несанкционированную физическую модификацию или подмену реализации ФБО и противодействовать им.

Требования компонентов данного семейства обеспечивают, чтобы ФБО были защищены от физического воздействия и вмешательства. Удовлетворение требований этих компонентов позволяет получить реализацию ФБО, компонуемую и используемую способом, предусматривающим обнаружение физического воздействия или противодействие ему. Без этих компонентов защита ФБО теряет эффективность в среде, где не может быть предотвращено физическое повреждение. Это семейство также содержит требования к реакции ФБО на попытки физического воздействия на их реализацию.

14.7.2 Ранжирование компонентов

Рисунок 63 — Ранжирование компонентов семейства FPT_PHP

FPT_PHP.1 «Пассивное обнаружение физического нападения» предоставляет возможность известить о вмешательстве в устройства или элементы, реализующие ФБО. Однако оповещение о вмешательстве не действует автоматически; уполномоченному пользователю необходимо вызвать административную функцию безопасности или проверить самому, произошло ли вмешательство.

FPT_PHP.2 «Оповещение о физическом нападении» обеспечивает автоматическое оповещение о вмешательстве для установленного подмножества физических проникновений.

FPT_PHP.3 «Противодействие физическому нападению» предоставляет возможности предотвращения или противодействия физическому вмешательству в устройства и элементы, реализующие ФБО.

14.7.3 Управление: FPT_PHP.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление пользователем или ролью, которые определяют, произошло ли физическое вмешательство.

14.7.4 Управление: FPT_PHP.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление пользователем или ролью, которые получают информацию о вторжениях;

b) управление списком устройств, о вторжении в которые следует оповестить указанного пользователя или роль.

14.7.5 Управление: FPT_PHP.3

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление автоматической реакцией на физическое воздействие.

14.7.6 Аудит: FPT_PHP.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: обнаружение вторжения средствами ИТ.

14.7.7 Аудит: FPT_PHP.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: обнаружение вторжения.

14.7.8 Аудит: FPT_PHP.3

Нет событий, для которых следует предусмотреть возможность аудита.

14.7.9 FPT_PHP.1 Пассивное обнаружение физического нападения

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.7.9.1 FPT_PHP.1.1

ФБО должны обеспечивать однозначное обнаружение физического воздействия, которое может угрожать выполнению ФБО.

14.7.9.2 FPT_PHP.1.2

ФБО должны предоставлять возможность определять, произошло ли физическое воздействие на устройства или элементы, реализующие ФБО.

14.7.10 FPT_PHP.2 Оповещение о физическом нападении

Иерархический для: FPT_PHP.1 Пассивное обнаружение физической атаки

Зависимости: FMT_MOF.1 Управление режимом выполнения функций безопасности

14.7.10.1 FPT_PHP.2.1

ФБО должны обеспечивать однозначное обнаружение физического воздействия, которое может угрожать выполнению ФБО.

14.7.10.2 FPT_PHP.2.2

ФБО должны предоставлять возможность определять, произошло ли физическое воздействие на устройства или элементы, реализующие ФБО.

14.7.10.3 FPT_PHP.2.3

Для [назначение: *список устройств/элементов, реализующих ФБО, для которых требуется активное обнаружение*] ФБО должны постоянно контролировать устройства, элементы и оповещать [назначение: *назначенный пользователь или роль*], что произошло физическое воздействие на устройства или элементы, реализующие ФБО.

14.7.11 FPT_PHP.3 Противодействие физическому нападению

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.7.11.1 FPT_PHP.3.1

ФБО должны противодействовать [назначение: *сценарии физического воздействия*] на [назначение: *список устройств/элементов, реализующих ФБО*], реагируя автоматически так, чтобы предотвращать нарушение ПБО.

14.8 Надежное восстановление (FPT_RCV)

14.8.1 Характеристика семейства

Требования семейства FPT_RCV обеспечивают, чтобы ФБО могли определить отсутствие нарушения защиты ФБО при запуске и восстанавливаться без нарушения защиты после прерывания операций. Это семейство важно, потому что начальное состояние ФБО при запуске или восстановлении определяет защищенность ОО в последующем.

14.8.2 Ранжирование компонентов

Рисунок 64 — Ранжирование компонентов семейства FPT_RCV

FPT_RCV.1 «Ручное восстановление» позволяет ОО предоставить только такие механизмы возврата к безопасному состоянию, которые предполагают вмешательство человека.

FPT_RCV.2 «Автоматическое восстановление» предоставляет хотя бы для одного типа прерывания обслуживания восстановление безопасного состояния без вмешательства человека; восстановление после прерываний других типов может потребовать вмешательства человека.

FPT_RCV.3 «Автоматическое восстановление без недопустимой потери» также предусматривает автоматическое восстановление, но повышает уровень требований, препятствуя недопустимой потере защищенных объектов.

FPT_RCV.4 «Восстановление функции» предусматривает восстановление на уровне отдельных ФБ, обеспечивая их нормальное завершение после сбоя либо возврат к безопасному состоянию данных ФБО.

14.8.3 Управление: FPT_RCV.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление списком доступа к средствам восстановления в режиме аварийной поддержки.

14.8.4 Управление: FPT_RCV.2, FPT_RCV.3

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление списком доступа к средствам восстановления в режиме аварийной поддержки;

b) управление списком сбоев/прерываний обслуживания, которые будут обрабатываться автоматическими процедурами.

14.8.5 Управление: FPT_RCV. 4

Действия по управлению не предусмотрены.

14.8.6 Аудит: FPT_RCV.1, FPT_RCV.2, FPT_RCV.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: факт возникновения сбоя или прерывания обслуживания;

b) минимальный: возобновление нормальной работы;

c) базовый: тип сбоя или прерывания обслуживания.

14.8.7 Аудит: FPT_RCV. 4

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: невозможность возврата к безопасному состоянию после сбоя функции безопасности, если аудит возможен;

b) базовый: обнаружение сбоя функции безопасности, если аудит возможен.

14.8.8 FPT_RCV.1 Ручное восстановление

Иерархический для: нет подчиненных компонентов.

Зависимости: AGD_ADM.1 Руководство администратора
ADV_SPM.1 Неформальная модель политики безопасности ОО

14.8.8.1 FPT_RCV.1.1

После [назначение: *список сбоев/прерываний обслуживания*] ФБО должны переходить в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию.

14.8.9 FPT_RCV.2 Автоматическое восстановление

Иерархический для: FPT_RCV.1 Ручное восстановление

Зависимости: AGD_ADM.1 Руководство администратора
ADV_SPM.1 Неформальная модель политики безопасности ОО

14.8.9.1 FPT_RCV.2.1

Если автоматическое восстановление после [назначение: *список сбоев/прерываний обслуживания*] **невозможно,** ФБО должны переходить в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию.

14.8.9.2 FPT_RCV.2.2

Для [назначение: *список сбоев/прерываний обслуживания*] ФБО должны обеспечивать возврат ОО к безопасному состоянию с использованием автоматических процедур.

14.8.10 FPT_RCV.3 Автоматическое восстановление без недопустимой потери

Иерархический для: FPT_RCV.2 Автоматическое восстановление

Зависимости: AGD_ADM.1 Руководство администратора
ADV_SPM.1 Неформальная модель политики безопасности ОО

14.8.10.1 FPT_RCV.3.1

Если автоматическое восстановление после [назначение: *список сбоев/прерываний обслуживания*] невозможно, ФБО должны переходить в режим аварийной поддержки, который предоставляет возможность возврата ОО к безопасному состоянию.

14.8.10.2 FPT_RCV.3.2

Для [назначение: *список сбоев/прерываний обслуживания*] ФБО должны обеспечивать возврат ОО к безопасному состоянию с использованием автоматических процедур.

14.8.10.3 FPT_RCV.3.3

Функции из числа ФБО, предназначенные для преодоления последствий сбоя или прерывания обслуживания, должны обеспечивать восстановление безопасного начального состояния без превышения [назначение: *количественная мера*] потери данных ФБО или объектов в пределах ОДФ.

14.8.10.4 FPT_RCV.3.4

ФБО должны обеспечивать способность определения, какие объекты могут, а какие не могут быть восстановлены.

14.8.11 FPT_RCV.4 Восстановление функции

Иерархический для: нет подчиненных компонентов.

Зависимости: ADV_SPM.1 Неформальная модель политики безопасности ОО

14.8.11.1 FPT_RCV.4.1

ФБО должны обеспечивать следующее свойство для [назначение: *список ФБ и сценариев сбоев*]: ФБ нормально заканчивает работу или, для предусмотренных сценариев сбоев, восстанавливается ее устойчивое и безопасное состояние.

14.9 Обнаружение повторного использования (FPT_RPL)

14.9.1 Характеристика семейства

Семейство FPT_RPL связано с обнаружением повторного использования различных типов сущностей (таких как сообщения, запросы на обслуживание, ответы на запросы обслуживания) и последующими действиями по его устранению. При обнаружении повторного использования выполнение требований семейства эффективно предотвращает его.

14.9.2 Ранжирование компонентов

Рисунок 65 — Ранжирование компонентов семейства FPT_RPL

Семейство состоит из одного компонента FPT_RPL.1 «Обнаружение повторного использования», который содержит требование, чтобы ФБО были способны обнаружить повторное использование идентифицированных сущностей.

14.9.3 Управление: FPT_RPL.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление списком идентифицированных сущностей, для которых повторное использование должно быть обнаружено;

b) управление списком действий, которые необходимо предпринять при повторном использовании.

14.9.4 Аудит: FPT_RPL.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: обнаруженные нападения посредством повторного использования;

b) детализированный: предпринятые специальные действия.

14.9.5 FPT_RPL.1 Обнаружение повторного использования

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.9.5.1 FPT_RPL.1.1

ФБО должны обнаруживать повторное использование для следующих сущностей: [назначение: *список идентифицированных сущностей*].

14.9.5.2 FPT_RPL.1.2

ФБО должны выполнять [назначение: *список специальных действий*] при обнаружении повторного использования.

14.10 Посредничество при обращениях (FPT_RVM)

14.10.1 Характеристика семейства

Требования семейства FPT_RVM связаны с аспектом «постоянная готовность» традиционного монитора обращений. Цель этого семейства состоит в обеспечении для заданной ПФБ, чтобы все действия, требующие осуществления политики, проверялись ФБО на соответствие ПФБ. Если помимо этого часть ФБО, осуществляющая ПФБ, выполняет требования соответствующих компонентов из семейств FPT_SEP «Разделение домена» и ADV_INT «Внутренняя структура ФБО», то эта часть ФБО обеспечивает «монитор обращений» для этой ПФБ.

ФБО при реализации ПФБ предоставляют эффективную защиту от несанкционированных операций тогда и только тогда, когда правомочность всех потенциально осуществляемых действий (например, доступа к объектам), запрошенных субъектами, недоверенными относительно всех или именно данной ПФБ, проверяется ФБО до выполнения действий. Если действия по проверке, которые должны выполняться ФБО, выполнены неправильно или проигнорированы (обойдены), то осуществление ПФБ в целом может быть поставлено под угрозу (ее можно обойти). Тогда субъекты смогут обходить ПФБ различными способами (такими как обход проверки доступа для некоторых субъектов и объектов, обход проверки для объектов, защита которых управляется прикладными программами, сохранение права доступа после истечения установленного срока действия, обход аудита действий, подлежащих аудиту, обход аутентификации). Важно отметить, что некоторым субъектам, так называемым «доверенным субъектам» относительно одной из ПФБ, может быть непосредственно доверено осуществление этой ПФБ, предоставляя тем самым возможность обойтись без ее посредничества.

14.10.2 Ранжирование компонентов

Рисунок 66 — Ранжирование компонентов семейства FPT_RVM

Это семейство состоит только из одного компонента, FPT_RVM.1 «Невозможность обхода ПБО», который содержит требование предотвращения обхода для всех ПФБ из ПБО.

14.10.3 Управление: FPT_RVM.1

Действия по управлению не предусмотрены.

14.10.4 Аудит: FPT_RVM.1

Нет событий, для которых следует предусмотреть возможность аудита.

14.10.5 FPT_RVM.1 Невозможность обхода ПБО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.10.5.1 FPT_RVM.1.1

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

14.11 Разделение домена (FPT_SEP)

14.11.1 Характеристика семейства

Компоненты семейства FPT_SEP обеспечивают, чтобы, по меньшей мере, один домен безопасности был доступен только для собственного выполнения ФБО, и этим ФБО были бы защищены от внешнего вмешательства и искажения (например, модификации кода или структур данных ФБО) со стороны недоверенных субъектов. Выполнение требований этого семейства устанавливает такую самозащиту ФБО, что недоверенный субъект не сможет модифицировать или повредить ФБО.

Это семейство содержит следующие требования:

a) ресурсы домена безопасности ФБО («защищенного домена») и ресурсы субъектов и активных сущностей, внешних по отношению к этому домену, должны разделяться так, чтобы сущности, внешние по отношению к защищенному домену, не могли получить или модифицировать данные или код ФБО в пределах защищенного домена;

b) обмен между доменами должен управляться так, чтобы произвольный вход в защищенный домен или произвольный выход из него были невозможны;

c) параметры пользователя или прикладной программы, переданные в защищенный домен по адресу, должны проверяться относительно адресного пространства защищенного домена, а переданные по значению — относительно значений, ожидаемых этим доменом;

d) защищенные домены субъектов должны быть разделены, за исключением случаев, когда совместное использование одного домена управляется ФБО.

14.11.2 Ранжирование компонентов

Рисунок 67 — Ранжирование компонентов семейства FPT_SEP

FPT_SEP.1 «Отделение домена ФБО» обеспечивает отдельный защищенный домен для ФБО и разделение между субъектами в ОДФ.

FPT_SEP.2 «Отделение домена ПФБ» содержит требования дальнейшего разбиения защищенного домена ФБО с выделением отдельного(ых) домена(ов) для идентифицированной совокупности ПФБ, которые действуют как мониторы обращений для них, и домена для остальной части ФБО, а также доменов для частей ОО, не связанных с ФБО.

FPT_SEP.3 «Полный монитор обращений» содержит требования, чтобы имелся отдельный(ые) домен(ы) для осуществления ПБО, домен для остальной части ФБО, а также домены для частей ОО, не связанных с ФБО.

14.11.3 Управление: FPT_SEP.1, FPT_SEP.2, FPT_SEP.3

Действия по управлению не предусмотрены.

14.11.4 Аудит: FPT_SEP.1, FPT_SEP.2, FPT_SEP.3

Нет событий, для которых следует предусмотреть возможность аудита.

14.11.5 FPT_SEP.1 Отделение домена ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.11.5.1 FPT_SEP.1.1

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

14.11.5.2 FPT_SEP.1.2

ФБО должны осуществлять разделение между доменами безопасности субъектов в ОДФ.

14.11.6 FPT_SEP.2 Отделение домена ПФБ

Иерархический для: FPT_SEP.1 Отделение домена ФБО

Зависимости: нет зависимостей.

14.11.6.1 FPT_SEP.2.1

Неизолированная часть ФБО должна поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

14.11.6.2 FPT_SEP.2.2

ФБО должны осуществлять разделение между доменами безопасности субъектов в ОДФ.

14.11.6.3 FPT_SEP.2.3

ФБО должны поддерживать часть ФБО, связанных с [назначение: *список ПФБ управления доступом и/или управления информационными потоками*], в домене безопасности для их собственного выполнения, защищающем их от вмешательства и искажения остальной частью ФБО и субъектами, недоверенными относительно этих ПФБ.

14.11.7 FPT_SEP.3 Полный монитор обращений

Иерархический для: FPT_SEP.2 Отделение домена ПФБ

Зависимости: отсутствуют.

14.11.7.1 FPT_SEP.3.1

Неизолированная часть ФБО должна поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

14.11.7.2 FPT_SEP.3.2

ФБО должны осуществлять разделение между доменами безопасности субъектов в ОДФ.

14.11.7.3 FPT_SEP.3.3

ФБО должны поддерживать часть ФБО, **которая осуществляет ПФБ управления доступом и/или управления информационными потоками,** в домене безопасности для **ее** собственного выполнения, защищающем их от вмешательства и искажения остальной частью ФБО и субъектами, недоверенными относительно **ПБО**.

14.12 Протокол синхронизации состояний (FPT_SSP)

14.12.1 Характеристика семейства

Распределенные системы могут иметь большую сложность, чем нераспределенные, из-за многообразия состояний частей системы, а также задержек связи. В большинстве случаев синхронизация состояния между распределенными функциями включает в себя помимо обычных действий применение протокола обмена. Если в среде распределенных систем существуют угрозы безопасности, потребуются более сложные защищенные протоколы.

Семейство FPT_SSP «Протокол синхронизации состояний» устанавливает требование использования надежных протоколов некоторыми критичными по безопасности функциями из числа ФБО. Данное семейство обеспечивает, чтобы две распределенные части ОО (например главные ЭВМ) синхронизировали свои состояния после действий, связанных с безопасностью.

14.12.2 Ранжирование компонентов

Рисунок 68 — Ранжирование компонентов семейства FPT_SSP

FPT_SSP.1 «Одностороннее надежное подтверждение» содержит требование подтверждения одним лишь получателем данных.

FPT_SSP.2 «Взаимное надежное подтверждение» содержит требование взаимного подтверждения обмена данными.

14.12.3 Управление: FPT_SSP.1, FPT_SSP.2

Действия по управлению не предусмотрены.

14.12.4 Аудит: FPT_SSP.1, FPT_SSP.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: неполучение ожидаемого подтверждения.

14.12.5 FPT_SSP.1 Одностороннее надежное подтверждение

Иерархический для: нет подчиненных компонентов.

Зависимости: FPT_ITT .1 Базовая защита внутренней передачи данных ФБО

14.12.5.1 FPT_SSP.1.1

ФБО должны подтверждать после запроса другой части ФБО получение немодифицированных данных ФБО при передаче.

14.12.6 FPT_SSP.2 Взаимное надежное подтверждение

Иерархический для: FPT_SSP.1 Одностороннее надежное подтверждение

Зависимости: FPT_ITT .1 Базовая защита внутренней передачи данных ФБО

14.12.6.1 FPT_SSP.2.1

ФБО должны подтверждать после запроса другой части ФБО получение немодифицированных данных ФБО при передаче.

14.12.6.2 FPT_SSP.2.2

ФБО должны обеспечивать, чтобы соответствующие части ФБО извещались, используя подтверждения о правильном состоянии данных, передаваемых между различными частями ФБО.

14.13 Метки времени (FPT_STM)

14.13.1 Характеристика семейства

Семейство FPT_STM содержит требования по предоставлению надежных меток времени в пределах ОО.

14.13.2 Ранжирование компонентов

Рисунок 69 — Ранжирование компонентов семейства FPT_STM

Это семейство состоит из одного компонента FPT_STM.1 «Надежные метки времени», который содержит требование, чтобы ФБО предоставляли надежные метки времени для функций из числа ФБО.

14.13.3 Управление: FPT_STM.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление внутренним представлением времени.

14.13.4 Аудит: FPT_STM.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: изменения внутреннего представления времени.

b) детализированный: предоставление меток времени.

14.13.5 FPT_STM.1 Надежные метки времени

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.13.5.1 FPT_STM.1.1

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

14.14 Согласованность данных ФБО между ФБО (FPT_TDC)

14.14.1 Характеристика семейства

В среде распределенной или сложной системы от ОО может потребоваться произвести обмен данными ФБО (например атрибутами ПФБ, ассоциированными с данными, информацией аудита или идентификации) с другим доверенным продуктом ИТ. Семейство FPT_TDC определяет требования для совместного использования и согласованной интерпретации этих атрибутов между ФБО и другим доверенным продуктом ИТ.

14.14.2 Ранжирование компонентов

Рисунок 70 — Ранжирование компонентов семейства FPT_TDC

FPT_TDC.1 «Базовая согласованность данных ФБО между ФБО» содержит требование, чтобы ФБО предоставили возможность обеспечить согласованность атрибутов между ФБО.

14.14.3 Управление: FPT_TDC.1

Действия по управлению не предусмотрены.

14.14.4 Аудит: FPT_TDC.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешное использование механизмов согласования данных ФБО;

b) базовый: использование механизмов согласования данных ФБО;

c) базовый: идентификация ФБО, данные которых интерпретируются;

d) базовый: обнаружение модифицированных данных ФБО.

14.14.5 FPT_TDC.1 Базовая согласованность данных ФБО между ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

14.14.5.1 FPT_TDC.1.1

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

14.14.5.2 FPT_TDC.1.2

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

14.15 Согласованность данных ФБО при дублировании в пределах ОО (FPT_TRC)

14.15.1 Характеристика семейства

Требования семейства FPT_TRC необходимы, чтобы обеспечить согласованность данных ФБО, если они дублируются в пределах ОО. Такие данные могут стать несогласованными при нарушении работоспособности внутреннего канала между частями ОО. Если ОО внутренне структурирован как сеть, то это может произойти из-за отключения отдельных частей сети при разрыве сетевых соединений.

14.15.2 Ранжирование компонентов

Рисунок 71 — Ранжирование компонентов семейства FPT_TRC

Это семейство состоит из одного компонента FPT_TRC.1 «Согласованность дублируемых данных ФБО», содержащего требование, чтобы ФБО обеспечили непротиворечивость данных ФБО, дублируемых в нескольких частях ОО.

14.15.3 Управление: для FPT_TRC.1

Действия по управлению не предусмотрены.

14.15.4 Аудит: для FPT_TRC.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: восстановление согласованности после восстановления соединения;

b) базовый: выявление несогласованности между данными ФБО.

14.15.5 FPT_TRC.1 Согласованность дублируемых данных ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: FPT_ITT .1 Базовая защита внутренней передачи данных ФБО

14.15.5.1 FPT_TRC.1.1

ФБО должны обеспечивать согласованность данных ФБО при дублировании их в различных частях ОО.

14.15.5.2 FPT_TRC.1.2

Когда части ОО, содержащие дублируемые данные ФБО, разъединены, ФБО должны обеспечивать согласованность дублируемых данных ФБО после восстановления соединения перед обработкой любых запросов к [назначение: *список ФБ, зависящих от согласованности дублируемых данных ФБО*].

14.16 Самотестирование ФБО (FPT_TST)

14.16.1 Характеристика семейства

Семейство FPT_TST определяет требования для самотестирования ФБО в части некоторых типичных операций с известным результатом. Примерами могут служить обращения к интерфейсам реализуемых функций, а также некоторые арифметические операции, выполняемые критичными частями ОО. Эти тесты

могут выполняться при запуске, периодически, по запросу уполномоченного пользователя или при удовлетворении других условий. Действия ОО, предпринимаемые по результатам самотестирования, определены в других семействах.

Требования этого семейства также необходимы для обнаружения искажения выполняемого кода ФБО (то есть программной реализации ФБО) и данных ФБО различными сбоями, которые не всегда приводят к приостановке функционирования ОО (рассмотренной в других семействах). Такие проверки необходимо выполнять, так как подобные сбои не всегда можно предотвратить. Такие сбои могут происходить из-за непредусмотренных видов сбоев или имеющихся неточностей в проекте аппаратных, программно-аппаратных и программных средств либо вследствие злонамеренного искажения ФБО, допущенного из-за неадекватной логической и/или физической защиты.

14.16.2 Ранжирование компонентов

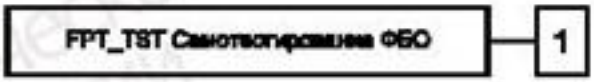

Рисунок 72 — Ранжирование компонентов семейства FPT_TST

FPT_TST.1 «Тестирование ФБО» позволяет проверять правильность выполнения ФБО. Тесты могут выполняться при запуске, периодически, по запросу уполномоченного пользователя или при выполнении других заранее оговоренных условий. Данный компонент также предоставляет возможность верифицировать целостность данных и выполняемого кода ФБО.

14.16.3 Управление: для FPT_TST.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление условиями, при которых происходит самотестирование ФБО (при запуске, с постоянным интервалом или при определенных условиях);

b) управление периодичностью выполнения (при необходимости).

14.16.4 Аудит: для FPT_TST.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) базовый: выполнение и результаты самотестирования ФБО.

14.16.5 FPT_TST.1 Тестирование ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: FPT_AMT.1 Тестирование абстрактной машины

14.16.5.1 FPT_TST.1.1

ФБО должны выполнять пакет программ самотестирования [выбор: *при запуске, периодически в процессе нормального функционирования, по запросу уполномоченного пользователя, при условиях [назначение: условия, при которых следует предусмотреть самотестирование]*] для демонстрации правильного выполнения [выбор: *[назначение: части ФБО]*, ФБО].

14.16.5.2 FPT_TST.1.2

ФБО должны предоставлять уполномоченным пользователям возможность верифицировать целостность [выбор: *[назначение: данных частей ФБО], данных ФБО*].

14.16.5.3 FPT_TST.1.3

ФБО должны предоставлять уполномоченным пользователям возможность верифицировать целостность хранимого выполняемого кода ФБО.

15 Класс FRU. Использование ресурсов

Класс FRU содержит три семейства, которые поддерживают доступность требуемых ресурсов, таких как вычислительные возможности и/или объем памяти. Семейство FRU_FLT «Отказоустойчивость» предоставляет защиту от недоступности ресурсов, вызванной сбоем ОО. Семейство FRU_PRS «Приоритет обслуживания» обеспечивает, чтобы ресурсы выделялись наиболее важным или критичным по времени задачам и не могли быть монополизированы задачами с более низким приоритетом. Семейство FRU_RSA

«Распределение ресурсов» устанавливает ограничения использования доступных ресурсов, предотвращая монополизацию ресурсов пользователями.

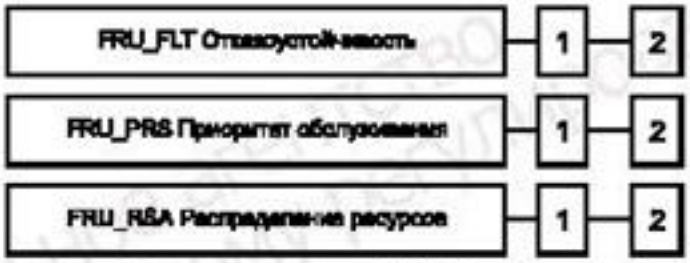

Рисунок 73 — Декомпозиция класса FRU «Использование ресурсов»

15.1 Отказоустойчивость (FRU_FLT)

15.1.1 Характеристика семейства

Требования семейства FRU_FLT обеспечивают, чтобы ОО продолжил поддерживать правильное функционирование даже в случае сбоев.

15.1.2 Ранжирование компонентов

Рисунок 74 — Ранжирование компонентов семейства FRU_FLT

FRU_FLT.1 «Пониженная отказоустойчивость» содержит требование, чтобы ОО продолжил правильное выполнение указанных возможностей в случае идентифицированных сбоев.

FRU_FLT.2 «Ограниченная отказоустойчивость» содержит требование, чтобы ОО продолжил правильное выполнение всех своих возможностей в случае идентифицированных сбоев.

15.1.3 Управление: FRU_FLT.1, FRU_FLT.2

Действия по управлению не предусмотрены.

15.1.4 Аудит: FRU_FLT.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: любой сбой, обнаруженный ФБО;

b) базовый: все операции ОО, прерванные из-за сбоя.

15.1.5 Аудит: FRU_FLT.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: любой сбой, обнаруженный ФБО.

15.1.6 FRU_FLT.1 Пониженная отказоустойчивость

Иерархический для: нет подчиненных компонентов.

Зависимости: FPT_FLS.1 Сбой с сохранением безопасного состояния

15.1.6.1 FRU_FLT.1.1

ФБО должны обеспечивать выполнение [назначение: *список возможностей ОО*], когда происходят следующие сбои: [назначение: *список типов сбоев*].

15.1.7 FRU_FLT.2 Ограниченная отказоустойчивость

Иерархический для: FRU_FLT.1 Пониженная отказоустойчивость

Зависимости: FPT_FLS.1 Сбой с сохранением безопасного состояния

15.1.7.1 FRU_FLT.2.1

ФБО должны обеспечивать выполнение **всех возможностей ОО**, когда происходят следующие сбои: [назначение: *список типов сбоев*].

15.2 Приоритет обслуживания (FRU_PRS)

15.2.1 Характеристика семейства

Требования семейства FRU_PRS позволяют ФБО управлять использованием ресурсов пользователями и субъектами в пределах своей области действия так, чтобы высокоприоритетные операции в пределах ОДФ всегда выполнялись без препятствий или задержек со стороны операций с более низким приоритетом.

15.2.2 Ранжирование компонентов

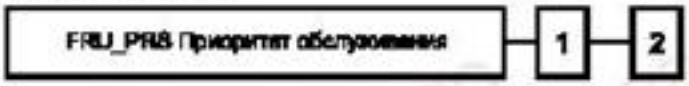

Рисунок 75 — Ранжирование компонентов семейства FRU_PRS

FRU_PRS.1 «Ограниченный приоритет обслуживания» предоставляет приоритеты для использования субъектами подмножества ресурсов в пределах ОДФ.

FRU_PRS.2 «Полный приоритет обслуживания» предоставляет приоритеты для использования субъектами всех ресурсов в пределах ОДФ.

15.2.3 Управление: FRU_PRS.1, FRU_PRS.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) назначение приоритетов каждому субъекту в ФБО.

15.2.4 Аудит: FRU_PRS.1, FRU_PRS.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: отклонение операции на основании использования приоритета при распределении ресурса;

b) базовый: все попытки использования функции распределения ресурсов с учетом приоритетности обслуживания.

15.2.5 FRU_PRS.1 Ограниченный приоритет обслуживания

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

15.2.5.1 FRU_PRS.1.1

ФБО должны устанавливать приоритет каждому субъекту в ФБО.

15.2.5.2 FRU_PRS.1.2

ФБО должны обеспечивать доступ к [назначение: *управляемые ресурсы*] на основе приоритетов, назначенных субъектам.

15.2.6 FRU_PRS.2 Полный приоритет обслуживания

Иерархический для: FRU_PRS.1 Ограниченный приоритет обслуживания

Зависимости: нет зависимостей.

15.2.6.1 FRU_PRS.2.1

ФБО должны устанавливать приоритет каждому субъекту в ФБО.

15.2.6.2 FRU_PRS.2.2

ФБО должны обеспечивать доступ ко **всем совместно используемым ресурсам** на основе приоритетов, назначенных субъектам.

15.3 Распределение ресурсов (FRU_RSA)

15.3.1 Характеристика семейства

Требования семейства FRU_RSA позволяют ФБО управлять использованием ресурсов пользователями и субъектами так, чтобы не происходило отказов в обслуживании из-за несанкционированной монополизации ресурсов.

15.3.2 Ранжирование компонентов

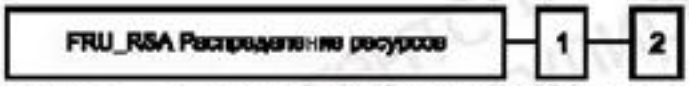

Рисунок 76 — Ранжирование компонентов семейства FRU_PSA

FRU_RSA.1 «Максимальные квоты» содержит требования к механизмам квотирования, которые обеспечивают, чтобы пользователи и субъекты не монополизировали управляемый ресурс.

FRU_RSA.2 «Минимальные и максимальные квоты» содержит требования к механизмам квотирования, которые обеспечивают, чтобы пользователи и субъекты всегда имели хотя бы минимум специфицированного ресурса, но при этом не могли бы монополизировать этот ресурс.

15.3.3 Управление: FRU_RSA.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) определение администратором максимальных квот ресурса для групп и/или отдельных пользователей и/или субъектов.

15.3.4 Управление: FRU_RSA.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) определение администратором минимальных и максимальных квот ресурса для групп и/или отдельных пользователей и/или субъектов.

15.3.5 Аудит: FRU_RSA.1, FRU_RSA.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: отклонение операции распределения ресурса из-за его ограниченности;

b) базовый: все обращения к функциям распределения ресурсов, управляемых ФБО.

15.3.6 FRU_RSA.1 Максимальные квоты

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

15.3.6.1 FRU_RSA.1.1

ФБО должны реализовывать максимальные квоты следующих ресурсов: [назначение: *управляемые ресурсы*], которые [выбор: *отдельные пользователи, определенные группы пользователей, субъекты*] могут использовать [выбор: *одновременно, в течение определенного периода времени*].

15.3.7 FRU_RSA.2 Минимальные и максимальные квоты

Иерархический для: FRU_RSA.1 Максимальные квоты

Зависимости: нет зависимостей.

15.3.7.1 FRU_RSA.2.1

ФБО должны реализовывать максимальные квоты следующих ресурсов: [назначение: *управляемые ресурсы*], которые [выбор: *отдельные пользователи, определенные группы пользователей, субъекты*] могут использовать [выбор: *одновременно, в течение определенного периода времени*].

15.3.7.2 FRU_RSA.2.2

ФБО должны обеспечивать выделение минимального числа каждого из [назначение: *управляемые ресурсы*], которые являются доступными для [выбор: *отдельный пользователь, определенная группа пользователей, субъекты*], чтобы использовать [выбор: *одновременно, в течение определенного периода времени*].

16 Класс FTA. Доступ к ОО

Класс FTA определяет функциональные требования к управлению открытием сеанса пользователя.

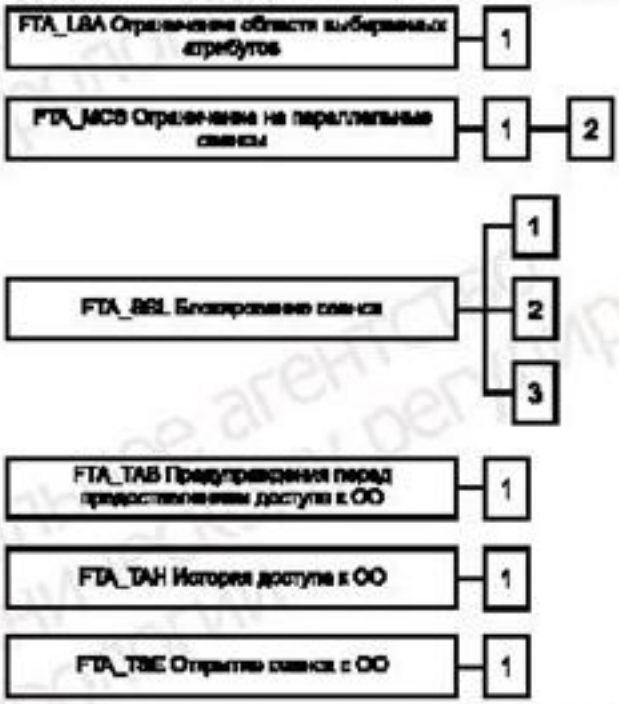

Рисунок 77 — Декомпозиция класса FTA «Доступ к ОО»

16.1 Ограничение области выбираемых атрибутов (FTA_LSA)

16.1.1 Характеристика семейства

Семейство FTA_LSA определяет требования по ограничению области атрибутов безопасности сеанса, которые может выбирать для него пользователь.

16.1.2 Ранжирование компонентов

Рисунок 78 — Ранжирование компонентов семейства FTA_LSA

FTA_LSA.1 «Ограничение области выбираемых атрибутов» содержит требование к ОО по ограничению области атрибутов безопасности сеанса во время его открытия.

16.1.3 Управление: FTA_LSA.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление администратором областью атрибутов безопасности сеанса.

16.1.4 Аудит: FTA_LSA.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: все неуспешные попытки выбора атрибутов безопасности сеанса;

b) базовый: все попытки выбора атрибутов безопасности сеанса;

c) детализированный: фиксация значений атрибутов безопасности каждого сеанса.

16.1.5 FTA_LSA.1 Ограничение области выбираемых атрибутов

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

16.1.5.1 FTA_LSA.1.1

ФБО должны ограничивать область атрибутов безопасности сеанса [назначение: *атрибуты безопасности сеанса*], основываясь на [назначение: *атрибуты*].

16.2 Ограничение на параллельные сеансы (FTA_MCS)

16.2.1 Характеристика семейства

Семейство FTA_MCS определяет требования по ограничению числа параллельных сеансов, предоставляемых одному и тому же пользователю.

16.2.2 Ранжирование компонентов

Рисунок 79 — Ранжирование компонентов семейства FTA_MCS

FTA_MCS.1 «Базовое ограничение на параллельные сеансы» предоставляет ограничения, которые применяются ко всем пользователям ФБО.

FTA_MCS.2 «Ограничение на параллельные сеансы по атрибутам пользователя» расширяет FTA_MCS.1 «Базовое ограничение на параллельные сеансы» требованием возможности определить ограничения на число параллельных сеансов, основываясь на атрибутах безопасности, связанных с пользователем.

16.2.3 Управление: FTA_MCS.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление администратором максимально допустимым числом параллельных сеансов, предоставляемых пользователю.

16.2.4 Управление: FTA_MCS.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) управление администратором правилами, которые определяют максимально допустимое число параллельных сеансов, предоставляемых пользователю.

16.2.5 Аудит: FTA_MCS.1, FTA_MCS.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

а) минимальный: отклонение нового сеанса, основанное на ограничении числа параллельных сеансов;

b) детализированный: фиксация числа параллельных сеансов пользователя, а также атрибутов безопасности этого пользователя.

16.2.6 FTA_MCS.1 Базовое ограничение на параллельные сеансы

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UID.1 Выбор момента идентификации

16.2.6.1 FTA_MCS.1.1

ФБО должны ограничивать максимальное число параллельных сеансов, предоставляемых одному и тому же пользователю.

16.2.6.2 FTA_MCS.1.2

ФБО должны задавать по умолчанию ограничение [назначение: *задаваемое по умолчанию число*] сеансов пользователя.

16.2.7 FTA_MCS.2 Ограничение на параллельные сеансы по атрибутам пользователя

Иерархический для: FTA_MCS.1 Базовое ограничение на параллельные сеансы

Зависимости: FIA_UID.1 Выбор момента идентификации

16.2.7.1 FTA_MCS.2.1

ФБО должны ограничивать максимальное число параллельных сеансов, предоставляемых одному и тому же пользователю, **согласно правилам [назначение: *правила определения максимального числа параллельных сеансов*]**.

16.2.7.2 FTA_MCS.2.2

ФБО должны задавать по умолчанию ограничение [назначение: *задаваемое по умолчанию число*] сеансов пользователя.

16.3 Блокирование сеанса (FTA_SSL)

16.3.1 Характеристика семейства

Семейство FTA_SSL определяет требования к ФБО по предоставлению возможности как ФБО, так и пользователю блокировать и разблокировать интерактивный сеанс.

16.3.2 Ранжирование компонентов

Рисунок 80 — Ранжирование компонентов семейства FTA_SSL

FTA_SSL.1 «Блокирование сеанса, инициированное ФБО» включает в себя инициированное системой блокирование интерактивного сеанса после определенного периода бездействия пользователя.

FTA_SSL.2 «Блокирование, инициированное пользователем» предоставляет пользователю возможность блокировать и разблокировать свои собственные интерактивные сеансы.

FTA_SSL.3 «Завершение, инициированное ФБО» предоставляет требования к ФБО по завершению сеанса после определенного периода бездействия пользователя.

16.3.3 Управление: FTA_SSL.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) задание времени бездействия пользователя, после которого происходит блокировка сеанса;

b) задание по умолчанию времени бездействия пользователя, после которого происходит блокировка;

c) управление событиями, которые предусматриваются до разблокирования сеанса.

16.3.4 Управление: FTA_SSL.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление событиями, которые предусматриваются до разблокирования сеанса.

16.3.5 Управление: FTA_SSL.3

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) задание времени бездействия пользователя, после которого происходит завершение интерактивного сеанса;

b) задание по умолчанию времени бездействия пользователя, после которого происходит завершение интерактивного сеанса.

16.3.6 Аудит: FTA_SSL.1, FTA_SSL.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: блокирование интерактивного сеанса механизмом блокирования сеанса;

b) минимальный: успешное разблокирование интерактивного сеанса;

c) базовый: все попытки разблокирования интерактивного сеанса.

16.3.7 Аудит: FTA_SSL.3

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: завершение интерактивного сеанса механизмом блокирования сеанса.

16.3.8 FTA_SSL.1 Блокирование сеанса, инициированное ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UAU.1 Выбор момента аутентификации

16.3.8.1 FTA_SSL.1.1

ФБО должны блокировать интерактивный сеанс после [назначение: *интервал времени бездействия пользователя*], для чего предпринимаются следующие действия:

a) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;

b) блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса.

16.3.8.2 FTA_SSL.1.2

ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [назначение: *события, которые будут происходить*].

16.3.9 FTA_SSL.2 Блокирование, инициированное пользователем

Иерархический для: нет подчиненных компонентов.

Зависимости: FIA_UAU.1 Выбор момента аутентификации

16.3.9.1 FTA_SSL.2.1

ФБО должны допускать инициированное пользователем блокирование своего собственного интерактивного сеанса, для чего предпринимаются следующие действия:

a) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;

b) блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса.

16.3.9.2 FTA_SSL.2.2

ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [назначение: *события, которые будут происходить*].

16.3.10 FTA_SSL.3 Завершение, инициированное ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

16.3.10.1 FTA_SSL.3.1

ФБО должны завершать интерактивный сеанс после [назначение: *интервал времени бездействия пользователя*].

16.4 Предупреждения перед предоставлением доступа к ОО (FTA_TAB)

16.4.1 Характеристика семейства

Семейство FTA_TAB определяет требования к отображению для пользователей предупреждающего сообщения с перестраиваемой конфигурацией относительно характера использования ОО.

16.4.2 Ранжирование компонентов

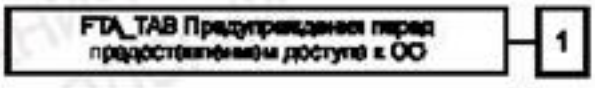

Рисунок 81 — Ранжирование компонентов семейства FTA_TAB

FTA_TAB.1 «Предупреждения по умолчанию перед предоставлением доступа к ОО» содержит требования к предупреждающим сообщениям, которые отображаются перед началом диалога в сеансе.

16.4.3 Управление: FTA_TAB.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

а) сопровождение уполномоченным администратором предупреждающих сообщений.

16.4.4 Аудит: FTA_TAB.1

Нет событий, для которых следует предусмотреть возможность аудита.

16.4.5 FTA_TAB.1 Предупреждения по умолчанию перед предоставлением доступа к ОО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

16.4.5.1 FTA_TAB.1.1

Перед открытием сеанса пользователя ФБО должны отображать предупреждающее сообщение о несанкционированном использовании ОО.

16.5 История доступа к ОО (FTA_TAH)

16.5.1 Характеристика семейства

Семейство FTA_TAH определяет требования к ФБО по отображению для пользователя, при успешном открытии сеанса, истории успешных и неуспешных попыток получить доступ от имени этого пользователя.

16.5.2 Ранжирование компонентов

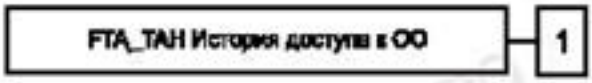

Рисунок 82 — Ранжирование компонентов семейства FTA_TAH

FTA_TAH.1 «История доступа к ОО» содержит требования к ОО по отображению информации, связанной с предыдущими попытками открыть сеанс.

16.5.3 Управление: FTA_TAH.1

Действия по управлению не предусмотрены.

16.5.4 Аудит: FTA_TAH.1

Нет событий, для которых следует предусмотреть возможность аудита.

16.5.5 FTA_TAH.1 История доступа к ОО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

16.5.5.1 FTA_TAH.1.1

При успешном открытии сеанса ФБО должны отображать [выбор: *дата, время, метод, расположение*] последнего успешного открытия сеанса от имени этого пользователя.

16.5.5.2 FTA_TAH.1.2

При успешном открытии сеанса ФБО должны отображать [выбор: *дата, время, метод, расположение*] последней неуспешной попытки открытия сеанса и число неуспешных попыток со времени последнего успешного открытия сеанса.

16.5.5.3 FTA_TAH.1.3

ФБО не должны удалять информацию об истории доступа из интерфейса пользователя без предоставления пользователю возможности просмотреть ее.

16.6 Открытие сеанса с ОО (FTA_TSE)

16.6.1 Характеристика семейства

Семейство FTA_TSE определяет требования по запрещению пользователям открытия сеанса с ОО.

16.6.2 Ранжирование компонентов

Рисунок 83 — Ранжирование компонентов семейства FTA_TSE

FTA_TSE.1 «Открытие сеанса с ОО» содержит условия запрещения пользователям доступа к ОО, основанного на атрибутах.

16.6.3 Управление: FTA_TSE.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) управление уполномоченным администратором условиями открытия сеанса.

16.6.4 Аудит: FTA_TSE.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: запрещение открытия сеанса механизмом открытия сеанса;

b) базовый: все попытки открытия сеанса пользователя;

c) детализированный: фиксация значений выбранных параметров доступа (таких, как место доступа или время доступа).

16.6.5 FTA_TSE.1 Открытие сеанса с ОО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

16.6.5.1 FTA_TSE.1.1

ФБО должны быть способны отказывать в открытии сеанса, основываясь на [назначение: *атрибуты*].

17 Класс FTP. Доверенный маршрут/канал

Семейства класса FTP содержат требования как к доверенному маршруту связи между пользователями и ФБО, так и к доверенному каналу связи между ФБО и другими доверенными продуктами ИТ. Доверенные маршруты и каналы имеют следующие общие свойства:

- маршрут связи создается с использованием внутренних и внешних каналов связи (в соответствии с компонентом), которые изолируют идентифицированное подмножество данных и команд ФБО от остальной части данных пользователей и ФБО;

- использование маршрута связи может быть инициировано пользователем и/или ФБО (в соответствии с компонентом);

- маршрут связи способен обеспечить доверие тому, что пользователь взаимодействует с требуемыми ФБО или ФБО — с требуемым пользователем (в соответствии с компонентом).

В данной парадигме доверенный канал — это канал связи, который может быть инициирован любой из связывающихся сторон и обеспечивает характеристики неотказуемости по отношению к идентификационным признакам сторон канала.

Доверенный маршрут предоставляет пользователям средства для выполнения функций путем обеспечения прямого взаимодействия с ФБО. Доверенный маршрут обычно желателен при начальной идентификации и/или аутентификации пользователя, но может быть также применен на протяжении всего сеанса пользователя. Обмены по доверенному маршруту могут быть инициированы пользователем или ФБО. Гарантируется, что ответы пользователя с применением доверенного маршрута будут защищены от модификации или раскрытия недоверенными приложениями.

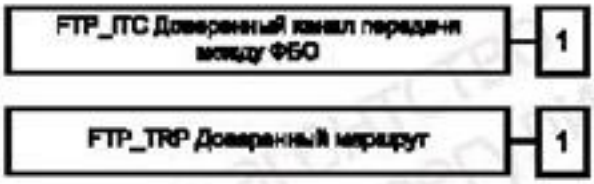

Рисунок 84 — Декомпозиция класса FPT «Доверенный маршрут/канал»

17.1 Доверенный канал передачи между ФБО (FTP_ITC)

17.1.1 Характеристика семейства

Семейство FTP_ITC определяет правила создания доверенного канала между ФБО и другими доверенными продуктами ИТ для выполнения операций, критичных для безопасности. Это семейство следует использовать всякий раз, когда имеются требования безопасной передачи данных пользователя или ФБО между ОО и другими доверенными продуктами ИТ.

17.1.2 Ранжирование компонентов

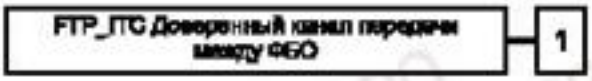

Рисунок 85 — Ранжирование компонентов FTP_ITC

FTP_ITC.1 «Доверенный канал передачи между ФБО» содержит требование, чтобы ФБО предоставляли доверенный канал связи между ними и другим доверенным продуктом ИТ.

17.1.3 Управление: FTP_ITC.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) изменение набора операций, которые требуют доверенного канала (если имеется).

17.1.4 Аудит: FTP_ITC.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: сбой функций доверенного канала;

b) минимальный: идентификация инициатора и адресата отказавших функций доверенного канала;

c) базовый: все попытки использования функций доверенного канала;

d) базовый: идентификация инициатора и адресата всех функций доверенного канала.

17.1.5 FTP_ITC.1 Доверенный канал передачи между ФБО

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

17.1.5.1 FTP_ITC.1.1

ФБО должны предоставлять канал связи между ними 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.

17.1.5.2 FTP_ITC.1.2

ФБО должны позволять [выбор: *ФБО, удаленный доверенный продукт ИТ*] инициировать связь через доверенный канал.

17.1.5.3 FTP_ITC.1.3

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

17.2 Доверенный маршрут (FTP_TRP)

17.2.1 Характеристика семейства

Семейство FTP_TRP определяет требования установки и поддержания доверенной связи между пользователями и ФБО. Доверенный маршрут может потребоваться для любого связанного с безопасностью взаимодействия. Обмен по доверенному маршруту может быть инициирован пользователем при взаимодействии с ФБО, или ФБО могут устанавливать связь с пользователем по доверенному маршруту.

17.2.2 Ранжирование компонентов

Рисунок 86 — Ранжирование компонентов семейства FTP_TRP

FTP_TRP.1 «Доверенный маршрут» содержит требование, чтобы доверенный маршрут между ФБО и пользователем предоставлялся для совокупности событий, определенных разработчиком ПЗ/ЗБ. Возможность инициировать доверенный маршрут могут иметь пользователь и/или ФБО.

17.2.3 Управление: FTP_TRP.1

Для функций управления из класса FMT могут рассматриваться следующие действия:

a) изменение набора операций, которые требуют доверенного маршрута, если он имеется.

17.2.4 Аудит: FTP_TRP.1

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: сбой функций доверенного маршрута;

b) минимальный: идентификация пользователей, ассоциированных со всеми отказами доверенного маршрута (если это возможно);

c) базовый: все попытки использования функций доверенного маршрута;

d) базовый: идентификация пользователей, ассоциированных со всеми вызовами доверенного маршрута (если это возможно).

17.2.5 FTP_TRP.1 Доверенный маршрут

Иерархический для: нет подчиненных компонентов.

Зависимости: нет зависимостей.

17.2.5.1 FTP_TRP.1.1

ФБО должны предоставлять маршрут связи между собой и [выбор: *удаленный, локальный*] пользователем, который логически отличим от других маршрутов связи и обеспечивает уверенную идентификацию его начала и конца, а также защиту передаваемых данных от модификации или раскрытия.

17.2.5.2 FTP_TRP.1.2

ФБО должны позволить [выбор: *ФБО, локальные пользователи, удаленные пользователи*] инициировать связь через доверенный маршрут.

17.2.5.3 FTP_TRP.1.3

ФБО должны требовать использования доверенного маршрута для [выбор: *начальная аутентификация пользователя, [назначение: другие услуги, для которых требуется доверенный маршрут]*].

Федеральное агентство по техническому регулированию и метрологии

Приложение А
(обязательное)

Замечания по применению функциональных требований безопасности

Настоящее приложение содержит дополнительное руководство по использованию семейств и компонентов, определенных в разделах настоящего стандарта, которое может понадобиться потребителям, разработчикам или оценщикам при использовании компонентов. Для упрощения поиска требуемой информации порядок следования классов, семейств и компонентов в приложениях тот же, что и в разделах настоящего стандарта.

А.1 Структура замечаний

Настоящий раздел определяет содержание и форму замечаний, относящихся к функциональным требованиям ИСО/МЭК 15408.

А.1.1 Структура класса

Структура функционального класса в приложениях С—М приведена на рисунке А.1.

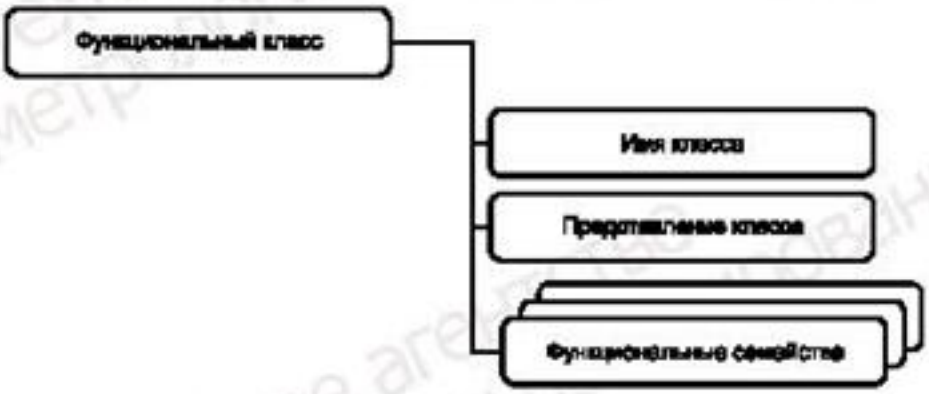

Рисунок А.1 — Структура функционального класса

А.1.1.1 Имя класса

Имя класса — это уникальное имя класса, определенное в соответствующих разделах настоящего стандарта.

А.1.1.2 Представление класса

В представлении класса в приложениях С—М приведена информация об использовании семейств и компонентов класса. Данная информация дополнена соответствующим рисунком, показывающим организацию каждого класса и семейств в каждом классе, а также иерархические связи между компонентами в каждом семействе.

А.1.2 Структура семейства

Структура функционального семейства в замечаниях по применению приведена на рисунке А.2.

Рисунок А.2 — Структура функционального семейства в замечаниях по применению

А.1.2.1 Имя семейства

Имя семейства — это уникальное имя семейства, определенное в соответствующих разделах настоящего стандарта.

А.1.2.2 Замечания для пользователя

Замечания для пользователя содержат дополнительную информацию, которая представляет интерес для потенциальных пользователей семейства, таких как разработчики ПЗ, ЗБ, функциональных пакетов, а также ОО. Данные замечания имеют информативный характер и могут охватывать предупреждения об ограничениях применения и аспектах, требующих особого внимания при использовании компонентов.

А.1.2.3 Замечания для оценщика

Замечания для оценщика содержат любую информацию, которая представляет интерес для разработчиков и оценщиков ОО при проверке его на соответствие компонентам семейства. Замечания носят информативный характер и могут относиться к различным областям, требующим особого внимания при оценке. Данные замечания могут включать в себя разъяснение назначения и определение возможных путей интерпретации требований, а также предостережения и предупреждения, представляющие особый интерес для оценщиков.

Подпункты с замечаниями для пользователя и оценщика не являются обязательными и приводятся только при необходимости.

А.1.3 Структура компонента

Структура функциональных компонентов в замечаниях по применению показана на рисунке А.3.

Рисунок А.3 — Структура функционального компонента

А.1.3.1 Идентификация компонента

Имя компонента — это уникальное имя компонента, определенное в соответствующих разделах настоящего стандарта.

А.1.3.2 Обоснование компонента и замечания по применению

В данном подпункте может содержаться любая относящаяся к компоненту «информация».

Обоснование содержит такие детали, которые уточняют общие формулировки применительно к определенному уровню; его следует использовать только в случае, если на этом уровне требуется расширенное описание.

Замечания по применению содержат дополнительное уточнение в виде описания, относящегося к определенному компоненту. Уточнение может касаться замечаний для пользователя и/или оценщика, как указано в А.1.2. Данное уточнение может использоваться при объяснении природы зависимостей (например, совместно применяемая информация или действие).

Данный подпункт не является обязательным и приводится только при необходимости.

А.1.3.3 Разрешенные операции

В данном подпункте для каждого компонента содержатся рекомендации по выполнению разрешенных в данном компоненте операций.

Этот подпункт не является обязательным и приводится только при необходимости.

А.2 Таблицы зависимостей

В следующих таблицах зависимостей для функциональных компонентов представлены прямые, косвенные и выбираемые зависимости функциональных компонентов. Для каждого компонента, от которого зависят какие-либо функциональные компоненты, отведен столбец таблицы. Для каждого функционального компонента отведена строка таблицы. Знаки на пересечении строк и столбцов таблицы указывают характер зависимости соответствующих компонентов: «X» — прямая зависимость; «-» — косвенная, а «O» — выбираемая.

Выбираемую зависимость рассмотрим на примере компонента FDP_ETC.1 «Экспорт данных пользователя без атрибутов безопасности», требующего присутствия компонента FDP_ACC.1 «Ограниченное управление доступом» либо компонента FDP_IFC.1 «Ограниченное управление информационными потоками». Так, если выбран компонент FDP_ACC.1 «Ограниченное управление доступом», то присутствие FDP_IFC.1 «Ограниченное

управление информационными потоками» необязательно и наоборот. Если пересечение строки и столбца таблицы пусто, компонент из строки не зависит от компонента из столбца.

Таблица А.1 — Таблица зависимостей для класса FAU «Аудит безопасности»

	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FAU_ARP.1	-	X							-
FAU_GEN.1									X
FAU_GEN.2	X				X				-
FAU_SAA.1	X								-
FAU_SAA.2					X				
FAU_SAA.3									
FAU_SAA.4									
FAU_SAR.1	X								-
FAU_SAR.2	-		X						-
FAU_SAR.3	-		X						-
FAU_SEL.1	X				-	X	-	-	-
FAU_STG.1	X								-
FAU_STG.2	X								-
FAU_STG.3	-			X					-
FAU_STG.4	-			X					-

Таблица А.2 — Таблица зависимостей для класса FCO «Связь»

	FIA_UID.1
FCO_NRO.1	X
FCO_NRO.2	X
FCO_NRR.1	X
FCO_NRR.2	X

Таблица А.3 — Таблица зависимостей для класса FCS «Криптографическая поддержка»

	ADV_SPM.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITC.2	FIA_UID.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FCS_CKM.1	-	-	O	X	O	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-
FCS_CKM.2	-	O	-	X	-	-	-	-	-	O	O	-	-	X	-	-	-	-	-	-
FCS_CKM.3	-	O	-	X	-	-	-	-	-	O	O	-	-	X	-	-	-	-	-	-
FCS_CKM.4	-	O	-	-	-	-	-	-	-	O	O	-	-	X	-	-	-	-	-	-
FCS_COP.1	-	O	-	X	-	-	-	-	-	O	O	-	-	X	-	-	-	-	-	-

Таблица А.4 — Таблица зависимостей для класса FDP «Защита данных пользователя»

	AVA_CCA.1	AVA_CCA.3	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITT.1	FDP_ITT.2	FDP_UIT.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FDP_ACC.1			-	X	-	-				-	-	-	-	-			
FDP_ACC.2			-	X	-	-				-	-	-	-	-			
FDP_ACF.1			X	-	-	-				-	-	X	-	-			
FDP_DAU.1																	
FDP_DAU.2										X							
FDP_ETC.1			O	-	O	-				-	-	-	-	-			
FDP_ETC.2			O	-	O	-				-	-	-	-	-			
FDP_IFC.1			-	-	-	X				-	-	-	-	-			
FDP_IFC.2			-	-	-	X				-	-	-	-	-			
FDP_IFF.1			-	-	X	-				-	-	X	-	-			
FDP_IFF.2			-	-	X	-				-	-	X	-	-			
FDP_IFF.3	X		-	-	X	-				-	-	-	-	-			
FDP_IFF.4	X		-	-	X	-				-	-	-	-	-			
FDP_IFF.5		X	-	-	X	-				-	-	-	-	-			
FDP_IFF.6	X		-	-	X	-				-	-	-	-	-			
FDP_ITC.1			O	-	O	-				-	-	X	-	-			
FDP_ITC.2			O	-	O	-				-	-	-	-	-	X	O	O
FDP_ITT.1			O	-	O	-				-	-	-	-	-			
FDP_ITT.2			O	-	O	-				-	-	-	-	-			
FDP_ITT.3			O	-	O	-	X			-	-	-	-	-			
FDP_ITT.4			O	-	O	-		X		-	-	-	-	-			
FDP_RIP.1																	
FDP_RIP.2																	
FDP_ROL.1			O	-	O	-				-	-	-	-	-			
FDP_ROL.2			O	-	O	-				-	-	-	-	-			
FDP_SDI.1																	
FDP_SDI.2																	
FDP_UCT.1			O	-	O	-				-	-	-	-	-		O	O
FDP_UIT.1			O	-	O	-				-	-	-	-	-		O	O
FDP_UIT.2			O	-	O	-			O	-	-	-	-	-		O	-
FDP_UIT.3			O	-	O	-			O	-	-	-	-	-		O	-

Таблица А.5 — Таблица зависимостей для класса FIA «Идентификация и аутентификация»

	FIA_ATD.1	FIA_UAU.1	FIA_UID.1
FIA_AFL.1		X	-
FIA_ATD.1			
FIA_SOS.1			
FIA_SOS.2			
FIA_UAU.1			X
FIA_UAU.2			X
FIA_UAU.3			
FIA_UAU.4			
FIA_UAU.5			
FIA_UAU.6			
FIA_UAU.7		X	-
FIA_UID.1			
FIA_UID.2			
FIA_USB.1	X		

Таблица А.6 — Таблица зависимостей для класса FMT «Управление безопасностью»

	ADV_SPM.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FMT_MOF.1						-				X	X	
FMT_MSA.1		O	-	O	-	-	-	-		X	X	
FMT_MSA.2	X	O	-	O	-	-	X	-		-	X	
FMT_MSA.3		-	-	-	-	-	X	-		-	X	
FMT_MTD.1						-				X	X	
FMT_MTD.2						-			X	-	X	
FMT_MTD.3	X					-			X	-	-	
FMT_REV.1						-					X	
FMT_SAE.1						-					X	X
FMT_SMF.1												
FMT_SMR.1						X						
FMT_SMR.2						X						
FMT_SMR.3						-					X	

Таблица А.7 — Таблица зависимостей для класса FPR «Приватность»

	FIA_UID.1	FPR_UNO.1
FPR_ANO.1		
FPR_ANO.2		
FPR_PSE.1		
FPR_PSE.2	X	
FPR_PSE.3		
FPR_UNL.1		
FPR_UNO.1		
FPR_UNO.2		
FPR_UNO.3		X
FPR_UNO.4		

Таблица А.8 — Таблица зависимостей для класса FPT «Защита ФБО»

	ADV_SPM.1	AGD_ADM.1	FIA_UID.1	FMT_MOF.1	FMT_SMF.1	FMT_SMR.1	FPT_AMT.1	FPT_ITT.1
FPT_AMT.1								
FPT_FLS.1	X							
FPT_ITA.1								
FPT_ITC.1								
FPT_ITI.1								
FPT_ITI.2								
FPT_ITT.1								
FPT_ITT.2								
FPT_ITT.3								X
FPT_PHP.1								
FPT_PHP.2			-	X	-	-		
FPT_PHP.3								
FPT_RCV.1	X	X						
FPT_RCV.2	X	X						
FPT_RCV.3	X	X						
FPT_RCV.4	X							
FPT_RPL.1								
FPT_RVM.1								
FPT_SEP.1								
FPT_SEP.2								
FPT_SEP.3								
FPT_SSP.1								X
FPT_SSP.2								X
FPT_STM.1								
FPT_TDC.1								
FPT_TRC.1								X
FPT_TST.1							X	

Таблица А.9 — Таблица зависимостей для класса FRU «Использование ресурсов»

	FRU_RSA.1	FPT_FLS.1
FRU_FLT.1	-	X
FRU_FLT.2	-	X
FRU_PRS.1		
FRU_PRS.2		
FRU_RSA.1		
FRU_RSA.2		

Таблица А.10 — Таблица зависимостей для класса FTA «Доступ к ОО»

	FIA_UAU.1	FIA_UID.1
FTA_LSA.1		
FTA_MCS.1		X
FTA_MCS.2		X
FTA_SSL.1	X	-
FTA_SSL.2	X	-
FTA_SSL.3		
FTA_TAB.1		
FTA_TAH.1		
FTA_TSE.1		

Федеральное агентство по техническому регулированию и метрологии

Приложение В
(обязательное)

Функциональные классы, семейства и компоненты

Приложения С—М содержат замечания по применению функциональных классов, определенных ранее в настоящем стандарте.

Приложение С
(обязательное)

Аудит безопасности (FAU)

Семейства аудита по ИСО/МЭК 15408 предоставляют авторам ПЗ/ЗБ возможность определить требования для мониторинга действий пользователя и в некоторых случаях обнаружить существующие, возможные или готовящиеся нарушения ПБО. Функции аудита безопасности ОО определены с тем, чтобы помочь осуществлять контроль за относящимися к безопасности событиями, и выступают как сдерживающий фактор нарушений безопасности. Требования семейств аудита используют функции, включающие в себя защиту данных аудита, формат записи, выбор событий, а также инструментальные средства анализа, сигналы оповещения при нарушении и анализ в реальном масштабе времени. Журнал аудита следует представлять в формате, доступном человеку либо явно (например, храня журнал аудита в таком формате), либо неявно (например, применяя инструментальные средства предварительной обработки данных аудита) или с использованием обоих методов.

При составлении требований аудита безопасности автору ПЗ/ЗБ следует обращать внимание на взаимосвязь семейств и компонентов аудита. Возможность реализации совокупности требований аудита в соответствии со списками зависимостей компонентов может привести и к некоторым недостаткам функции аудита (например, при проведении аудита всех событий, относящихся к безопасности, не будет возможности управлять ими на селективной основе, такой как принадлежность к отдельному пользователю или объекту).

С.1 Требования аудита в распределенной среде

Реализация требований аудита для сетей и других больших систем может значительно отличаться от реализации таких требований в автономной системе. Для больших и сложных систем требуется более продуманный план сбора и управления данными аудита, поскольку их труднее интерпретировать (и даже хранить). Обычный список, упорядоченный по времени, или журнал событий, подвергающихся аудиту, не применимы в глобальных, не синхронизированных сетях, в которых одновременно происходит множество событий.

Кроме того, в распределенном ОО в различных хост-компьютерах и серверах могут быть различные политики назначения имен. Для того чтобы избежать избыточности и «столкновения» имен, может потребоваться общесетевое соглашение об их согласованном представлении для аудита.

Для обслуживания распределенной системы может потребоваться хранилище данных аудита из многих объектов, доступное потенциально широкому кругу уполномоченных пользователей.

Наконец, к злоупотреблениям уполномоченных пользователей своими правами следует отнести систематическое уничтожение отдельных областей хранения данных аудита, относящихся к действиям администратора.

Декомпозиция класса FAU «Аудит безопасности» на составляющие его компоненты показана на рисунке С.1.

С.2 Автоматическая реакция аудита безопасности (FAU_ARP)

С.2.1 Замечания по применению

Семейство FAU_ARP «Автоматическая реакция аудита безопасности» содержит требования по обработке событий аудита. Конкретное требование может включать в себя требования сигнала тревоги или действий ФБО (автоматическая реакция). Например, ФБО могут обеспечивать подачу сигнала тревоги в реальном времени, прерывание процесса с выявленным нарушением, прекращение обслуживания, блокирование или закрытие учетных данных пользователя.

Событие аудита определяется как «возможное нарушение безопасности», если так указано в компонентах семейства FAU_SAA «Анализ аудита безопасности».

С.2.2 FAU_ARP.1 Сигналы нарушения безопасности

С.2.2.1 Замечания по применению для пользователя

При сигнале тревоги следует предпринять определенные действия. Они могут включать в себя информирование уполномоченного пользователя, предоставление уполномоченному пользователю перечня возможных мер противодействия или выполнение корректирующих действий. Автору ПЗ/ЗБ следует быть особенно внимательным при определении последовательности проведения таких действий.

С.2.2.2 Операции

С.2.2.2.1 Назначение

В элементе FAU_ARP.1.1 автору ПЗ/ЗБ следует определить действия, предпринимаемые в случае возможного нарушения безопасности. Примером списка таких действий является: «информировать уполномоченного пользователя, блокировать субъекта, действия которого могут привести к нарушению безопасности». Можно также указать, что предпринимаемые действия могут определяться уполномоченным пользователем.

С.3 Генерация данных аудита безопасности (FAU_GEN)

С.3.1 Замечания по применению

Семейство FAU_GEN «Генерация данных аудита безопасности» содержит требования по спецификации событий аудита, которые следует генерировать с использованием ФБО для событий, относящихся к безопасности.

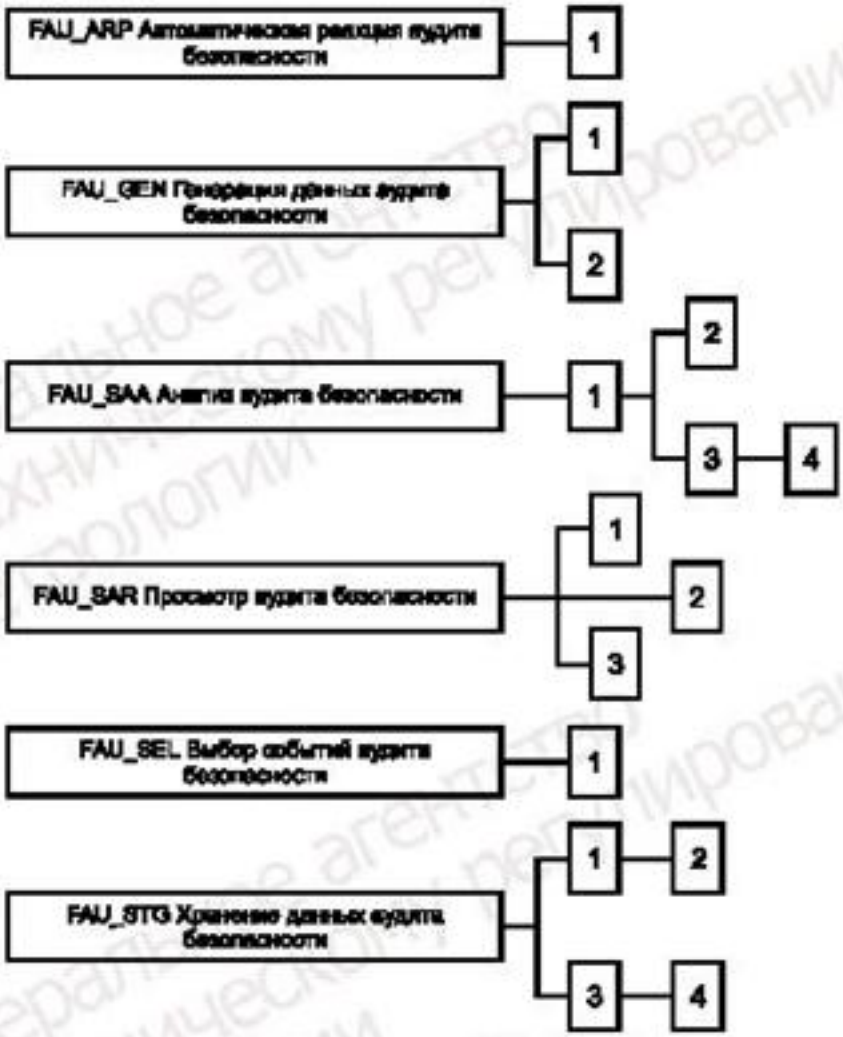

Рисунок С.1 — Декомпозиция класса FAU «Аудит безопасности»

Это семейство организовано так, чтобы избежать зависимостей от всех компонентов, требующих поддержки аудита. В каждом компоненте имеется подготовленная секция «Аудит», в которой перечислены события, предлагаемые для аудита в его функциональной области. Содержание указанной области аудита используется автором ПЗ/ЗБ при составлении ПЗ/ЗБ для завершения операций этого компонента. Таким образом, спецификация того, что может подвергаться аудиту в функциональной области, содержится в указанной области.

Список событий, потенциально подвергаемых аудиту, полностью зависит от других функциональных семейств в ПЗ/ЗБ. Поэтому в описание каждого семейства следует включать список событий, относящихся к семейству и потенциально подвергаемых аудиту, для каждого компонента семейства. Каждое событие в списке потенциально подвергаемых аудиту событий, специфицированное в функциональном семействе, следует отнести к одному из принятых уровней генерации событий аудита (то есть минимальному, базовому, детализированному). Это предоставляет автору ПЗ/ЗБ информацию, позволяющую обеспечить, чтобы все события, потенциально подвергаемые аудиту, были специфицированы в ПЗ/ЗБ. Как необходимо специфицировать события, потенциально подвергаемые аудиту, в соответствующих функциональных семействах показано на следующем примере.

«Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

a) минимальный: успешное использование функций административного управления атрибутами безопасности пользователя;

b) базовый: все попытки использования функций административного управления атрибутами безопасности пользователя;

c) базовый: идентификация модифицированных атрибутов безопасности пользователя;

d) детализированный: новые значения атрибутов, за исключением чувствительных атрибутов (например, паролей, ключей шифрования)».

Для каждого выбранного функционального компонента в общую совокупность событий, потенциально подвергаемых аудиту, следует включить те указанные в нем события, которые соответствуют уровню, установленному в FAU_GEN «Генерация данных аудита безопасности». Если в приведенном выше примере в FAU_GEN «Генерация данных аудита безопасности» выбран уровень «базовый», события, указанные в перечислениях a) — c), следует отнести к потенциально подвергаемым аудиту.

Следует обратить внимание на то, что категорирование событий, потенциально подвергаемых аудиту, иерархично. Например, если требуется «Генерация базового аудита», то все события, потенциально подвергаемые как минимальному, так и базовому аудиту, следует включить в ПЗ/ЗБ с помощью соответствующей операции назначения, за исключением случая, когда событие более высокого уровня имеет большую детализацию, чем событие более низкого уровня. Если требуется «Генерация детализированного аудита», то в ПЗ/ЗБ следует включить все события, потенциально подвергаемые аудиту (минимальному, базовому и детализированному).

По усмотрению авторов ПЗ/ЗБ в список событий, потенциально подвергаемых аудиту, могут включаться события помимо требуемых для данного уровня аудита. Например, в ПЗ/ЗБ можно заявить только возможности проведения минимального аудита, несмотря на включение большой части возможностей базового аудита, поскольку некоторые из оставшихся вступают в противоречие с ограничениями ПЗ/ЗБ (например, могут требовать сбора недоступных данных).

Функциональные возможности, выполнение которых порождает события, потенциально подвергаемые аудиту, следует устанавливать в ПЗ или ЗБ как функциональные требования.

Ниже приведены примеры типов событий, которые следует определить как потенциально подвергаемые аудиту в каждом функциональном компоненте ПЗ/ЗБ:

a) введение объектов из ОДФ в адресное пространство субъекта;

b) удаление объектов;

c) предоставление или отмена прав или возможностей доступа;

d) изменение атрибутов безопасности субъекта или объекта;

e) проверки политики, выполняемые ФБО как результат запроса субъекта;

f) использование прав доступа для обхода проверок политики;

g) использование функций идентификации и аутентификации;

h) действия, предпринимаемые оператором и/или уполномоченным пользователем (например, подавление такого механизма защиты ФБО, как доступные человеку метки);

i) ввод/вывод данных с/на заменяемые носители (например, печатные материалы, ленты, дискеты).

С.3.2 FAU_GEN.1 Генерация данных аудита

С.3.2.1 Замечания по применению для пользователя

Компонент FAU_GEN.1 «Генерация данных аудита» определяет требования по идентификации событий, потенциально подвергаемых аудиту, для которых следует генерировать записи аудита, и состав информации в этих записях.

Если ПБО не предусматривает ассоциации событий аудита с идентификатором пользователя, то достаточно применения только компонента FAU_GEN.1 «Генерация данных аудита». То же приемлемо и в случае, когда ПЗ/ЗБ содержит требования приватности. Если необходимо подключение идентификатора пользователя, допускается дополнительно использовать компонент FAU_GEN.2 «Ассоциация идентификатора пользователя».

С.3.2.2 Замечания по применению для оценщика

Имеется зависимость от FPT_STM «Метки времени». Если точное значение времени событий для данного ОО несущественно, то допускается логически обоснованный отказ от этой зависимости.

С.3.2.3 Операции

С.3.2.3.1 Выбор

В FAU_GEN.1.1 в разделе аудита функциональных требований, входящих в ПЗ/ЗБ, следует выбрать уровень событий, потенциально подвергаемых аудиту, указанный в разделе аудита других функциональных компонентов, включенных в ПЗ/ЗБ. Этот уровень может быть «минимальным», «базовым», «детализированным» или «неопределенным».

С.3.2.3.2 Назначение

В FAU_GEN.1.1 автору ПЗ/ЗБ следует составить список и других событий, потенциально подвергаемых аудиту, для включения в список событий, потенциально подвергаемых аудиту. Назначение в перечислении c) может не включать в себя ни одного события («нет») или включать события из функциональных требований, потенциально подвергаемые аудиту более высокого уровня, чем требуется в перечислении b), а также события, генерируемые при использовании специфицированного интерфейса прикладного программирования (API).

В FAU_GEN.1.2 автору ПЗ/ЗБ следует для всех событий, потенциально подвергаемых аудиту и включенных в ПЗ/ЗБ, составить список иной информации, имеющей отношение к аудиту, для включения в записи событий аудита.

С.3.3 FAU_GEN.2 Ассоциация идентификатора пользователя

С.3.3.1 Замечания по применению для пользователя

Компонент FAU_GEN.2 связан с требованием использования идентификаторов пользователей при учете событий, потенциально подвергаемых аудиту. Этот компонент следует использовать в дополнение к FAU_GEN.1 «Генерация данных аудита».

Требования аудита и приватности могут противоречить друг другу. При проведении аудита желательно знать, кто выполнил действие. Пользователь может не пожелать предавать свои действия огласке, а также может не захотеть, чтобы его идентифицировали другие лица (например, на сайте поиска работы). Требование защиты идентификатора пользователя может также содержаться в политике безопасности организации. В таких случаях цели аудита и сохранения приватности прямо противоположны друг другу. Поэтому, если при выполнении требований аудита необходимо сохранить приватность, в этом компоненте можно использовать псевдоним пользователя. Требования по определению подлинного имени пользователя по псевдониму содержатся в классе «Приватность».

С.4 Анализ аудита безопасности (FAU_SAA)

С.4.1 Замечания по применению

Семейство FAU_SAA определяет требования для автоматизированных средств, которые анализируют показатели функционирования системы и данные аудита в целях поиска возможных или реальных нарушений безопасности. Этот анализ может использоваться для поддержки как обнаружения вторжения, так и автоматической реакции на ожидаемое нарушение безопасности.

Действия для выполнения ФБО при обнаружении ожидаемого или потенциального нарушения определяются в компонентах семейства FAU_ARP «Автоматическая реакция аудита безопасности».

Для анализа в режиме реального времени данные аудита могут преобразовываться не только в формат, используемый для автоматической обработки, но также в формат, удобный для просмотра уполномоченными пользователями.

С.4.2 FAU_SAA.1 Анализ потенциального нарушения

С.4.2.1 Замечания по применению для пользователя

Компонент FAU_SAA.1 используется для определения совокупности событий, потенциально подвергаемых аудиту, появление которых (каждого отдельно или в совокупности) указывает на потенциальные нарушения ПБО, и правил, применяемых для анализа этих нарушений.

С.4.2.2 Операции

С.4.2.2.1 Назначение

В FAU_SAA.1.2 автору ПЗ/ЗБ следует определить совокупность событий, потенциально подвергаемых аудиту, проявление которых (каждого в отдельности или совместно) будет указывать на возможные нарушения ПБО.

В FAU_SAA.1.2 автору ПЗ/ЗБ следует определить любые другие правила, которые ФБО следует использовать для анализа журнала аудита. Эти правила могут включать в себя конкретные требования, согласно которым необходимо, чтобы в течение указанного периода времени (например, установленного времени суток, заданного интервала времени) произошли определенные события. Если нет никаких дополнительных правил, которые должны использовать ФБО при анализе журнала аудита, то данное назначение может быть выполнено как «нет».

С.4.3 FAU_SAA.2 Выявление аномалии, основанное на профиле

С.4.3.1 Замечания по применению для пользователя

Профиль является структурой, характеризующей поведение пользователей и/или субъектов; он описывает различные способы взаимодействия пользователей/субъектов с ФБО. Шаблоны использования для пользователей/субъектов устанавливают по отношению к различным видам результатов их деятельности, включая, например, шаблоны возникновения исключительных ситуаций, шаблоны использования ресурсов (когда, каких, как), шаблоны выполняемых действий. Метрики профиля ссылаются на способы, которыми различные виды деятельности отражаются в профиле (например, измерение использованных ресурсов, счетчики событий, таймеры).

Каждый профиль представляет собой ожидаемые шаблоны использования, выполняемые членами группы, на которую он ориентирован (целевая группа профиля). Данный шаблон может основываться на предшествующем использовании (шаблон предыстории) или на обычном использовании пользователями подобных целевых групп (ожидаемое поведение). Целевая группа профиля включает в себя одного или нескольких пользователей, взаимодействующих с ФБО. Деятельность каждого члена группы данного профиля анализируется инструментальными средствами, чтобы сравнить ее с шаблоном, представленным в профиле. Примерами целевых групп профиля являются:

a) учетная запись отдельного пользователя — один профиль для каждого пользователя;

b) идентификатор группы или учетная запись группы — один профиль для всех пользователей, которые имеют один и тот же идентификатор группы или работают, используя общую учетную запись;

c) операционная роль — один профиль на всех пользователей, выполняющих данную операционную роль;

d) система в целом — один профиль на всех пользователей системы.

Каждому члену целевой группы профиля присваивают индивидуальный рейтинг подозрительной активности, показывающий, насколько его деятельность соответствует шаблону использования системы, установленному в профиле этой группы.

Сложность средств обнаружения отклонений в значительной степени будет определяться числом целевых групп, предусмотренных в ПЗ/ЗБ, и сложностью метрики профиля.

Данный компонент используют для определения как совокупности событий, потенциально подвергаемых аудиту, появление которых (каждого в отдельности или вместе) указывает на возможные нарушения ПБО, так и

правил проведения анализа нарушений. Указанная совокупность событий и правил может быть модифицирована уполномоченным пользователем путем добавления, модификации или удаления событий или правил.

При составлении ПЗ/ЗБ следует перечислить виды деятельности, которые следует отслеживать и анализировать с использованием ФБО. Автору ПЗ/ЗБ следует особо указать, какая информация о деятельности пользователей необходима при составлении профилей использования системы.

FAU_SAA.2 «Выявление аномалии, основанное на профиле» содержит требование, чтобы ФБО сопровождали профили использования системы. Под сопровождением понимается активное участие детектора отклонений в обновлении профиля использования системы в соответствии с новыми действиями, выполняемыми членами целевой группы этого профиля. Важно, чтобы автором ПЗ/ЗБ была определена метрика представления деятельности пользователя. Индивид может выполнять тысячи различных действий, но детектор отклонений способен отобрать для контроля только некоторые из них. Результаты аномальной деятельности интегрируются в профиль так же, как и результаты нормальной деятельности (при условии выполнения мониторинга этих действий). То, что считалось отклонением четыре месяца назад, сегодня может стать нормой (и наоборот) из-за изменения условий работы пользователей. ФБО не будут способны учесть изменение ситуации, если в алгоритмах обновления профиля не отражена какая-либо аномальная деятельность пользователей.

Административные уведомления следует доводить до уполномоченного пользователя так, чтобы он понимал важность рейтинга подозрительной активности.

Автору ПЗ/ЗБ следует определить, как интерпретировать рейтинги подозрительной активности и условия, при которых в случае аномального поведения нужно обращаться к механизму семейства FAU_ARP «Автоматическая реакция аудита безопасности».

С.4.3.2 Операции

С.4.3.2.1 Выбор

В FAU_SAA.2.1 автору ПЗ/ЗБ следует определить целевую группу профиля. Один ПЗ/ЗБ может включать в себя несколько целевых групп профиля.

В FAU_SAA.2.3 автору ПЗ/ЗБ следует определить условия, при которых ФБО сообщают об аномальном поведении. Условия могут включать в себя достижение рейтингом подозрительной активности некоторого значения или основываться на определенном виде аномального поведения.

С.4.4 FAU_SAA.3 Простая эвристика атаки

С.4.4.1 Замечания по применению для пользователя

На практике случай, когда средства анализа могут точно предсказать ожидаемое нарушение безопасности, является редкой удачей. Тем не менее, существуют некоторые системные события, важные настолько, что всегда заслуживают отдельного отслеживания. Примерами таких событий являются удаление файла с ключевыми данными безопасности ФБО (например, файла паролей) или попытка удаленного пользователя получить административные привилегии. Такие события называют «характерными», поскольку они в отличие от остальных событий свидетельствуют о попытках вторжения в систему.

Сложность средств анализа в значительной степени будет зависеть от назначений, сделанных автором ПЗ/ЗБ при определении базового множества «характерных» событий.

В ПЗ/ЗБ следует перечислить события, отслеживаемые ФБО с целью их анализа. Автору ПЗ/ЗБ следует указать, на основании какой информации о событии его следует отнести к «характерным».

Административные уведомления следует доводить до уполномоченного пользователя так, чтобы он понимал значение этих событий и приемлемую реакцию на них.

При спецификации этих требований предусмотрена возможность привлечения иных источников данных, кроме данных аудита, для мониторинга системы. Это было сделано с целью расширения привлекаемых методов обнаружения вторжения, которые при анализе показателей функционирования системы используют не только данные аудита (примерами других типов источников данных являются параметры сетевых дейтаграмм, данные о ресурсах/учете или комбинации различных системных данных).

Элементы FAU_SAA.3 «Простая эвристика атаки» не требуют, чтобы реализация эвристик распознавания прямой атаки осуществлялась теми же ФБО, выполнение которых подлежит мониторингу. Поэтому компоненты, применяемые для обнаружения вторжения, можно разрабатывать независимо от системы, показатели функционирования которой подлежит анализу.

С.4.4.2 Операции

С.4.4.2.1 Назначение

В FAU_SAA.3.1 автору ПЗ/ЗБ следует идентифицировать базовое подмножество системных событий, появление которых, в отличие от иных показателей функционирования системы, может указывать на нарушение ПБО. К ним относятся как события, сами по себе указывающие на очевидные нарушения ПБО, так и события, появление которых является достаточным основанием для принятия мер предосторожности.

В FAU_SAA.3.2 автору ПЗ/ЗБ следует специфицировать информацию, используемую при определении показателей функционирования системы. Данная информация является исходной для инструментальных средств анализа показателей функционирования системы, применяемых в ОО. Эта информация может включать в себя данные аудита, комбинации данных аудита с другими системными данными и данные, отличные от данных аудита. При составлении ПЗ/ЗБ следует точно определить, какие системные события и атрибуты событий используются в качестве исходной информации.

С.4.5 FAU_SAA.4 Сложная эвристика атаки

С.4.5.1 Замечания по применению для пользователя

На практике случай, когда средства анализа могут точно предсказать ожидаемое нарушение безопасности, является редкой удачей. Тем не менее, существуют некоторые системные события, важные настолько, что всегда заслуживают отдельного отслеживания. Примерами таких событий являются удаление файла с ключевыми данными безопасности ФБО (например, файла паролей) или попытка удаленного пользователя получить административные привилегии. Такие события называют «характерными», поскольку они, в отличие от остальных событий, свидетельствуют о попытках вторжения в систему. Последовательность событий является упорядоченным множеством «характерных» событий, которые могут указывать на попытки вторжения.

Сложность средств анализа в значительной степени будет зависеть от назначений, сделанных автором ПЗ/ЗБ при определении базового множества «характерных» событий и последовательностей событий.

Автору ПЗ/ЗБ следует определить базовое множество «характерных» событий и последовательностей событий, которые будут представлены в ФБО. Дополнительные «характерные» события и последовательности событий могут быть определены разработчиком системы.

В ПЗ/ЗБ следует перечислить события, которые следует отслеживать ФБО с целью их анализа. Автору ПЗ/ЗБ следует указать, на основании какой информации о событии его можно отнести к «характерным».

Административные уведомления следует доводить до уполномоченного пользователя так, чтобы он понимал значение этих событий и приемлемую реакцию на них.

При спецификации данных требований предусмотрена возможность привлечения иных источников данных о функционировании системы, кроме данных аудита. Это сделано с целью расширения привлекаемых методов обнаружения вторжения, которые при анализе показателей функционирования системы используют не только данные аудита (примерами других типов источников данных являются параметры сетевых дейтаграмм, данные о ресурсах/учете или комбинации различных системных данных). Поэтому от автора ПЗ/ЗБ требуется специфицировать виды данных, используемых при контроле показателей функционирования системы.

Элементы FAU_SAA.4 «Сложная эвристика атаки» не требуют, чтобы реализация эвристик распознавания прямой атаки осуществлялась теми же ФБО, выполнение которых подлежит мониторингу. Поэтому компоненты, применяемые для обнаружения вторжения, можно разрабатывать независимо от системы, показатели функционирования которой подлежат анализу.

С.4.5.2 Операции

С.4.5.2.1 Назначение

В FAU_SAA.4.1 автору ПЗ/ЗБ следует идентифицировать базовое множество перечня последовательностей системных событий, совпадение которых типично для известных сценариев проникновения. Эти последовательности событий представляют известные сценарии проникновения. Каждое событие в последовательности следует сопоставлять с контролируемыми системными событиями, и если в итоге все системные события произошли в действительности, это подтверждает (отображает) попытку проникновения.

В FAU_SAA.4.1 автору ПЗ/ЗБ следует специфицировать базовое подмножество системных событий, появление которых, в отличие от иных показателей функционирования системы, может указывать на нарушение ПБО. К ним относятся как события, сами по себе указывающие на очевидные нарушения ПБО, так и события, появление которых является достаточным основанием для принятия мер предосторожности.

В FAU_SAA.4.2 автору ПЗ/ЗБ следует специфицировать информацию, используемую при определении показателей функционирования системы. Информация является исходной для инструментальных средств анализа показателей функционирования системы, применяемых в ОО. В эту информацию могут входить данные аудита, комбинации данных аудита с другими системными данными и данные, отличные от данных аудита. При составлении ПЗ/ЗБ следует точно определить, какие системные события и атрибуты событий используются в качестве исходной информации.

С.5 Просмотр аудита безопасности (FAU_SAR)

С.5.1 Замечания по применению

Семейство FAU_SAR определяет требования, относящиеся к просмотру информации аудита.

Следует, чтобы функции предоставляли возможность отбирать данные аудита до или после сохранения, обеспечивая, например, возможность избирательного просмотра данных о следующих действиях:

- действия одного или нескольких пользователей (например идентификация, аутентификация, вход в ОО и действия по управлению доступом);
- действия, выполненные над определенным объектом или ресурсом ОО;
- все события из указанного множества исключительных событий, подвергающихся аудиту;
- действия, связанные с определенным атрибутом ПБО.

Виды просмотра различаются по функциональным возможностям. Обычный просмотр позволяет только просматривать данные аудита. Выборочный просмотр более сложен и содержит требования возможности поиска на основании одного или нескольких критериев с логическими (то есть типа «и/или») отношениями, сортировки или фильтрации данных аудита до их просмотра.

С.5.2 FAU_SAR.1 Просмотр аудита

С.5.2.1 Обоснование

Данный компонент обеспечит уполномоченным пользователям возможность получения и интерпретации информации. В случае пользователя-человека данная информация должна представляться в понятном для человека виде. В случае внешних сущностей ИТ информация должна быть однозначно представлена в электронном виде.

С.5.2.2 Замечания по применению для пользователя

Компонент FAU_SAR.1 используется для определения возможности читать записи аудита для пользователей и/или уполномоченных пользователей. Эти записи аудита будут представляться в удобном для пользователя виде. У пользователей различных типов могут быть разные требования к представлению данных аудита.

Содержание записей аудита, предназначенных для просмотра, может быть установлено заранее.

С.5.2.3 Операции

С.5.2.3.1 Назначение

В FAU_SAR.1.1 автору ПЗ/ЗБ следует указать уполномоченных пользователей, которые могут просматривать данные аудита. Если это необходимо, автор ПЗ/ЗБ может указать роли безопасности (см. FMT_SMR.1 «Роли безопасности»).

В FAU_SAR.1.1 автору ПЗ/ЗБ следует указать, какие виды информации может получать из записей аудита данный пользователь. Примерами являются «вся информация», «идентификатор субъекта», «вся информация из записей аудита, имеющих ссылки на этого пользователя».

С.5.3 FAU_SAR.2 Ограниченный просмотр аудита

С.5.3.1 Замечания по применению для пользователя

В компоненте FAU_SAR.2 определяется, что ни один пользователь, не указанный в FAU_SAR.1 «Просмотр аудита», не сможет читать записи аудита.

С.5.4 FAU_SAR.3 Выборочный просмотр аудита

С.5.4.1 Замечания по применению для пользователя

Компонент FAU_SAR.3 определяет возможность выборочного просмотра данных аудита. Если просмотр проводится на основе нескольких критериев, то необходимо, чтобы они были логически связаны (например, операциями «и», «или»), а инструментальные средства предоставили возможность обработки данных аудита (например, сортировки, фильтрации).

С.5.4.2 Операции

С.5.4.2.1 Выбор

В FAU_SAR.3.1 автору ПЗ/ЗБ следует выбрать, какие действия (поиск, сортировку и/или упорядочение) могут выполнять ФБО.

С.5.4.2.2 Назначение

В FAU_SAR.3.1 автору ПЗ/ЗБ следует установить критерии, возможно логически связанные, на основании которых проводится выбор данных аудита для просмотра. Логические связи используют при определении, проводится ли операция над отдельными атрибутами или совокупностью атрибутов. Примерами такого назначения могут быть прикладная задача, учетные данные и/или место нахождения пользователя. В данном случае операцию допускается специфицировать с помощью любой комбинации этих трех атрибутов.

С.6 Выбор событий аудита безопасности (FAU_SEL)

С.6.1 Замечания по применению

Семейство FAU_SEL «Выбор событий аудита безопасности» содержит требования, связанные с идентификацией того, какие события, потенциально подвергаемые аудиту, действительно подлежат аудиту. События, потенциально подвергаемые аудиту, определяются в семействе FAU_GEN «Генерация данных аудита безопасности», но для выполнения аудита этих событий их следует определить как выбираемые в компоненте FAU_SEL.1.

Это семейство обеспечивает возможность предотвращения разрастания журнала аудита до таких размеров, когда он становится бесполезным, путем определения приемлемой избирательности событий аудита безопасности.

С.6.2 FAU_SEL.1 Избирательный аудит

С.6.2.1 Замечания по применению для пользователя

Компонент FAU_SEL.1 определяет критерии, используемые для отбора событий, которые будут подвергнуты аудиту. Критерии могут допускать включение или исключение событий из совокупности событий, подвергающихся аудиту, на основе атрибутов пользователей, субъектов и объектов или типов событий.

Для этого компонента не предполагается существование идентификаторов отдельных пользователей, что позволяет применять его для таких ОО, как например, маршрутизаторы, которые могут не поддерживать понятие пользователей.

В распределенной среде в качестве критерия для отбора событий, которые будут подвергнуты аудиту, может быть использован идентификатор узла сети.

Права уполномоченных пользователей по просмотру или модификации условий отбора будут регулироваться функциями управления компонента FMT_MTD.1 «Управление данными ФБО».

С.6.2.2 Операции

С.6.2.2.1 Выбор

В FAU_SEL.1.1 автору ПЗ/ЗБ следует выбрать, на каких атрибутах безопасности основана избирательность аудита: идентификатор объекта, идентификатор пользователя, идентификатор субъекта, идентификатор узла сети или тип события.

С.6.2.2.2 Назначение

В FAU_SEL.1.1 автору ПЗ/ЗБ следует определить дополнительные атрибуты, на которых основана избирательность аудита. Если нет дополнительных правил, на которых основана избирательность аудита, то данное назначение может быть выполнено как «нет».

С.7 Хранение данных аудита безопасности (FAU_STG)

В.7.1 Замечания по применению

Семейство FAU_STG описывает требования по хранению данных аудита для последующего использования, включая требования контроля за потерей информации аудита из-за сбоя системы, нападения и/или превышения объема памяти, отведенной для хранения.

С.7.2 FAU_STG.1 Защищенное хранение журнала аудита

С.7.2.1 Замечания по применению для пользователя

Поскольку в распределенной среде расположение журнала аудита, который находится в ОДФ, не обязательно совпадает с расположением функций генерации данных аудита, автор ПЗ/ЗБ может потребовать обеспечения неотказуемости отправления записи аудита или проведения аутентификации отправителя перед занесением записи в журнал аудита.

ФБО будут защищать журнал аудита от несанкционированного уничтожения или модификации. Отметим, что в некоторых системах аудитор (роль) может не располагать полномочиями на удаление записей аудита в течение определенного периода времени.

С.7.2.2 Операции

С.7.2.2.1 Выбор

В FAU_STG.1.2 автору ПЗ/ЗБ следует специфицировать, должны ли ФБО предотвращать или только выявлять модификацию журнала аудита. Может быть выбран только один из этих вариантов.

С.7.3 FAU_STG.2 Гарантии доступности данных аудита

С.7.3.1 Замечания по применению для пользователя

Компонент FAU_STG.2 позволяет автору ПЗ/ЗБ определить метрику для журнала аудита.

Поскольку в распределенной среде расположение журнала аудита, который находится в ОДФ, не обязательно совпадает с расположением функций генерации данных аудита, автор ПЗ/ЗБ может потребовать обеспечения неотказуемости отправления записи аудита или проведения аутентификации отправителя перед занесением записи в журнал аудита.

С.7.3.2 Операции

С.7.3.2.1 Выбор

В FAU_STG.2.2 автору ПЗ/ЗБ следует специфицировать, должны ли ФБО предотвращать или только выявлять модификацию журнала аудита. Может быть выбран только один из этих вариантов.

С.7.3.2.2 Назначение

В FAU_STG.2.3 автору ПЗ/ЗБ следует специфицировать метрику, которую ФБО должны обеспечить для журнала аудита. Эта метрика ограничивает потерю данных указанием максимального числа записей, которые необходимо сохранять, или временем, в течение которого обеспечивается хранение записей. Примером метрики может быть число 100000, указывающее, что журнал аудита рассчитан на 100000 записей.

С.7.3.2.3 Выбор

В FAU_STG.2.3 автору ПЗ/ЗБ следует специфицировать условие, при котором ФБО должны быть все еще способны сопровождать определенный объем данных аудита. Это может быть одно из следующих условий: переполнение журнала аудита, сбой, атака.

С.7.4 FAU_STG.3 Действия в случае возможной потери данных аудита

С.7.4.1 Замечания по применению для пользователя

Компонент FAU_STG.3 содержит требование выполнения определенных действий в случае превышения журналом аудита некоторого заранее определяемого предела.

С.7.4.2 Операции

С.7.4.2.1 Назначение

В FAU_STG.3.1 автору ПЗ/ЗБ следует указать значение заранее определяемого предела принятого ограничения. Если функции управления допускают, что уполномоченный пользователь может его изменить, то предел принятого ограничения является значением по умолчанию. Автор ПЗ/ЗБ может позволить уполномоченному пользователю всегда определять это ограничение. В этом случае назначение может быть, например, следующим: «ограничение устанавливает уполномоченный пользователь».

В FAU_STG.3.1 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые в случае возможного переполнения журнала аудита. Эти действия могут включать в себя информирование уполномоченного пользователя.

С.7.5 FAU_STG.4 Предотвращение потери данных аудита

С.7.5.1 Замечания по применению для пользователя

В компоненте FAU_STG.4 определяется режим функционирования ОО при переполнении журнала аудита: игнорирование записей аудита либо приостановка функционирования ОО для предотвращения возникновения событий, подвергающихся аудиту. Устанавливают, что независимо от принятого решения, уполномоченный пользователь, имеющий соответствующие права, может продолжать генерировать события (действия), подвергающиеся аудиту. Это делается потому, что в противном случае уполномоченный администратор не смог бы осуществить даже перезапуск системы. Следует также предусмотреть действия, предпринимаемые ФБО при переполнении журнала аудита, поскольку игнорирование событий, способствующее лучшей доступности ОО, приведет также к возможности совершать действия, не оставляя о них записей и не относя их на счет определенного пользователя.

С.7.5.2 Операции

С.7.5.2.1 Выбор

В FAU_STG.4.1 автору ПЗ/ЗБ следует выбрать, должны ли ФБО в случае переполнения журнала аудита игнорировать проведение аудита, следует ли предотвращать действия, подвергающиеся аудиту, или следует новые записи помещать вместо старых. Может быть выбран только один из вариантов.

С.7.5.2.2 Назначение

В FAU_STG.4.1 автору ПЗ/ЗБ следует определить другие действия, предпринимаемые в случае сбоя хранения данных аудита, такие как информирование уполномоченного пользователя. Если нет никаких других действий, которые нужно предпринять в случае сбоя хранения данных аудита, то данное назначение может быть выполнено как «нет».

Федеральное агентство по техническому регулированию и метрологии

Приложение D
(обязательное)

Связь (FCO)

Класс FCO «Связь» содержит требования, которые имеют важное значение для ОО, используемого для обмена информацией. Семейства этого класса предназначены для обеспечения неотказуемости (то есть невозможности отрицать факт отправления или получения передаваемой информации).

В этом классе использовано понятие «информация». Информация здесь интерпретируется как объект, предназначенный для передачи, который может содержать сообщение электронной почты, файл или совокупность атрибутов предопределенных типов.

Термины «доказательство отправления» и «доказательство получения» приняты в литературе. Однако необходимо иметь в виду, что термин «доказательство» может интерпретироваться как в юридическом смысле, так и в форме математического обоснования. В компонентах этого класса «доказательство» понимается как «свидетельство», то есть ФБО демонстрируют неотказуемость обмена информацией.

Декомпозиция класса FCO «Связь» на составляющие его компоненты показана на рисунке D.1.

Рисунок D.1 — Декомпозиция класса FCO «Связь»

D.1 Неотказуемость отправления (FCO_NRO)

D.1.1 Замечания для пользователя

«Неотказуемость отправления» определяет требования по предоставлению пользователям/субъектам свидетельства идентичности отправителя некоторой информации. Отправитель не сможет отрицать факт передачи информации, поскольку свидетельство отправления (например цифровая подпись) доказывает связь между отправителем и переданной информацией. Получатель или третья сторона может проверить свидетельство отправления. Не следует допускать возможность подделки этого свидетельства.

Если информация или ассоциированные с ней атрибуты каким-либо образом изменяются, подтверждение правильности свидетельства отправления может дать отрицательный результат. Поэтому автору ПЗ/ЗБ следует предусмотреть включение в ПЗ/ЗБ требований целостности из компонента FDP_UIT.1 «Целостность передаваемых данных».

Неотказуемость связана с несколькими различными ролями, выполняемыми одним или несколькими субъектами. Во-первых, это субъект, который запрашивает свидетельство отправления (только в FCO_NRO.1 «Избирательное доказательство отправления»). Во-вторых, получатель и/или другие субъекты, которым предоставляется свидетельство (например, нотариус). В-третьих, субъект, который запрашивает верификацию свидетельства отправления, например, получатель или третье лицо, например, арбитр.

Автору ПЗ/ЗБ необходимо специфицировать условия, выполнение которых обеспечивает возможность верифицировать правильность свидетельства. Примером такого условия может быть возможность верификации свидетельства в течение суток. Эти условия позволяют также приспособить неотказуемость к юридическим требованиям, таким, например, как наличие возможности предоставления свидетельства в течение нескольких лет.

В большинстве случаев идентификатор отправителя будет совпадать с идентификатором пользователя, который инициировал передачу. В некоторых случаях автор ПЗ/ЗБ может не пожелать экспортировать идентификатор пользователя. В этом случае ему необходимо принять решение о том, нужно ли привлекать этот класс или использовать идентификатор провайдера услуг связи или идентификатор узла сети.

Автор ПЗ/ЗБ может использовать момент передачи информации в дополнение к идентификатору пользователя или вместо него. Например, запросы будут рассмотрены, если они были отправлены до известного срока. В таком случае требования могут быть приспособлены к использованию меток времени (времени отправления).

D.1.2 FCO_NRO.1 Избирательное доказательство отправления

D.1.2.1 Операции

D.1.2.1.1 Назначение

В FCO_NRO.1.1 автору ПЗ/ЗБ следует указать типы субъектов информации, для которых требуется предоставление свидетельства отправления, например, сообщения электронной почты.

D.1.2.1.2 Выбор

В FCO_NRO.1.1 автору ПЗ/ЗБ следует специфицировать пользователя/субъект, который может запросить свидетельство отправления.

D.1.2.1.3 Назначение

В FCO_NRO.1.1 автору ПЗ/ЗБ в соответствии с выбором следует специфицировать третьих лиц, которые могут запросить свидетельство отправления. Третьим лицом может быть арбитр, судья или юридический орган.

В FCO_NRO.1.2 автору ПЗ/ЗБ следует внести в список те атрибуты, которые должны быть связаны с информацией, например идентификатор отправителя, время и место отправления.

В FCO_NRO.1.2 автору ПЗ/ЗБ следует внести в список те информационные поля, атрибуты которых обеспечивают свидетельство отправления, например текст сообщения.

D.1.2.1.4 Выбор

В FCO_NRO.1.3 автору ПЗ/ЗБ следует специфицировать пользователя/субъект, который может верифицировать свидетельство отправления.

D.1.2.1.5 Назначение

В FCO_NRO.1.3 автору ПЗ/ЗБ следует сформировать список ограничений, при которых может быть верифицировано свидетельство. Например, свидетельство может быть верифицировано только в течение суток. Допустимо назначение «немедленно» или «неограниченно».

В FCO_NRO.1.3 автору ПЗ/ЗБ в соответствии с выбором следует специфицировать третью сторону, которая может верифицировать свидетельство отправления.

D.1.3 FCO_NRO.2 Принудительное доказательство отправления

D.1.3.1 Операции

D.1.3.1.1 Назначение

В FCO_NRO.2.1 автору ПЗ/ЗБ следует указать типы субъектов информации, для которых требуется предоставление свидетельства отправления, например сообщения электронной почты.

В FCO_NRO.2.2 автору ПЗ/ЗБ следует внести в список те атрибуты, которые должны быть связаны с информацией, например идентификатор отправителя, время и место отправления.

В FCO_NRO.2.2 автору ПЗ/ЗБ следует внести в список те информационные поля, атрибуты которых обеспечивают свидетельство отправления, например текст сообщения.

D.1.3.1.2 Выбор

В FCO_NRO.2.3 автору ПЗ/ЗБ следует специфицировать пользователя/субъект, который может верифицировать свидетельство отправления.

D.1.3.1.3 Назначение

В FCO_NRO.2.3 автору ПЗ/ЗБ следует сформировать список ограничений, при которых может быть верифицировано свидетельство. Например, свидетельство может быть верифицировано только в течение суток. Допустимо назначение «немедленно» или «неограниченно».

В FCO_NRO.2.3 автору ПЗ/ЗБ в соответствии с выбором следует специфицировать третью сторону, которая может верифицировать свидетельство отправления. Третьей стороной может быть арбитр, судья или юридический орган.

D.2 Неотказуемость получения (FCO_NRR)

D.2.1 Замечания для пользователя

«Неотказуемость получения» определяет требования по предоставлению пользователям/субъектам свидетельства о том, что информация была принята получателем. Получатель не сможет отрицать факт приема информации, поскольку свидетельство получения (например цифровая подпись) доказывает связь между атрибутами получателя и информацией. Отправитель или третья сторона может проверить свидетельство получения. Не следует допускать возможность подделки этого свидетельства.

Следует иметь в виду, что предоставление свидетельства получения информации означает только, что она доставлена, а не что информация обязательно прочитана или понята.

Если информация или ассоциированные с ней атрибуты каким-либо образом изменяются, проверка правильности свидетельства получения может дать отрицательный результат. Поэтому автору ПЗ/ЗБ следует предусмотреть включение в ПЗ/ЗБ требований целостности из компонента FDP_UIT.1 «Целостность передаваемых данных».

Неотказуемость связана с несколькими различными ролями, выполняемыми одним или несколькими субъектами. Во-первых, это субъект, который запрашивает свидетельство получения (только в FCO_NRR.1 «Избирательное доказательство получения»). Во-вторых, получатель и/или другие субъекты, которым предоставляется свидетельство (например нотариус). В-третьих, субъект, который запрашивает верификацию свидетельства получения, например, отправитель или третья сторона, например арбитр.

Автору ПЗ/ЗБ необходимо специфицировать условия, выполнение которых обеспечивает возможность верифицировать правильность свидетельства. Примером такого условия может быть возможность верификации свидетельства в течение суток. Эти условия позволяют также привести требование неотказуемости в соответствие с юридическими требованиями, такими, например, как наличие возможности предоставления свидетельства в течение нескольких лет.

В большинстве случаев идентификатор получателя будет совпадать с идентификатором пользователя, который принял передачу. В некоторых случаях автор ПЗ/ЗБ может не пожелать передавать сведения об идентификаторе пользователя. В этом случае ему необходимо принять решение, нужно ли привлекать этот класс или же использовать идентификатор провайдера услуг связи или идентификатор узла сети.

Автор ПЗ/ЗБ может использовать момент получения информации в дополнение к идентификатору пользователя или вместо него. Например, заявки о предложениях будут рассмотрены, если поступили до установленного срока. Когда предложение ограничено известным сроком, заказы будут рассмотрены, если они получены до этого срока. В этом случае данные требования могут предусматривать использование метки времени (времени получения).

D.2.2 FCO_NRR.1 Избирательное доказательство получения

D.2.2.1 Операции

D.2.2.1.1 Назначение

В FCO_NRR.1.1 автору ПЗ/ЗБ следует указать типы субъектов информации, для которых требуется предоставление свидетельства получения, например сообщения электронной почты.

D.2.2.1.2 Выбор

В FCO_NRR.1.1 автору ПЗ/ЗБ следует специфицировать пользователя/субъект, который может запросить свидетельство получения.

D.2.2.1.3 Назначение

В FCO_NRR.1.1 автору ПЗ/ЗБ в соответствии с выбором следует специфицировать третьи стороны, которые могут запросить свидетельство получения. Третьей стороной может быть арбитр, судья или юридический орган.

В FCO_NRR.1.2 автору ПЗ/ЗБ следует внести в список те атрибуты, которые должны быть связаны с информацией, например идентификатор получателя, время и место получения.

В FCO_NRR.1.2 автору ПЗ/ЗБ следует внести в список те информационные поля, атрибуты которых обеспечивают свидетельство получения, например текст сообщения.

D.2.2.1.4 Выбор

В FCO_NRR.1.3 автору ПЗ/ЗБ следует специфицировать пользователя/субъект, который может верифицировать свидетельство получения.

D.2.2.1.5 Назначение

В FCO_NRR.1.3 автору ПЗ/ЗБ следует сформировать список ограничений, при которых может быть верифицировано свидетельство. Например, свидетельство может быть верифицировано только в течение суток. Допустимо назначение «немедленно» или «неограниченно».

В FCO_NRR.1.3 автору ПЗ/ЗБ в соответствии с выбором следует специфицировать третью сторону, которая может верифицировать свидетельство получения.

D.2.3 FCO_NRR.2 Принудительное доказательство получения

D.2.3.1 Операции

D.2.3.1.1 Назначение

В FCO_NRR.2.1 автору ПЗ/ЗБ следует указать типы субъектов информации, для которых требуется предоставление свидетельства получения, например сообщения электронной почты.

В FCO_NRR.2.2 автору ПЗ/ЗБ следует внести в список те атрибуты, которые должны быть связаны с информацией, например идентификатор получателя, время и место получения.

В FCO_NRR.2.2 автору ПЗ/ЗБ следует внести в список те информационные поля, атрибуты которых обеспечивают свидетельство получения, например текст сообщения.

D.2.3.1.2 Выбор

В FCO_NRR.2.3 автору ПЗ/ЗБ следует специфицировать пользователя/субъект, который может верифицировать свидетельство получения.

D.2.3.1.3 Назначение

В FCO_NRR.2.3 автору ПЗ/ЗБ следует сформировать список ограничений, при которых может быть верифицировано свидетельство. Например, свидетельство может быть верифицировано только в течение суток. Допустимо назначение «немедленно» или «неограниченно».

В FCO_NRR.2.3 автору ПЗ/ЗБ в соответствии с выбором следует специфицировать третьи стороны, которые могут верифицировать свидетельство получения. Третьей стороной может быть арбитр, судья или юридический орган.

Федеральное агентство по техническому регулированию и метрологии

Приложение Е
(обязательное)

Криптографическая поддержка (FCS)

ФБО могут использовать криптографические функциональные возможности для содействия достижению некоторых, наиболее важных целей безопасности. К ним относятся (но ими не ограничиваются) следующие цели: идентификация и аутентификация, неотказуемость, доверенный маршрут, доверенный канал, разделение данных. Класс FCS применяют, если ОО имеет криптографические функции, которые могут быть реализованы аппаратными, программно-аппаратными и/или программными средствами.

Класс FCS «Криптографическая поддержка» состоит из двух семейств: FCS_CKM «Управление криптографическими ключами» и FCS_COP «Криптографические операции». В семействе FCS_CKM рассмотрены аспекты управления криптографическими ключами, тогда как в семействе FCS_COP рассмотрено практическое применение этих криптографических ключей.

Для каждого метода генерации криптографических ключей, реализованного в ОО, автору ПЗ/ЗБ следует применить компонент FCS_CKM.1 «Генерация криптографических ключей».

Для каждого метода распределения криптографических ключей, реализованного в ОО, автору ПЗ/ЗБ следует применить компонент FCS_CKM.2 «Распределение криптографических ключей».

Для каждого метода доступа к криптографическим ключам, реализованного в ОО, автору ПЗ/ЗБ следует применить компонент FCS_CKM.3 «Доступ к криптографическим ключам».

Для каждого метода уничтожения криптографических ключей, реализованного в ОО, автору ПЗ/ЗБ следует применить компонент FCS_CKM.4 «Уничтожение криптографических ключей».

Для каждой из криптографических операций, реализованных в ОО, таких как цифровая подпись, шифрование данных, согласование ключей, хэширование и т. д., автору ПЗ/ЗБ следует применить компонент FCS_COP.1 «Криптографические операции».

Криптографические функциональные возможности применимы для достижения целей безопасности, специфицированных в классе FCO «Связь», а также в семействах FDP_DAU «Аутентификация данных», FDP_SDI «Целостность хранимых данных», FDP_UCT «Защита конфиденциальности данных пользователя при передаче между ФБО», FDP_UIT «Защита целостности данных пользователя при передаче между ФБО», FIA_SOS «Спецификация секретов», FIA_UAU «Аутентификация пользователя». В случае, если криптографические функциональные возможности используют для достижения целей безопасности из других классов, цели, требующие применения криптографических средств, специфицируют в отдельных компонентах. Цели класса FSC «Криптографическая поддержка» должны использоваться, если потребители нуждаются в криптографических функциональных возможностях ОО.

Декомпозиция класса FCS «Криптографическая поддержка» на составляющие его компоненты показана на рисунке Е.1.

Рисунок Е.1 — Декомпозиция класса FSC «Криптографическая поддержка»

Е.1 Управление криптографическими ключами (FCS_CKM)

Е.1.1 Замечания для пользователя

Криптографическими ключами необходимо управлять на протяжении всего их существования. Основными этапами жизненного цикла криптографических ключей являются: генерация, распределение, ввод в действие, хранение, доступ (например, к резервному копированию, передаче на хранение, архивации и восстановлению) и уничтожение.

Поскольку ОО не обязательно используют на всех этапах жизненного цикла ключей, то им может выполняться, например, только генерация и уничтожение криптографических ключей.

Семейство FCS_CKM предназначено для поддержки жизненного цикла и поэтому определяет требования к следующим действиям с криптографическими ключами: генерация, распределение, доступ к ним и их уничтожение. Это семейство следует использовать в случаях, если имеются функциональные требования управления криптографическими ключами.

Если в ПЗ/ЗБ включен компонент семейства FAU_GEN «Генерация данных аудита безопасности», то аудиту следует подвергать события, связанные с:

a) атрибутами объекта, которые могут содержать сведения о пользователе данного криптографического ключа, роли пользователя, криптографических операциях, в которых используется данный криптографический ключ, идентификаторе криптографического ключа и его сроке действия;

b) параметрами объекта, включая значения криптографического ключа (ключей), за исключением любой чувствительной информации, например, секретных или приватных криптографических ключей.

Для генерации криптографических ключей обычно используют случайные числа. Тогда вместо FIA_SOS.2 «Генерация секретов ФБО» следует использовать компонент FCS_CKM.1. Компонент FIA_SOS.2 следует применять, если генерация случайных чисел требуется для иных целей.

Е.1.2 FCS_CKM.1 Генерация криптографических ключей

Е.1.2.1 Замечания по применению для пользователя

Компонент FCS_CKM.1 содержит требования по определению длины криптографических ключей и метода их генерации, что может быть сделано в соответствии с некоторыми принятыми стандартами. Его следует использовать для определения длины криптографических ключей и метода (то есть алгоритма) их генерации. Для одного и того же метода и нескольких значений длины ключа этот компонент необходимо использовать только один раз. Длина ключа может быть одной и той же или разной для различных сущностей, а также быть входным либо выходным значением алгоритма.

Е.1.2.2 Операции

Е.1.2.2.1 Назначение

В FCS_CKM.1.1 автору ПЗ/ЗБ следует определить, какой алгоритм генерации криптографических ключей будет использоваться.

В FCS_CKM.1.1 автору ПЗ/ЗБ следует определить, какой длины криптографические ключи будут использоваться. Следует, чтобы длина ключа соответствовала выбранному алгоритму и предполагаемому применению ключа.

В FCS_CKM.1.1 автору ПЗ/ЗБ следует определить стандарт, который устанавливает метод генерации криптографических ключей. При этом можно ссылаться на один или несколько действующих опубликованных стандартов, например, на международные, национальные стандарты или стандарты предприятия.

Е.1.3 FCS_CKM.2 Распределение криптографических ключей

Е.1.3.1 Замечания по применению для пользователя

Компонент FCS_CKM.2 содержит требование определения метода распределения криптографических ключей, который может соответствовать некоторому назначенному стандарту.

Е.1.3.2 Операции

Е.1.3.2.1 Назначение

В FCS_CKM.2.1 автору ПЗ/ЗБ следует определить, какой метод используется для распределения криптографических ключей.

В FCS_CKM.2.1 автору ПЗ/ЗБ следует определить назначенный стандарт, в котором описан используемый метод распределения криптографических ключей. При этом можно ссылаться на один или несколько действующих опубликованных стандартов, например, на международные, национальные стандарты или стандарты предприятия.

Е.1.4 FCS_CKM.3 Доступ к криптографическим ключам

Е.1.4.1 Замечания по применению для пользователя

Компонент FCS_CKM.3 содержит требование определения метода доступа к криптографическим ключам, который может соответствовать некоторому назначенному стандарту.

Е.1.4.2 Операции

Е.1.4.2.1 Назначение

В FCS_CKM.3.1 автору ПЗ/ЗБ следует определить используемый тип доступа к криптографическим ключам. Примерами операций с криптографическими ключами, к которым предоставляется доступ, являются (но не ограничиваются ими): резервное копирование, архивирование, передача на хранение и восстановление.

В FCS_CKM.3.1 автору ПЗ/ЗБ следует определить, какой метод будет использоваться для доступа к криптографическим ключам.

В FCS_CKM.3.1 автору ПЗ/ЗБ следует определить назначенный стандарт, в котором описан используемый метод доступа к криптографическим ключам. При этом можно ссылаться на один или несколько действующих опубликованных стандартов, например, на международные, национальные стандарты или стандарты предприятия.

E.1.5 FCS_CKM.4 Уничтожение криптографических ключей

E.1.5.1 Замечания по применению для пользователя

Компонент FCS_CKM.4 содержит требование определения метода уничтожения криптографических ключей, который может соответствовать некоторому назначенному стандарту.

E.1.5.2 Операции

E.1.5.2.1 Назначение

В FCS_CKM.4.1 автору ПЗ/ЗБ следует определить, какой метод будет использован для уничтожения криптографических ключей.

В FCS_CKM.4.1 автору ПЗ/ЗБ следует определить назначенный стандарт, в котором описан используемый метод ликвидации криптографических ключей. При этом можно ссылаться на один или несколько действующих опубликованных стандартов, например, на международные, национальные стандарты или стандарты предприятия.

E.2 Криптографические операции (FCS_COP)

E.2.1 Замечания для пользователя

У криптографической операции могут быть один или несколько криптографических режимов операции, ассоциированных с ней. В этом случае его (их) необходимо определить. Примерами криптографических режимов операции являются сцепление блоков зашифрованного текста, осуществление обратной связи по выходу, применение электроной книги кодов и осуществление обратной связи по зашифрованному тексту.

Криптографические операции могут использоваться для поддержки одной или нескольких функций безопасности ОО. Может возникнуть необходимость в итерациях компонента FCS_COP в зависимости от:

a) прикладной программы пользователя, для которой понадобилась данная функция;

b) применения различных криптографических алгоритмов и/или длины криптографических ключей;

c) типа или чувствительности обрабатываемых данных.

Если в ПЗ/ЗБ включен компонент семейства FAU_GEN «Генерация данных аудита безопасности», то аудиту следует подвергать события, связанные с:

a) типами криптографических операций, к которым могут относиться генерация и/или верификация цифровых подписей, генерация криптографических контрольных сумм для обеспечения целостности и/или верификации контрольных сумм, хэширование (вычисление хэш-образа сообщения), зашифрование и/или расшифрование данных, зашифрование и/или расшифрование криптографических ключей, согласование криптографических ключей и генерация случайных чисел;

b) атрибутами субъекта, которые могут включать в себя как роли субъектов, так и пользователей, ассоциированных с этими субъектами;

c) атрибутами объекта, которые могут включать в себя сведения о пользователях криптографического ключа, роли пользователя, криптографической операции, для которой используется данный ключ, идентификаторе криптографического ключа и сроке его действия.

E.2.2 FCS_COP.1 Криптографические операции

E.2.2.1 Замечания по применению для пользователя

В этом компоненте содержатся требования указания криптографических алгоритмов и длины ключей, используемых при выполнении определяемых криптографических операций и основанных на некотором выбранном стандарте.

E.2.2.2 Операции

E.2.2.2.1 Назначение

В FCS_COP.1.1 автору ПЗ/ЗБ следует определить выполняемые криптографические операции. Типичными криптографическими операциями являются генерация и/или верификация цифровых подписей, генерация криптографических контрольных сумм для обеспечения целостности и/или верификации контрольных сумм, безопасное хэширование (вычисление хэш-образа сообщения), зашифрование и/или расшифрование данных, зашифрование и/или расшифрование криптографических ключей, согласование криптографических ключей и генерация случайных чисел. Криптографические операции могут выполняться с данными как пользователя, так и ФБО.

В FCS_COP.1.1 автору ПЗ/ЗБ следует определить, какой криптографический алгоритм будет использован.

В FCS_COP.1.1 автору ПЗ/ЗБ следует определить, какой длины криптографические ключи будут использоваться. Необходимо, чтобы длина ключа соответствовала выбранному алгоритму и предполагаемому применению ключа.

В FCS_COP.1.1 автору ПЗ/ЗБ следует определить стандарт, в соответствии с которым выполняются идентифицированные криптографические операции. При этом можно ссылаться на один или несколько действующих опубликованных стандартов, например, на международные, национальные стандарты или стандарты предприятия.

Федеральное агентство по техническому регулированию и метрологии

Приложение F
(обязательное)

Защита данных пользователя (FDP)

Класс FDP «Защита данных пользователя» содержит семейства, определяющие требования к функциям безопасности ОО и политикам функций безопасности ОО, связанным с защитой данных пользователя. Этот класс отличается от классов FIA и FPT тем, что определяет компоненты для защиты данных пользователя, тогда как класс FIA определяет компоненты для защиты атрибутов, ассоциированных с пользователем, а класс FPT — для защиты информации ФБО.

Данный класс не содержит явного требования мандатного управления доступом (Mandatory Access Controls — MAC) или традиционного дискреционного управления доступом (Discretionary Access Controls — DAC); тем не менее, такие требования могут быть выражены с использованием компонентов этого класса.

Класс FDP «Защита данных пользователя» не касается явно конфиденциальности, целостности или доступности, чаще всего сочетающихся в политике и механизмах. Тем не менее в ПЗ/ЗБ политику безопасности ОО необходимо адекватно распространить на эти три цели.

Заключительным аспектом этого класса является то, что он специфицирует управление доступом в терминах «операций». «Операция» определяется как специфический тип доступа к конкретному объекту. В зависимости от уровня абстракции описания автором ПЗ/ЗБ этих операций, они могут определяться как «чтение» и/или «запись» или как более сложные операции, например «обновление базы данных».

Политики управления доступом определяют доступ к хранилищам информации. Атрибуты представлены атрибутами места хранения. Как только информация считана из хранилища, лицо, имеющее доступ к ней, может бесконтрольно использовать эту информацию, включая ее запись в различные хранилища с другими атрибутами. Напротив, политики управления информационными потоками контролируют доступ к информации, независимо от места ее хранения. Атрибуты информации, которые могут быть (или не быть, как в случае многоуровневых баз данных) ассоциированы с атрибутами места хранения, остаются с информацией при ее перемещении. Получатель доступа к информации не имеет возможности изменять ее атрибуты без явного разрешения.

Класс FDP не рассматривается как полная таксономия политик управления доступом ИТ, поскольку могут быть предложены иные. В него включены те политики, для которых спецификация требований основана на накопленном опыте применения существующих систем. Возможны и другие формы доступа, которые не учтены в имеющихся формулировках.

Так, можно представить себе задачу иметь способы управления информационным потоком, определяемые пользователем (например, реализующие автоматизированную обработку информации «Не для посторонних»). Подобные понятия могли бы быть учтены путем уточнения или расширения компонентов класса FDP.

Наконец, при рассмотрении компонентов класса FDP «Защита данных пользователя» важно помнить, что эти компоненты содержат требования для функций, которые могут быть реализованы механизмами, которые служат или могли бы служить и для других целей. Например, возможно формирование политики управления доступом (FDP_ACC), которая использует метки (FDP_IFF.1 «Простые атрибуты безопасности») как основу для механизма управления доступом.

Политика безопасности ОО может содержать несколько политик функций безопасности (ПФБ), каждая из которых будет идентифицирована компонентами двух ориентированных на политики семейств «Политика управления безопасностью» FDP_ACC и «Политика управления информационными потоками» FDP_IFC. Эти политики будут, как правило, учитывать аспекты конфиденциальности, целостности и доступности так, как это потребуется для удовлетворения требований к ОО. Следует обеспечить, чтобы на каждый объект обязательно распространялась, по меньшей мере, одна ПФБ и при реализации различных ПФБ не возникали конфликты.

В процессе разработки ПЗ/ЗБ с использованием компонентов класса FDP «Защита данных пользователя» при их просмотре и выборе необходимо руководствоваться нижеследующими положениями.

Требования класса FDP «Защита данных пользователя» определены в терминах функций безопасности (ФБ), которые реализуют ПФБ. Поскольку ОО может одновременно следовать нескольким ПФБ, автору ПЗ/ЗБ необходимо дать каждой из ПФБ название, на которое можно ссылаться в других семействах. Это название будет затем использоваться в каждом компоненте, выбранном для определения части требований для соответствующей функции, что позволит автору ПЗ/ЗБ легко указать область действия, например охватываемые объекты и операции, уполномоченные пользователи и т.д.

Как правило, каждое применение компонента возможно только для одной ПФБ. Поэтому, если ПФБ специфицирована в компоненте, то она будет применена во всех элементах этого компонента. Эти компоненты могут применяться в ПЗ/ЗБ несколько раз, если желательно учесть несколько политик.

Ключом к выбору компонентов этого семейства является наличие полностью определенной политики безопасности ОО, обеспечивающей правильный выбор компонентов из семейств «Политика управления доступом» FDP_ACC и «Политика управления информационными потоками» FDP_IFC. В FDP_ACC «Политика управления

доступом» и FDP_IFC «Политика управления информационными потоками» присваивают имя соответственно каждой политике управления доступом или информационными потоками. Кроме того, эти компоненты определяют субъекты, объекты и операции, входящие в область действия соответствующей функции безопасности. Предполагается, что имена этих политик будут использоваться повсеместно в тех функциональных компонентах, которые имеют операцию, запрашивающую назначение или выбор «ПФБ управления доступом» и/или «ПФБ управления информационными потоками». Правила, которые определяют функциональные возможности именованных ПФБ управления доступом или информационными потоками, будут установлены в семействах FDP_ACF «Функции управления доступом» и FDP_IFF «Функции управления информационными потоками» соответственно.

Ниже приведена рекомендуемая последовательность применения этого класса при построении ПЗ/ЗБ, для чего необходимо идентифицировать:

a) осуществляемые политики, применив семейства FDP_ACC «Политика управления доступом» и FDP_IFC «Политика управления информационными потоками». Эти семейства определяют область действия каждой политики, уровень детализации управления и могут идентифицировать некоторые правила следования политике;

b) требуемые компоненты, после чего выполнить все применяемые операции в компонентах, относящихся к политикам. Операции назначения могут выполняться как в обобщенном виде (например «все файлы»), так и конкретно («файлы «A», «B» и т.д.) в зависимости от уровня детализации;

c) все потенциально применяемые компоненты, относящиеся к функциям, из семейств FDP_ACF «Функции управления доступом» и FDP_IFF «Функции управления информационными потоками», связанные с именованными политиками из семейств FDP_ACC «Политика управления доступом» и FDP_IFC «Политика управления информационными потоками». Далее выполнить операции, чтобы получить компоненты, определяющие правила этих политик. Это следует сделать так, чтобы компоненты отражали требования выбранной функции, которые уже можно себе представить или которые только подлежат разработке;

d) тех, кому будет предоставлена возможность управления атрибутами функций безопасности и их изменения, например, только администратору безопасности, только владельцу объекта и т.д., после чего выбрать соответствующие компоненты из класса FMT «Управление безопасностью» и выполнить в них операции. При этом могут быть полезны уточнения для идентификации недостающих свойств, например, некоторые или все изменения необходимо выполнять только с использованием доверенного маршрута;

e) все подходящие компоненты класса FMT «Управление безопасностью», необходимые для спецификации начальных значений новых объектов и субъектов;

f) все компоненты семейства FDP_ROL «Откат», применяемые для отката к предшествующему состоянию;

g) все требования из семейства FDP_RIP «Защита остаточной информации», применяемые для защиты остаточной информации;

h) все компоненты из семейств FDP_ITC «Импорт данных из-за пределов действия ФБО» и FDP_ETC «Экспорт данных за пределы действия ФБО», используемые при импорте или экспорте данных, указав, как следует обращаться при этом с атрибутами безопасности;

i) все используемые компоненты, относящиеся к внутренним передачам ОО, из семейства FDP_ITT «Передача в пределах ОО»;

j) требования защиты целостности хранимой информации из семейства FDP_SDI «Целостность хранимых данных»;

k) все применяемые компоненты, относящиеся к передаче данных между ФБО, из семейств FDP_UCT «Защита конфиденциальности данных пользователя при передаче между ФБО» или FDP_UIT «Защита целостности данных пользователя при передаче между ФБО».

Декомпозиция класса FDP на составляющие его компоненты показана на рисунке F.1.

F.1 Политика управления доступом (FDP_ACC)

F.1.1 Замечания для пользователя

В основу семейства FDP_ACC положена концепция произвольного управления взаимодействием субъектов и объектов. Область и цель управления определяются атрибутами получателя прав доступа (субъекта), атрибутами хранилища данных, к которому предоставляется доступ (объекта), действиями (операциями) и ассоциированными правилами управления доступом.

Компоненты этого семейства дают возможность идентификации (по имени) ПФБ управления доступом, в основе которых лежат традиционные механизмы дискреционного управления доступом (DAC). В семействе определяются субъекты, объекты и операции, которые входят в область действия идентифицированных политик управления доступом. Правила, определяющие функциональные возможности ПФБ управления доступом, будут установлены другими семействами, такими как FDP_ACF «Функции управления доступом» и FDP_RIP «Защита остаточной информации». Предполагается, что имена ПФБ, идентифицированные в семействе FDP_ACC «Политика управления доступом», будут использоваться повсеместно в тех функциональных компонентах, которые имеют операцию, запрашивающую назначение или выбор «ПФБ управления доступом».

В область действия ПФБ управления доступом входит множество триад «субъект, объект, операции». Следовательно, на субъект могут распространяться несколько ПФБ, но только в различных сочетаниях с объектами и операциями. То же относится к объектам и операциям.

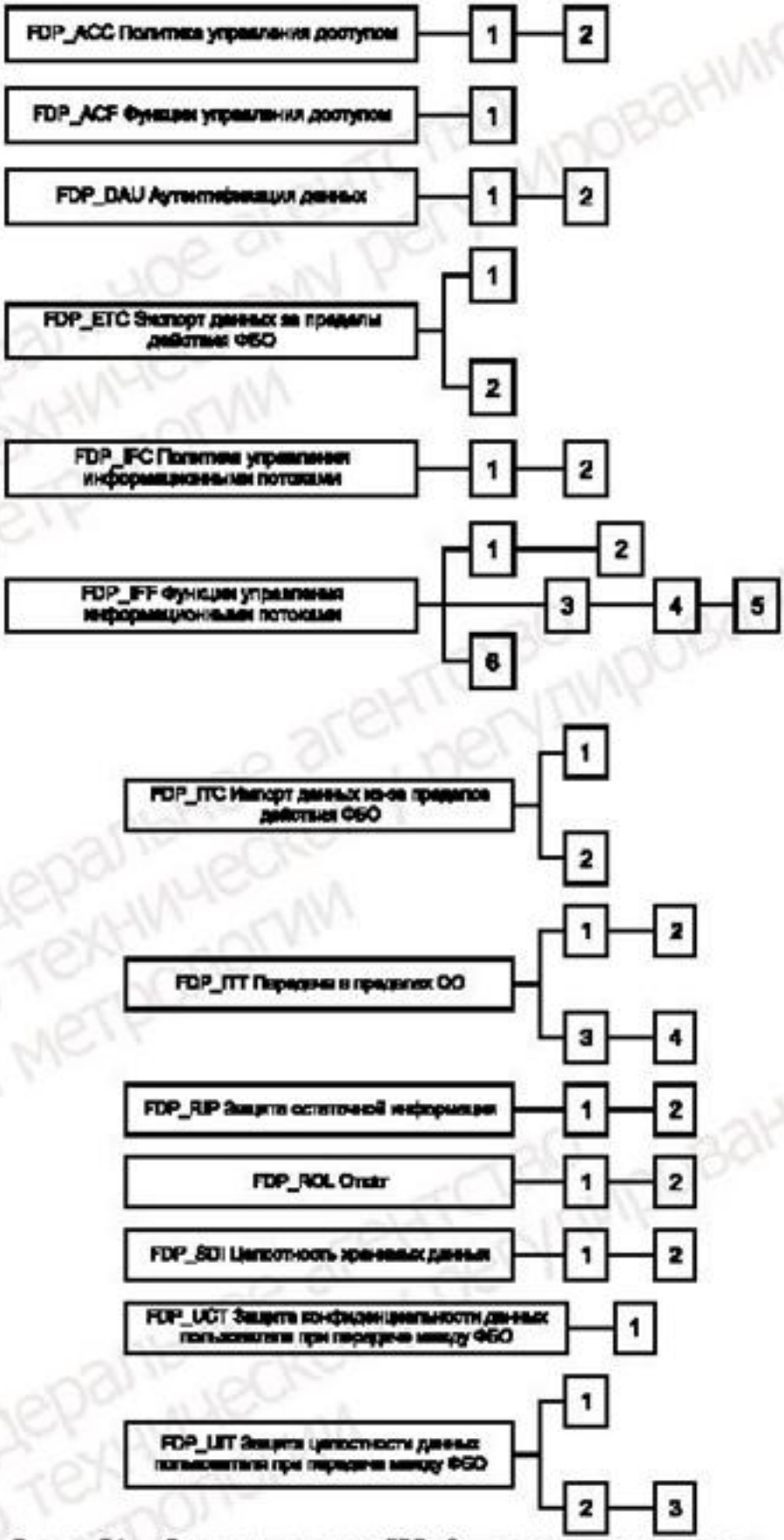

Рисунок F.1 — Декомпозиция класса FDP «Защита данных пользователя»

Важнейшим аспектом функции управления доступом, осуществляющей ПФБ управления доступом, является предоставление пользователям возможности модифицировать атрибуты управления доступом. Семейство FDP_ACC «Политика управления доступом» для этого не предназначено. Часть относящихся к этой проблеме требований не определена, но их можно ввести как уточнение; часть содержится в других семействах и классах, например, в классе FMT «Управление безопасностью».

В семействе FDP_ACC «Политика управления доступом» нет требований аудита, поскольку оно специфицирует только требования ПФБ управления доступом. Требования аудита присутствуют в семействах, специфицирующих функции для удовлетворения ПФБ управления доступом, идентифицированных в этом семействе.

Это семейство предоставляет автору ПЗ/ЗБ возможность спецификации нескольких политик, например, жесткую ПФБ управления доступом в одной области действия и гибкую в другой. Для спецификации нескольких политик управления доступом компоненты этого семейства могут использоваться в ПЗ/ЗБ несколько раз для различных подмножеств операций и объектов. Это применимо к ОО, в которых предусмотрено несколько политик для различных подмножеств операций и объектов. Другими словами, автору ПЗ/ЗБ следует специфицировать, применяя компонент ACC, необходимую информацию о каждой из ПФБ, которые будут осуществляться ФБО. Например, ПЗ/ЗБ для ОО, включающего в себя три ПФБ, каждая из которых действует для своей части объектов, субъектов и операций в пределах ОО, будет содержать по одному компоненту FDP_ACC.1 «Ограниченное управление доступом» для каждой из трех ПФБ.

F.1.2 FDP_ACC.1 Ограниченное управление доступом

F.1.2.1 Замечания по применению для пользователя

Термины «объект» и «субъект» являются обобщенными понятиями для ОО. Для каждой реализуемой политики необходимо четко идентифицировать сущности этой политики. В ПЗ объекты и операции можно представить с использованием типов, например, именованные объекты, хранилища данных, доступ для чтения и т. п. Для конкретной системы необходимо уточнение обобщенных терминов «объект» и «субъект», например файлы, регистры, порты, присоединенные процедуры, запросы на открытие и т. п.

Компонент FDP_ACC.1 определяет, что политика распространяется на некоторое полностью определенное множество операций на каком-либо подмножестве объектов. Данный компонент не накладывает никаких ограничений на операции, не входящие в это множество, в том числе операции на объектах, на которых иные операции управляются.

F.1.2.2 Операции

F.1.2.2.1 Назначение

В FDP_ACC.1.1 автору ПЗ/ЗБ следует специфицировать уникально именованную ПФБ управления доступом, осуществляемую ФБО.

В FDP_ACC.1.1 автору ПЗ/ЗБ следует специфицировать список субъектов, объектов и операций субъектов на объектах, на которые распространяется данная ПФБ.

F.1.3 FDP_ACC.2 Полное управление доступом

F.1.3.1 Замечания по применению для пользователя

Компонент FDP_ACC.2 содержит требование, чтобы ПФБ управления доступом распространялась на все возможные операции над объектами, включенными в ПФБ.

Автору ПЗ/ЗБ необходимо продемонстрировать, что на любую комбинацию объектов и субъектов распространяется какая-либо ПФБ управления доступом.

F.1.3.2 Операции

F.1.3.2.1 Назначение

В FDP_ACC.2.1 автору ПЗ/ЗБ следует специфицировать уникально именованную ПФБ управления доступом, осуществляемую ФБО.

В FDP_ACC.2.1 автору ПЗ/ЗБ следует специфицировать список субъектов и объектов, на которые распространяется данная ПФБ. ПФБ будет распространяться на все операции между этими субъектами и объектами.

F.2 Функции управления доступом (FDP_ACF)

F.2.1 Замечания для пользователя

Семейство FDP_ACF описывает правила для конкретных функций, которые могут реализовать политики управления доступом, именованные в FDP_ACC «Политика управления доступом». В FDP_ACC также определяется область действия этих политик.

Данное семейство позволяет автору ПЗ/ЗБ описать правила управления доступом. В результате правила доступа к объектам системы не будут изменяться. Примером такого объекта является рубрика «Новости дня», которую читать могут все, а изменять — только уполномоченный администратор. Данное семейство также позволяет автору ПЗ/ЗБ устанавливать исключения из общих правил управления доступом. Такие исключения будут явно разрешать или запрещать авторизацию доступа к объекту.

Спецификация других возможных типов функций управления, например двойное управление, правила последовательности операций или управление исключениями, явно не предусмотрена. Однако эти механизмы, как и механизм дискреционного управления доступом, можно представить с помощью имеющихся компонентов при внимательном отношении к формулированию правил управления доступом.

В этом семействе можно определить ряд ФБ управления доступом, имеющих в основе:

- списки контроля доступа (матрица доступа);

- спецификации управления доступом на основе времени;
- спецификации управления доступом на основе источника;
- атрибуты управления доступом, управляемые их владельцем.

F.2.2 FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

F.2.2.1 Замечания по применению для пользователя

Компонент FDP_ACF.1 обеспечивает требования к механизму, который поддерживает управление доступом, основанное на атрибутах безопасности, ассоциированных с субъектами и объектами. Каждый объект и субъект имеет совокупность ассоциированных с ним атрибутов, таких как расположение, время создания, права доступа (например списки контроля доступа). Данный компонент позволяет автору ПЗ/ЗБ специфицировать атрибуты, которые будут использоваться для посредничества при управлении доступом, а также правила управления доступом на основе этих атрибутов.

Примеры атрибутов, которые может назначать автор ПЗ/ЗБ, представлены ниже.

Атрибут «идентификатор» может быть ассоциирован с пользователями, субъектами или объектами для использования при посредничестве. Примерами этого атрибута могут быть имя загрузочного модуля программы, используемой при создании субъекта, или атрибут безопасности, назначенный загрузочному модулю программы.

Атрибут «время» может использоваться для определения того, что доступ будет предоставляться только в указанные время суток, дни недели или календарный год.

Атрибут «местоположение» мог бы определять место как формирования запроса на операцию, так и выполнения операции, либо то и другое. Применение таких атрибутов может основываться на внутренних таблицах для сопоставления логических интерфейсов ФБО с местами расположения терминалов, процессоров и т. д.

Атрибут «группирование» позволяет, в целях управления доступом, ассоциировать единую группу пользователей с некоторой операцией. При необходимости, для спецификации максимального числа групп пользователей, пользователей в группе и групп, в которые может одновременно входить пользователь, следует использовать операцию уточнения.

Компонент FDP_ACF.1 содержит также требования, дающие функциям управления доступом возможность явно предоставлять или запрещать доступ к объектам на основании атрибутов безопасности. Его можно использовать для предоставления полномочий, прав доступа или разрешения доступа в пределах ОО. Такие полномочия, права или разрешения можно применять к пользователям, субъектам (представляющим пользователей или приложения) и объектам.

F.2.2.2 Операции

F.2.2.2.1 Назначение

В FDP_ACF.1.1 автору ПЗ/ЗБ следует специфицировать имя ПФБ управления доступом, осуществляемой ФБО. Имя и область действия ПФБ управления доступом определяются в компонентах семейства FDP_ACC.

В FDP_ACF.1.1 автору ПЗ/ЗБ следует специфицировать атрибуты безопасности и/или именованные группы атрибутов безопасности, которые функция будет использовать при спецификации правил, для каждого управляемого субъекта или объекта. Такими атрибутами безопасности могут быть, например идентификатор пользователя, идентификатор субъекта, роль, время суток, местоположение, списки контроля доступа, а также любые другие атрибуты, специфицированные автором ПЗ/ЗБ. Для удобства ссылок на атрибуты безопасности неоднократного применения можно ввести именованные группы атрибутов безопасности. Именованные группы могут оказаться полезными при ассоциации «ролей», определенных в семействе FMT_SMR «Роли управления безопасностью», и соответствующих им атрибутов с субъектами. Другими словами, каждую роль можно связать с именованной группой атрибутов.

В FDP_ACF.1.2 автору ПЗ/ЗБ следует специфицировать для данной ПФБ правила управления доступом контролируемых субъектов к контролируемым объектам и контролируемым операциям на контролируемых объектах. Эти правила определяют, когда доступ предоставляется, а когда в нем отказано. В них могут быть специфицированы функции управления доступом общего характера (использующие, например обычные биты разрешения) или структурированные функции управления доступом (использующие, например списки контроля доступа).

В FDP_ACF.1.3 автору ПЗ/ЗБ следует специфицировать основанные на атрибутах безопасности правила, которые будут использоваться для явного разрешения доступа субъектов к объектам и дополняют правила, установленные в FDP_ACF.1.1. Они вынесены в отдельный элемент FDP_ACF.1.3, поскольку описывают исключения из правил, установленных в FDP_ACF.1.1. Например, правила явного разрешения доступа могут быть основаны на векторе полномочий, ассоциированном с субъектом и всегда обеспечивающим ему доступ к объектам, на которые распространяется специфицируемая ПФБ управления доступом. Если подобная возможность нежелательна, то автору ПЗ/ЗБ следует указать «Нет» в данной операции.

В FDP_ACF.1.4 автору ПЗ/ЗБ следует специфицировать основанные на атрибутах безопасности правила, которые будут использоваться для явного отказа в доступе субъектов к объектам и дополняют правила, установленные в FDP_ACF.1.1. Они вынесены в отдельный элемент FDP_ACF.1.4, поскольку описывают исключения из правил, установленных в FDP_ACF.1.1. Например, правила явного отказа в доступе могут быть основаны на векторе полномочий, ассоциированном с субъектом и явно отказывающем ему в доступе к объектам, на которые распространяется специфицируемая ПФБ управления доступом. Если подобная возможность нежелательна, то автору ПЗ/ЗБ следует указать «Нет» в данной операции.

F.3 Аутентификация данных (FDP_DAU)

F.3.1 Замечания для пользователя

Семейство FDP_DAU описывает специальные функции, используемые для аутентификации «статических» данных.

Компоненты этого семейства используют при наличии требования аутентификации «статических» данных, то есть, если данные обозначаются, но не передаются (при передаче данных для обеспечения неотказуемости отправления информации используют семейство FCO_NRO «Неотказуемость отправления»).

F.3.2 FDP_DAU.1 Базовая аутентификация данных

F.3.2.1 Замечания по применению для пользователя

Компонент FDP_DAU.1 может быть реализован с помощью односторонних хэш-функций (криптографической контрольной суммы, отображения отпечатков пальцев, хэш-образа сообщения) для генерации хэш-значения определяемого документа, которое может использоваться при верификации правильности или подлинности содержащейся в нем информации.

F.3.2.2 Операции

F.3.2.2.1 Назначение

В FDP_DAU.1.1 автору ПЗ/ЗБ следует специфицировать список объектов или типов информации, для которых ФБО должны быть в состоянии генерировать свидетельство аутентификации данных.

В FDP_DAU.1.2 автору ПЗ/ЗБ следует специфицировать список субъектов, которые будут в состоянии верифицировать свидетельства аутентификации данных для объектов, указанных в предыдущем элементе. Список может просто перечислить субъектов, если все они известны, или описание субъектов в списке может носить более общий характер и ссылаться на «тип» субъекта, например, на идентифицированную роль.

F.3.3 FDP_DAU.2 Аутентификация данных с идентификацией гаранта

F.3.3.1 Замечания по применению для пользователя

Компонент FDP_DAU.2 дополнительно содержит требование наличия возможности верифицировать идентификатор пользователя, предоставляющего гарантию аутентификации (например, доверенного третьего лица).

F.3.3.2 Операции

F.3.3.2.1 Назначение

В FDP_DAU.2.1 автору ПЗ/ЗБ следует специфицировать список объектов или типов информации, для которых ФБО должны быть в состоянии генерировать свидетельство аутентификации данных.

В FDP_DAU.2.2 автору ПЗ/ЗБ следует специфицировать список субъектов, которые будут в состоянии верифицировать свидетельства аутентификации данных для объектов, указанных в предыдущем элементе, а также идентификатор пользователя, который создал свидетельство аутентификации данных.

F.4 Экспорт данных за пределы действия ФБО (FDP_ETC)

F.4.1 Замечания для пользователя

Семейство FDP_ETC определяет функции для экспорта данных пользователя из ОО так, что их атрибуты безопасности могут полностью сохраняться или игнорироваться при экспорте этих данных. Согласованность этих атрибутов безопасности обеспечивается семейством FPT_TDC «Согласованность данных ФБО между ФБО».

В семействе FDP_ETC «Экспорт данных за пределы действия ФБО» также рассматриваются ограничения на экспорт и ассоциация атрибутов безопасности с экспортируемыми данными пользователя.

FDP_ETC и соответствующее семейство для импорта данных FDP_ITC «Импорт данных из-за пределов действия ФБО» определяют, как ОО поступает с данными пользователей, передаваемыми из ОДФ и поступающими в нее. Фактически, семейство FDP_ETC обеспечивает экспорт данных пользователей и связанных с ними атрибутов безопасности.

В данном семействе могут рассматриваться следующие действия:

a) экспорт данных пользователей без каких-либо атрибутов безопасности;

b) экспорт данных пользователей с атрибутами безопасности, ассоциированными с этими данными, причем атрибуты безопасности однозначно представляют экспортируемые данные пользователя.

Если применяются несколько ПФБ управления доступом и/или информационными потоками, то может потребоваться повторить этот компонент отдельно для каждой политики (то есть применить к нему операцию итерации).

F.4.2 FDP_ETC.1 Экспорт данных пользователя без атрибутов безопасности

F.4.2.1 Замечания по применению для пользователя

Компонент FDP_ETC.1 используется для спецификации экспорта информации без экспорта атрибутов безопасности.

F.4.2.2 Операции

F.4.2.2.1 Назначение

В FDP_ETC.1.1 автору ПЗ/ЗБ следует специфицировать, какие ПФБ управления доступом и/или информационными потоками будут осуществляться при экспорте данных пользователя. Данные пользователя, которые экспортируются этой функцией, ограничиваются назначением этих ПФБ.

F.4.3 FDP_ETC.2 Экспорт данных пользователя с атрибутами безопасности

F.4.3.1 Замечания по применению для пользователя

Данные пользователя экспортируются вместе со своими атрибутами безопасности. Эти атрибуты безопасности однозначно ассоциированы с данными пользователя. Ассоциация может устанавливаться различными

способами. К способам установления ассоциации относятся совместное физическое размещение данных пользователя и атрибутов безопасности (например, на одной дискете) или использование криптографических методов, например, цифровых подписей, для ассоциации этих атрибутов и данных пользователя. Для обеспечения получения правильных значений атрибутов другим доверенным продуктом ИТ можно использовать семейство FTP_ITC «Доверенный канал передачи между ФБО», в то время как семейство FPT_TDC «Согласованность данных ФБО между ФБО» может применяться для достижения уверенности в правильной интерпретации этих атрибутов. В свою очередь, семейство FTP_TRP «Доверенный маршрут» может применяться для достижения уверенности в инициации экспорта надлежащим пользователем.

F.4.3.2 Операции

F.4.3.2.1 Назначение

В FDP_ETC.2.1 автору ПЗ/ЗБ следует специфицировать, какие ПФБ управления доступом и/или информационными потоками будут осуществляться при экспорте данных пользователя. Данные пользователя, которые экспортируются этой функцией, ограничиваются назначением этих ПФБ.

В FDP_ETC.2.4 автору ПЗ/ЗБ следует специфицировать все дополнительные правила управления экспортом или указать «Нет» при их отсутствии. Эти правила будут реализованы ФБО в дополнение к ПФБ управления доступом и/или информационными потоками, выбранным в FDP_ETC.2.1.

F.5 Политика управления информационными потоками (FDP_IFC)

F.5.1 Замечания для пользователя

В семействе FDP_IFC идентифицируются ПФБ управления информационными потоками и специфицируются области действия каждой такой политики.

Примерами политик безопасности, которые могут быть применены, являются:

- модель безопасности Белла и Ла Падулы [1];
- модель целостности Биба [2];
- невмешательство [5], [6].

Компоненты этого семейства дают возможность идентификации ПФБ управления информационными потоками, осуществляемых традиционными механизмами мандатного управления доступом при их наличии в ОО. Однако их возможности шире традиционных механизмов мандатного управления доступом. Они могут использоваться для определения политик невмешательства и политик, основанных на переходах между состояниями. В этом семействе для каждой из ПФБ управления информационными потоками ОО определяются субъекты, информация и операции перемещения информации к субъектам и от субъектов. Правила, определяющие функциональные возможности ПФБ управления информационными потоками, будут установлены другими семействами, такими как FDP_IFF «Функции управления информационными потоками» и FDP_RIP «Защита остаточной информации». ПФБ управления информационными потоками, определенные в семействе FDP_IFC, в дальнейшем будут использоваться повсеместно в тех функциональных компонентах, которые включают в себя операцию, запрашивающую назначение или выбор «ПФБ управления информационными потоками».

Компоненты этого семейства достаточно гибки. Они позволяют специфицировать домен управления потоками, не требуя, чтобы механизм управления был основан на метках. Разные элементы компонентов управления информационными потоками также допускают различную степень исключений из осуществляемой политики.

Каждая ПФБ распространяется на некоторое множество триад: «субъект, информация, операции перемещения информации к субъектам и от субъектов». Некоторые политики управления информационными потоками могут иметь очень подробную детализацию и описывать субъекты непосредственно в терминах процессов операционной системы. Другие политики могут определяться с меньшими подробностями и описывать субъекты в терминах пользователей или каналов ввода/вывода. Если политика управления информационными потоками задана недостаточно подробно, то четкое определение требуемых функций безопасности ИТ может оказаться невыполнимым. В этом случае целесообразнее описывать политики управления информационными потоками как цели безопасности. Тогда требуемые функции безопасности ИТ можно специфицировать, исходя из этих целей.

Во втором компоненте (FDP_IFC.2 «Полное управление информационными потоками») каждая ПФБ управления информационными потоками будет охватывать все возможные операции перемещения информации к субъектам и от субъектов под управлением этой ПФБ. Более того, требуется, чтобы все информационные потоки были охвачены какой-либо ПФБ, поэтому для каждого действия, вызвавшего перемещение информации, будет существовать совокупность правил, определяющих, является ли данное действие допустимым. Если данный информационный поток подчинен нескольким ПФБ, то необходимо его разрешение всеми этими политиками до его начала.

Политика управления информационными потоками охватывает полностью определенное множество операций. Для некоторых информационных потоков этот охват может быть «полным», а для других потоков он может относиться только к некоторым из предусмотренных для них операций.

Политика управления доступом обеспечивает доступ к объектам, содержащим информацию. Политика управления информационными потоками обеспечивает доступ к информации, независимо от места ее хранения. Атрибуты информации, которые могут быть (или не быть, в случае многоуровневых баз данных) ассоциированы с атрибутами места хранения, остаются с информацией при ее перемещении. Получатель доступа к информации не имеет возможности без явного разрешения изменять ее атрибуты.

Возможны различные уровни представления информационных потоков и операций. В ЗБ информационные потоки и операции можно специфицировать на уровне конкретной системы, например, в терминах пакетов TCP/IP, проходящих через межсетевой экран по известным IP-адресам. В ПЗ информационные потоки и операции можно представить с использованием следующих типов: электронная почта, хранилища данных, доступ для чтения и т. д.

Компоненты семейства FDP_IFC могут неоднократно применяться в ПЗ/ЗБ к различным подмножествам операций и объектов (то есть к ним может быть применена операция итерации). Это позволит адаптировать данное семейство к объектам оценки, включающим в себя несколько политик, каждая из которых действует на собственное подмножество субъектов, информации и операций.

F.5.2 FDP_IFC.1 Ограниченное управление информационными потоками

F.5.2.1 Замечания по применению для пользователя

Компонент FDP_IFC.1 содержит требование, чтобы политика управления информационным потоком применялась к подмножеству возможных операций в ОО.

F.5.2.2 Операции

F.5.2.2.1 Назначение

В FDP_IFC.1.1 автору ПЗ/ЗБ следует специфицировать уникально именованную ПФБ управления информационными потоками, осуществляемую ФБО.

В FDP_IFC.1.1 автору ПЗ/ЗБ следует специфицировать список субъектов, информации и операций, вызывающих перемещение управляемой информации к управляемым субъектам и от них, на которые распространяется данная ПФБ. Как указано выше, этот список субъектов может быть задан с различной степенью детализации, определяемой потребностями автора ПЗ/ЗБ. Автор может, например, специфицировать пользователей, устройства или процессы. Информация может относиться к таким данным, как электронная почта, сетевые протоколы, или к более конкретным объектам, аналогичным специфицированным в политике управления доступом. Если информация содержится в объекте, который подчинен политике управления доступом, то политики управления доступом и информационными потоками необходимо применять совместно, прежде чем начнется перемещение специфицированной информации в объект или из него.

F.5.3 FDP_IFC.2 Полное управление информационными потоками

F.5.3.1 Замечания по применению для пользователя

Компонент FDP_IFC.2 содержит требование, чтобы ПФБ управления информационными потоками распространялась на все возможные операции, вызывающие информационные потоки к субъектам и от субъектов, включенных в ПФБ.

Автору ПЗ/ЗБ необходимо продемонстрировать, что на любую комбинацию информационных потоков и субъектов распространяется какая-либо ПФБ управления информационным потоком.

F.5.3.2 Операции

F.5.3.2.1 Назначение

В FDP_IFC.2.1 автору ПЗ/ЗБ следует специфицировать уникально именованную ПФБ управления информационными потоками, осуществляемую ФБО.

В FDP_IFC.2.1 автору ПЗ/ЗБ следует специфицировать список субъектов и информации, на которые будет распространяться данная ПФБ. ПФБ будет распространяться на все операции, вызывающие перемещение этой информации к этим субъектам и от них. Как указано выше, этот список субъектов может быть задан с различной степенью детализации, определяемой потребностями автора ПЗ/ЗБ. Автор может, например, специфицировать пользователей, устройства или процессы. Информация может относиться к таким данным, как электронная почта, сетевые протоколы или к более конкретным объектам, аналогичным специфицированным в политике управления доступом. Если информация содержится в объекте, который подчинен политике управления доступом, то политики управления доступом и информационными потоками необходимо применять совместно, прежде чем начнется перемещение специфицированной информации в объект или из него.

F.6 Функции управления информационными потоками (FDP_IFF)

F.6.1 Замечания для пользователя

Семейство FDP_IFF описывает правила для конкретных функций, которые могут реализовать ПФБ управления информационными потоками, именованные в FDP_IFC «Политика управления информационными потоками», где также определена область действия соответствующей политики. Семейство содержит два типа требований: один связан с обычными информационными потоками, второй — с неразрешенными информационными потоками (скрытыми каналами), запрещенными одной или несколькими ПФБ. Это разделение возникает, потому что проблема неразрешенных информационных потоков в некотором смысле противоречит остальным аспектам ПФБ управления информационными потоками. Неразрешенные информационные потоки возникают в нарушение политики, поэтому они не являются результатом применения политики.

Для реализации надежной защиты от раскрытия или модификации в условиях недоверенного программного обеспечения требуется управлять информационными потоками. Одного управления доступом недостаточно, так как при нем контролируется только доступ к хранилищам, что позволяет информации, содержащейся в них, бесконтрольно распространяться в системе.

В этом семействе употребляется выражение «типы неразрешенных информационных потоков». Это выражение может применяться при ссылке на известные типы классификации потоков, такие как «каналы памяти»

или «каналы синхронизации (временные каналы)», или на иную классификацию, отражающую потребности автора ПЗ/ЗБ.

Гибкость этих компонентов позволяет специфицировать в FDP_IFF.1 «Простые атрибуты безопасности» и FDP_IFF.2 «Иерархические атрибуты безопасности» политику полномочий, дающую возможность контролируемого обхода ПФБ в целом или частично. Если необходимо заранее предопределить обход ПФБ, автору ПЗ/ЗБ следует предусмотреть применение политики полномочий.

F.6.2 FDP_IFF.1 Простые атрибуты безопасности

F.6.2.1 Замечания по применению для пользователя

Компонент FDP_IFF.1 содержит требования наличия атрибутов безопасности у информации и субъектов, являющихся отправителями или получателями этой информации. Следует также учитывать атрибуты безопасности мест хранения информации, если требуется их участие в управлении информационными потоками, или если на эти атрибуты распространяется политика управления доступом. Этот компонент специфицирует ключевые осуществляемые правила и описывает, как вводятся атрибуты безопасности. Например, компонент следует применять, если хотя бы одна из ПФБ управления информационными потоками основана на метках, как это определяет модель политики безопасности Белла и Ла Падулы [B&L], но эти атрибуты безопасности не образуют иерархию.

Этот компонент не определяет детали присвоения значений атрибутам безопасности (то есть пользователем или процессом). Гибкость политики обеспечивается операциями назначения, которые позволяют, при необходимости, специфицировать дополнительные требования к политике и функциям.

Компонент FDP_IFF.1 также содержит требования к функциям управления информационными потоками с тем, чтобы они могли явно разрешать или запрещать информационный поток на основе атрибутов безопасности. Он может применяться для реализации политики полномочий, предусматривающей исключения из основной политики, определенной в этом компоненте.

F.6.2.2 Операции

F.6.2.2.1 Назначение

В FDP_IFF.1.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления информационными потоками, осуществляемые ФБО. Имя и область действия ПФБ управления информационными потоками определяются в компонентах семейства FDP_IFC.

В FDP_IFF.1.1 автору ПЗ/ЗБ для каждого типа управляемых субъектов и информации следует специфицировать атрибуты безопасности, которые необходимы для спецификации правил ПФБ. Такими атрибутами безопасности могут быть, например идентификатор субъекта, метка чувствительности субъекта, метка допуска субъекта к информации, метка чувствительности информации и т. д. Типы атрибутов безопасности должны быть достаточными для поддержки потребностей среды.

В FDP_IFF.1.2 автору ПЗ/ЗБ следует специфицировать для каждой операции реализуемые ФБО и основанные на атрибутах безопасности отношения, которые необходимо поддерживать между атрибутами безопасности субъектов и информации.

В FDP_IFF.1.3 автору ПЗ/ЗБ следует специфицировать все дополнительные правила ПФБ управления информационными потоками, которые от ФБО требуется реализовать. Если дополнительные правила не используются, то автору ПЗ/ЗБ следует указать «Нет» при выполнении рассматриваемой операции.

В FDP_IFF.1.4 автору ПЗ/ЗБ следует специфицировать все дополнительные возможности ПФБ, которые от ФБО требуется предоставить. Если дополнительные возможности не предоставляются, то автору ПЗ/ЗБ следует указать «Нет» при выполнении рассматриваемой операции.

В FDP_IFF.1.5 автору ПЗ/ЗБ следует специфицировать основанные на атрибутах безопасности правила, явно разрешающие информационные потоки и дополняющие правила, определенные в предыдущих элементах. Они вынесены в отдельный элемент FDP_IFF.1.5, поскольку описывают исключения из правил в предыдущих элементах. Например, правила явного разрешения информационного потока могут быть основаны на векторе полномочий, ассоциированном с субъектом и всегда обеспечивающим ему возможность инициировать перемещение информации, на которую распространяется специфицированная ПФБ. Если подобная возможность нежелательна, то автору ПЗ/ЗБ следует указать «Нет» в данной операции.

В FDP_IFF.1.6 автору ПЗ/ЗБ следует специфицировать основанные на атрибутах безопасности правила, явно запрещающие информационные потоки и дополняющие правила, определенные в предыдущих элементах. Они вынесены в отдельный элемент FDP_IFF.1.6, поскольку описывают исключения из правил в предыдущих элементах. Например, правила явного запрещения информационного потока могут быть основаны на векторе полномочий, ассоциированном с субъектом и всегда отказывающим ему в возможности инициировать перемещение информации, на которую распространяется специфицированная ПФБ. Если подобная возможность нежелательна, то автору ПЗ/ЗБ следует указать «Нет» в данной операции.

F.6.3 FDP_IFF.2 Иерархические атрибуты безопасности

F.6.3.1 Замечания по применению для пользователя

Компонент FDP_IFF.2 содержит требование, чтобы все ПФБ управления информационными потоками в ПБО использовали иерархические атрибуты безопасности, которые образуют некоторую структуру.

Например, этот компонент следует применять, когда хотя бы одна из ПФБ управления информационными потоками основана на метках, как это определяет модель политики безопасности Белла и Ла Падулы [1], и эти атрибуты безопасности образуют иерархию.

Важно отметить, что требования иерархических отношений, идентифицируемые в FDP_IFF.2.7, применимы только к атрибутам безопасности управления информационными потоками для ПФБ управления информационными потоками, идентифицированным в FDP_IFF.2.1. Этот компонент не применим к другим ПФБ, например, к ПФБ управления доступом.

Компонент FDP_IFF.2, как и предыдущий, может использоваться для реализации политики полномочий, содержащей правила, позволяющие явно разрешать или запрещать информационные потоки.

В случае, если необходимо специфицировать несколько ПФБ управления информационными потоками, каждая из которых будет иметь собственные атрибуты безопасности, не связанные с атрибутами других политик, в ПЗ/ЗБ следует специфицировать этот компонент для каждой из ПФБ (то есть выполнить для него операцию итерации). Если этого не сделать, то различные части FDP_IFF.2.7 могут противоречить друг другу, поскольку не будут связаны необходимыми соотношениями.

F.6.3.2 Операции

F.6.3.2.1 Назначение

В FDP_IFF.2.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления информационными потоками, осуществляемые ФБО. Имя и область действия ПФБ управления информационными потоками определяются в компонентах семейства FDP_IFC.

В FDP_IFF.2.1 автору ПЗ/ЗБ следует специфицировать для каждого типа управляемых субъектов и информации атрибуты безопасности, необходимые для спецификации правил ПФБ. Такими атрибутами безопасности могут быть, например идентификатор субъекта, метка чувствительности субъекта, метка допуска субъекта к информации, метка чувствительности информации и т. д. Типы атрибутов безопасности должны быть достаточными для поддержки потребностей среды.

В FDP_IFF.2.2 автору ПЗ/ЗБ следует специфицировать для каждой операции реализуемые ФБО и основанные на атрибутах безопасности отношения, которые необходимо поддерживать между атрибутами безопасности субъектов и информации. Эти отношения следует основывать на упорядоченных связях между атрибутами безопасности.

В FDP_IFF.2.3 автору ПЗ/ЗБ следует специфицировать все дополнительные правила ПФБ управления информационными потоками, которые от ФБО требуется реализовать. Если дополнительные правила не используются, то автору ПЗ/ЗБ следует указать «Нет» при выполнении рассматриваемой операции.

В FDP_IFF.2.4 автору ПЗ/ЗБ следует специфицировать все дополнительные возможности ПФБ, которые от ФБО требуется предоставить. Если дополнительные возможности не предоставляются, то автору ПЗ/ЗБ следует указать «Нет» при выполнении рассматриваемой операции.

В FDP_IFF.2.5 автору ПЗ/ЗБ следует специфицировать основанные на атрибутах безопасности правила, явно разрешающие информационные потоки и дополняющие правила, определенные в предыдущих элементах. Данные правила включены в отдельный элемент FDP_IFF.2.5, поскольку описывают исключения из правил в предыдущих элементах. Например, правила явного разрешения информационного потока могут быть основаны на векторе полномочий, ассоциированном с субъектом и всегда обеспечивающим ему возможность инициировать перемещение информации, на которую распространяется специфицированная ПФБ. Если подобная возможность нежелательна, то автору ПЗ/ЗБ следует указать «Нет» в данной операции.

В FDP_IFF.2.6 автору ПЗ/ЗБ следует специфицировать основанные на атрибутах безопасности правила, явно запрещающие информационные потоки и дополняющие правила, определенные в предыдущих элементах. Они вынесены в отдельный элемент FDP_IFF.2.6, поскольку описывают исключения из правил в предыдущих элементах. Например, правила явного запрещения информационного потока могут быть основаны на векторе полномочий, ассоциированном с субъектом и всегда отказывающим ему в возможности инициировать перемещение информации, на которую распространяется специфицированная ПФБ. Если подобная возможность нежелательна, то автору ПЗ/ЗБ следует указать «Нет» в данной операции.

F.6.4 FDP_IFF.3 Ограничение неразрешенных информационных потоков

F.6.4.1 Замечания по применению для пользователя

Компонент FDP_IFF.3 следует использовать, если одно или несколько правил ПФБ содержат требования по управлению неразрешенными информационными потоками, но ни одна из них не включает в себя требования их устранения.

Для специфицированных неразрешенных информационных потоков следует установить максимально допустимые интенсивности. Кроме того, автор ПЗ/ЗБ имеет возможность определить, необходимо ли подвергать аудиту неразрешенные информационные потоки.

F.6.4.2 Операции

F.6.4.2.1 Назначение

В FDP_IFF.3.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления информационными потоками, осуществляемые ФБО. Имя и область действия ПФБ управления информационными потоками определяются в компонентах семейства FDP_IFC.

В FDP_IFF.3.1 автору ПЗ/ЗБ следует специфицировать типы неразрешенных информационных потоков, максимальная интенсивность которых ограничивается.

В FDP_IFF.3.1 автору ПЗ/ЗБ следует специфицировать максимальную интенсивность, допустимую для каждого из идентифицированных неразрешенных информационных потоков.

F.6.5 FDP_IFF.4 Частичное устранение неразрешенных информационных потоков

F.6.5.1 Замечания по применению для пользователя

Компонент FDP_IFF.4 следует использовать, если все правила ПФБ содержат требования по управлению неразрешенными информационными потоками, и при этом хотя бы одна из них включает в себя требования устранения хотя бы одного неразрешенного информационного потока.

F.6.5.2 Операции

F.6.5.2.1 Назначение

В FDP_IFF.4.1 автору ПЗ/ЗБ следует специфицировать правила ПФБ управления информационными потоками, осуществляемые ФБО. Имя и область действия ПФБ управления информационными потоками определяются в компонентах семейства FDP_IFC «Политика управления информационными потоками».

В FDP_IFF.4.1 автору ПЗ/ЗБ следует специфицировать типы неразрешенных информационных потоков, максимальная интенсивность которых ограничивается.

В FDP_IFF.4.1 автору ПЗ/ЗБ следует специфицировать максимальную интенсивность, допустимую для каждого из идентифицированных неразрешенных информационных потоков.

В FDP_IFF.4.2 автору ПЗ/ЗБ следует специфицировать типы неразрешенных информационных потоков, подлежащих устранению. Список не может быть пустым, поскольку данный компонент содержит требование устранения хотя бы части неразрешенных информационных потоков.

F.6.6 FDP_IFF.5 Отсутствие неразрешенных информационных потоков

F.6.6.1 Замечания по применению для пользователя

Компонент FDP_IFF.5 следует использовать, если правила ПФБ, содержащие требования по управлению неразрешенными информационными потоками, включают в себя требование полного их устранения. Однако автору ПЗ/ЗБ следует внимательно изучить, какое влияние подобное устранение может оказать на нормальное функционирование ОО. Практика показывает возможность опосредованного влияния неразрешенных информационных потоков на работу ОО, поэтому их полное устранение может привести к нежелательным последствиям.

F.6.6.2 Операции

F.6.6.2.1 Назначение

В FDP_IFF.5.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления информационными потоками, для которой неразрешенные информационные потоки требуется устранить. Имя и область действия ПФБ управления информационными потоками определяют в компонентах семейства FDP_IFC «Политика управления информационными потоками».

F.6.7 FDP_IFF.6 Мониторинг неразрешенных информационных потоков

F.6.7.1 Замечания по применению для пользователя

Компонент FDP_IFF.6 следует использовать, если от ФБО требуется проведение мониторинга неразрешенных информационных потоков, интенсивность которых превышает специфицированное пороговое значение. Если такой поток требуется подвергнуть аудиту, то этот компонент может служить источником событий аудита для компонентов семейства FAU_GEN «Генерация данных аудита безопасности».

F.6.7.2 Операции

F.6.7.2.1 Назначение

В FDP_IFF.6.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления информационными потоками, осуществляемые ФБО. Имя и область действия ПФБ управления информационными потоками определяются в компонентах семейства FDP_IFC «Политика управления информационными потоками».

В FDP_IFF.6.1 автору ПЗ/ЗБ следует специфицировать типы неразрешенных информационных потоков, подлежащих мониторингу на превышение максимального значения интенсивности.

В FDP_IFF.6.1 автору ПЗ/ЗБ следует специфицировать максимальную интенсивность, превышение которой неразрешенным информационным потоком будет отслеживаться ФБО.

F.7 Импорт данных из-за пределов действия ФБО (FDP_ITC)

F.7.1 Замечания для пользователя

Семейство FDP_ITC определяет механизмы для импорта данных пользователя в ОО из-за пределов ОДФ так, чтобы атрибуты безопасности данных пользователя при этом сохранялись. Согласованность этих атрибутов безопасности определяется семейством FPT_TDC «Согласованность данных ФБО между ФБО».

В семействе FDP_ITC «Импорт данных из-за пределов действия ФБО» рассматриваются ограничения на импорт, спецификация атрибутов безопасности пользователем и ассоциация атрибутов безопасности и данных пользователя.

Семейство FDP_ITC и соответствующее семейство для экспорта данных FDP_ETC «Экспорт данных за пределы действия ФБО» определяют, как ОО обращается с данными пользователей, поступающими в ОДФ и передаваемыми из нее. Оно связано с назначением и игнорированием атрибутов безопасности данных пользователя.

В семействе могут рассматриваться следующие действия:

а) импорт данных пользователя с бесформатного (по отношению к безопасности) носителя (такого, как гибкий диск, магнитная лента, сканер, видео- или аудиосигнал) без атрибутов безопасности и физическая маркировка носителя для указания на его содержание;

b) импорт данных пользователя, включая атрибуты безопасности, с носителя и верификация соответствия атрибутов безопасности объекта;

c) импорт данных пользователя, включая атрибуты безопасности, с носителя с использованием криптографических методов для защиты ассоциации данных пользователя с атрибутами безопасности.

Семейство FDP_ITC не имеет отношения к определению возможности импорта данных пользователя. Здесь рассматриваются лишь значения атрибутов безопасности для ассоциации с импортируемыми данными пользователя.

Существуют две возможности при импорте данных пользователя: либо они однозначно ассоциируются с достоверными атрибутами безопасности объекта (значения и смысл атрибутов безопасности не меняются), либо никакие достоверные атрибуты безопасности (или вообще какие-либо атрибуты безопасности) не могут быть получены от источника данных. В этом семействе рассмотрены обе возможности.

Если имеются достоверные атрибуты безопасности, их можно ассоциировать с данными пользователя физически (атрибуты безопасности находятся на том же самом носителе) или логически (атрибуты безопасности передаются отдельно, но включают в себя уникальную идентификацию объекта, например, криптографическую контрольную сумму).

Семейство связано с импортом данных пользователя и сопровождением их ассоциации с атрибутами безопасности в соответствии с требованиями ПФБ. С аспектами импорта, которые находятся вне области действия этого семейства (например, с непротиворечивостью, доверенными каналами, целостностью), связаны другие семейства. Более того, в семействе FDP_ITC «Импорт данных из-за пределов действия ФБО» рассматривается только интерфейс для выполнения импорта. Участие в передаче с другой стороны (как источника) рассматривается в семействе FDP_ETC «Экспорт данных за пределы действия ФБО».

Хорошо известны следующие требования импорта:

a) импорт данных пользователя без каких-либо атрибутов безопасности;

b) импорт данных пользователя, включая ассоциированные с ними атрибуты безопасности, причем атрибуты безопасности однозначно представляют импортируемую информацию.

Эти требования импорта могут быть реализованы ФБО при участии или без участия человека в соответствии с ограничениями ИТ и политикой безопасности организации. Например, если данные пользователя получены по «конфиденциальному» каналу, атрибуты безопасности объекта будут установлены как «конфиденциальные».

Если применяются несколько ПФБ управления доступом и/или информационными потоками, то может потребоваться повторить этот компонент отдельно для каждой политики (то есть применить к нему операцию итерации).

F.7.2 FDP_ITC.1 Импорт данных пользователя без атрибутов безопасности

F.7.2.1 Замечания по применению для пользователя

Компонент FDP_ITC.1 используется для спецификации импорта данных пользователя, не имеющих достоверных (или вообще никаких) атрибутов безопасности. Эта функция требует, чтобы атрибуты безопасности данных пользователя инициировались ФБО. Правила импорта может специфицировать и автор ПЗ/ЗБ. В некоторых средах может потребоваться использование для передачи этих атрибутов механизма доверенного маршрута или канала.

F.7.2.2 Операции

F.7.2.2.1 Назначение

В FDP_ITC.1.1 автору ПЗ/ЗБ следует специфицировать, какие ПФБ управления доступом и/или информационными потоками будут осуществляться при импорте данных пользователя в ОДФ. Данные пользователя, которые импортируются этой функцией, ограничиваются назначением этих ПФБ.

В FDP_ITC.1.3 автору ПЗ/ЗБ следует специфицировать все дополнительные правила управления импортом или указать «Нет» при отсутствии таковых. Эти правила будут реализованы ФБО в дополнение к ПФБ управления доступом и/или информационными потоками, выбранным в FDP_ITC.1.1.

F.7.3 FDP_ITC.2 Импорт данных пользователя с атрибутами безопасности

F.7.3.1 Замечания по применению для пользователя

Компонент FDP_ITC.2 используется для спецификации импорта данных пользователя, имеющих достоверные атрибуты безопасности, ассоциированные с ними. Эта функция использует атрибуты безопасности, точно и однозначно связанные с объектами на носителе импортируемых данных. После завершения импорта такие объекты будут иметь те же атрибуты безопасности. При этом требуется привлечение семейства FPT_TDC «Согласованность данных ФБО между ФБО» для обеспечения непротиворечивости данных. Правила импорта может специфицировать и автор ПЗ/ЗБ.

F.7.3.2 Операции

F.7.3.2 1 Назначение

В FDP_ITC.2.1 автору ПЗ/ЗБ следует специфицировать, какие ПФБ управления доступом и/или информационными потоками будут осуществляться при импорте данных пользователя в ОДФ. Данные пользователя, которые импортируются этой функцией, ограничиваются назначением ПФБ.

В FDP_ITC.2.5 автору ПЗ/ЗБ следует специфицировать все дополнительные правила управления импортом или указать «Нет» при их отсутствии. Эти правила будут реализованы ФБО в дополнение к ПФБ управления доступом и/или информационными потоками, выбранным в FDP_ITC.2.1.

F.8 Передача в пределах ОО (FDP_ITT)

F.8.1 Замечания для пользователя

Семейство FDP_ITT содержит требования, связанные с защитой данных пользователя при их передаче между различными частями ОО по внутреннему каналу. Этим данное семейство отличается от семейств FDP_UCT «Защита конфиденциальности данных пользователя при передаче между ФБО» и FDP_UIT «Защита целостности данных пользователя при передаче между ФБО», которые обеспечивают защиту данных пользователя при их передаче между различными ФБО по внешнему каналу, а также от семейств FDP_ETC «Экспорт данных за пределы действия ФБО» и FDP_ITC «Импорт данных из-за пределов действия ФБО», которые связаны с передачей данных за пределы или из-за пределов действия ФБО.

Требования данного семейства позволяют автору ПЗ/ЗБ специфицировать желательный способ защиты данных пользователя во время их передачи в пределах ОО. Это может быть защита от раскрытия, модификации или нарушения доступности.

Принятие решения о степени физического разделения, в условиях которого следует использовать данное семейство, зависит от предполагаемой среды эксплуатации. В неблагоприятной среде могут возникать риски, связанные с передачей между частями ОО, разделенными всего лишь системной шиной. В более благоприятной среде для передачи можно использовать обычные сетевые средства.

Если применяются несколько ПФБ управления доступом и/или информационными потоками, то может потребоваться повторить этот компонент отдельно для каждой именованной политики (то есть применить к нему операцию итерации).

F.8.2 FDP_ITT.1 Базовая защита внутренней передачи

F.8.2.1 Операции

F.8.2.1.1 Назначение

В FDP_ITT.1.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления доступом и/или информационными потоками, распространяющиеся на передаваемую информацию.

F.8.2.1.2 Выбор

В FDP_ITT.1.1 автору ПЗ/ЗБ следует специфицировать типы ошибок передачи, от которых следует защищать, используя ФБО, данные пользователя при их передаче. Варианты: раскрытие, модификация, недоступность.

F.8.3 FDP_ITT.2 Разделение передачи по атрибутам

F.8.3.1 Замечания по применению для пользователя

Компонент FDP_ITT.2 может быть использован, например, для обеспечения различных видов защиты информации в соответствии с различными уровнями критичности.

Одним из способов разделения данных при передаче является использование разделенных логических или физических каналов.

F.8.3.2 Операции

F.8.3.2.1 Назначение

В FDP_ITT.2.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления доступом и/или информационными потоками, распространяющиеся на передаваемую информацию.

F.8.3.2.2 Выбор

В FDP_ITT.2.1 автору ПЗ/ЗБ следует специфицировать типы ошибок передачи, от которых следует защищать, используя ФБО, данные пользователя при их передаче. Варианты: раскрытие, модификация, недоступность.

F.8.3.2.3 Назначение

В FDP_ITT.2.2 автору ПЗ/ЗБ следует специфицировать атрибуты безопасности, по значениям которых ФБО будут определять, когда данные, пересылаемые между физически разделенными частями ОО, требуют разделения. Например, данные пользователя, ассоциированные с идентификатором одного владельца, передаются отдельно от данных, ассоциированных с идентификаторами других владельцев. Тогда для определения необходимости разделения данных при передаче используется значение идентификатора их владельца.

F.8.4 FDP_ITT.3 Мониторинг целостности

F.8.4.1 Замечания по применению для пользователя

Компонент FDP_ITT.3 используется в сочетании с FDP_ITT.1 «Базовая защита внутренней передачи» или FDP_ITT.2 «Разделение передачи по атрибутам». Он обеспечивает, чтобы ФБО проверяли целостность полученных данных пользователя (и их атрибутов). Компоненты FDP_ITT.1 «Базовая защита внутренней передачи» или FDP_ITT.2 «Разделение передачи по атрибутам» предоставят данные способом, защищающим данные от модификации, а FDP_ITT.3 «Мониторинг целостности» позволит обнаружить некоторые из модификаций.

Автор ПЗ/ЗБ должен специфицировать виды ошибок, подлежащих обнаружению. Автору ПЗ/ЗБ следует рассмотреть, помимо прочих нарушений целостности, следующие виды ошибок данных: модификация, подмена, невосстанавливаемое изменение последовательности, повторное использование, неполнота.

Автору ПЗ/ЗБ необходимо специфицировать, какие действия следует предпринять ФБО при обнаружении ошибки, например, игнорировать данные пользователя, запросить данные повторно, сообщить уполномоченному администратору, направить трафик по другим каналам.

F.8.4.2 Операции

F.8.4.2.1 Назначение

В FDP_ITT.3.1 автору ПЗ/ЗБ следует специфицировать, какие ПФБ управления доступом и/или информационными потоками распространяются на передаваемую и проверяемую на ошибки целостности информацию.

В FDP_ITT.3.1 автору ПЗ/ЗБ следует специфицировать типы возможных ошибок целостности, отслеживаемых во время передачи данных пользователя.

В FDP_ITT.3.2 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые ФБО в случае обнаружения ошибки целостности. ФБО, например, могут запросить повторную передачу данных пользователя. ПФБ, специфицированные в FDP_ITT.3.1, будут осуществляться как действия, предпринимаемые ФБО.

F.8.5 FDP_ITT.4 Мониторинг целостности по атрибутам

F.8.5.1 Замечания по применению для пользователя

Компонент FDP_ITT.4 используется в сочетании с FDP_ITT.2 «Разделение передачи по атрибутам». Он обеспечивает, чтобы ФБО проверяли целостность полученных данных пользователя, переданных по разделенным каналам (в соответствии со значениями специфицированных атрибутов безопасности). Компонент позволяет автору ПЗ/ЗБ специфицировать действия, предпринимаемые в случае обнаружения ошибки целостности.

Компонент, например, может использоваться как для обеспечения обнаружения различных ошибок целостности, так и действий над информацией на различных уровнях целостности.

Автор ПЗ/ЗБ должен специфицировать виды ошибок, подлежащих обнаружению. Автору ПЗ/ЗБ следует рассмотреть, помимо прочих нарушений целостности, следующие виды ошибок данных: модификация, подмена, невосстанавливаемое изменение последовательности, повторное использование, неполнота.

Автору ПЗ/ЗБ следует специфицировать атрибуты (и ассоциированные с ними каналы передачи), требующие мониторинга ошибок целостности.

Автору ПЗ/ЗБ необходимо специфицировать, какие действия следует предпринять ФБО при обнаружении ошибки, например, игнорировать данные пользователя, запросить данные повторно, сообщить уполномоченному администратору, направить трафик по другим каналам.

F.8.5.2 Операции

F.8.5.2.1 Назначение

В FDP_ITT.4.1 автору ПЗ/ЗБ следует специфицировать, какие ПФБ управления доступом и/или информационными потоками распространяются на передаваемую и проверяемую на ошибки целостности информацию.

В FDP_ITT.4.1 автору ПЗ/ЗБ следует специфицировать типы возможных ошибок целостности, отслеживаемых во время передачи данных пользователя.

В FDP_ITT.4.1 автору ПЗ/ЗБ следует специфицировать список атрибутов безопасности, требующих разделения каналов передачи. Этот список используется для определения того, какие данные пользователя будут отслеживаться на ошибки целостности на основе атрибутов безопасности данных и каналов передачи данных. Этот элемент прямо зависит от компонента FDP_ITT.2 «Разделение передачи по атрибутам».

В FDP_ITT.4.2 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые ФБО в случае обнаружения ошибки целостности. ФБО, например, могут запросить повторную передачу данных пользователя. ПФБ, специфицированные в FDP_ITT.4.1, будут осуществляться как действия, предпринимаемые ФБО.

F.9 Защита остаточной информации (FDP_RIP)

F.9.1 Замечания для пользователя

Семейство FDP_RIP связано с необходимостью обеспечения последующей недоступности удаленной информации и отсутствия во вновь созданных объектах информации из объектов, ранее использовавшихся в ОО. Это семейство не применяется к объектам, хранимым автономно.

Данное семейство содержит требования защиты информации, которая уже логически удалена или освобождена (недоступна для пользователя, но все еще находится в пределах системы и может быть восстановлена). В частности, это относится к информации, которая содержится в объекте как часть ресурсов ФБО многократного использования, если уничтожение объекта необязательно эквивалентно уничтожению ресурса или какой-либо части ресурса.

Данное семейство применимо также при попеременном использовании различными субъектами ресурсов в системе. Например, в большинстве операционных систем для поддержки системных процессов обычно используются аппаратные регистры (в качестве ресурсов). Поскольку процессы постоянно переходят из активного состояния в состояние ожидания и обратно, эти регистры попеременно используются различными субъектами. Хотя подобные действия «подкачки» можно не считать занятием или освобождением ресурса, к таким событиям и ресурсам может быть применено семейство FDP_RIP «Защита остаточной информации».

Семейство FDP_RIP «Защита остаточной информации» обычно связано с доступом к информации, не являющейся частью объекта, который определен в данный момент, или к которому осуществляется доступ; однако это правило не всегда соблюдается. Пусть, например, объект А является файлом, а объект В — диском, на котором размещается этот файл. Когда объект А удален, доступ к его остаточной информации определяется семейством FDP_RIP «Защита остаточной информации», хотя она все еще остается частью объекта В.

Важно иметь в виду, что FDP_RIP «Защита остаточной информации» применяется только к объектам типа on-line, а не off-line (то есть не к автономным объектам, таким как резервные копии объектов на магнитных лентах). Например, если в ОО удаляется файл, в FDP_RIP может быть отображено требование отсутствия любой

остаточной информации при освобождении ресурса; тем не менее, ФБО не могут распространить осуществление этого требования на тот же файл, существующий в виде автономной резервной копии. Следовательно, этот файл по-прежнему доступен. Если важно обеспечить недоступность, то автору ПЗ/ЗБ следует удостовериться, что соответствующая цель безопасности для среды отражена в руководстве администратора применительно к автономным объектам.

Семейства FDP_RIP «Защита остаточной информации» и FDP_ROL «Откат» могут вступать в конфликт, если в первом отображено требование уничтожения остаточной информации во время передачи объекта от приложения к функциям безопасности (то есть при освобождении объекта). Поэтому результат выполнения операции выбора «недоступность при освобождении ресурса» в FDP_RIP «Защита остаточной информации» нельзя совместить с использованием FDP_ROL «Откат» из-за возможного отсутствия информации, необходимой для отката в предыдущее состояние. В этом случае в FDP_RIP «Защита остаточной информации» следует выбрать «недоступность при распределении ресурса», что позволяет использовать FDP_ROL «Откат», хотя существует риск, что ресурс, содержавший информацию, распределен новому объекту до выполнения отката. Если это произойдет, то откат будет невозможен.

В FDP_RIP «Защита остаточной информации» нет требований аудита из-за того, что в нем не отражены функции, вызываемые пользователем. Аудит распределенных или освобожденных ресурсов будет возможен как часть операций ПФБ управления доступом или информационными потоками.

Это семейство следует применять к объектам, специфицированным в ПФБ управления доступом или информационными потоками автором ПЗ/ЗБ.

F.9.2 FDP_RIP.1 Ограниченная защита остаточной информации

F.9.2.1 Замечания по применению для пользователя

Компонент FDP_RIP.1 содержит требование, что ФБО будут обеспечивать для подмножества объектов ОО отсутствие в распределенном этим объектам или освобожденном ими ресурсе доступной остаточной информации.

F.9.2.2 Операции

F.9.2.2.1 Выбор

В FDP_RIP.1.1 автору ПЗ/ЗБ следует специфицировать, в каком именно случае, при распределении или освобождении ресурсов, вызывается функция защиты остаточной информации.

F.9.2.2.2 Назначение

В FDP_RIP.1.1 автору ПЗ/ЗБ следует привести список объектов, для которых выполняется защита остаточной информации.

F.9.3 FDP_RIP.2 Полная защита остаточной информации

F.9.3.1 Замечания по применению для пользователя

Компонент FDP_RIP.2 содержит требование, что ФБО будут обеспечивать для всех объектов ОО отсутствие в распределенном этим объектам или освобожденном ими ресурсе доступной остаточной информации.

F.9.3.2 Операции

F.9.3.2.1 Выбор

В FDP_RIP.2.1 автору ПЗ/ЗБ следует специфицировать, в каком именно случае, при распределении или освобождении ресурсов, вызывается функция защиты остаточной информации.

F.10 Откат (FDP_ROL)

F.10.1 Замечания для пользователя

Семейство FDP_ROL связано с необходимостью возврата в полностью определенное допустимое состояние, например, если пользователю требуется отменить модификацию файла или отменить транзакции при незаконченной серии транзакций применительно к базе данных.

Данное семейство предназначено для содействия пользователю в возвращении в полностью определенное допустимое состояние после того, как он решил отменить некоторую совокупность последних действий или, для распределенной базы данных, вернуть все распределенные копии базы данных к состоянию перед выполнением отмененной операции.

Семейства FDP_RIP «Защита остаточной информации» и FDP_ROL «Откат» вступают в конфликт, если FDP_RIP «Защита остаточной информации» устанавливает, что содержание ресурса становится недоступным при освобождении ресурса объектом. Тогда FDP_RIP «Защита остаточной информации» нельзя использовать совместно с FDP_ROL «Откат» из-за отсутствия необходимой для отката информации. FDP_RIP «Защита остаточной информации» можно использовать совместно с FDP_ROL «Откат», если FDP_RIP «Защита остаточной информации» устанавливает, что при распределении ресурса объекту предыдущее содержание ресурса будет недоступно. Это возможно потому, что для успешного отката механизм FDP_ROL «Откат» получит доступ к предыдущей информации, которая все еще может находиться в ОО.

На требование отката накладываются некоторые ограничения. Например, текстовый редактор обычно позволяет откат только на определенное число команд. Другой пример связан с резервными копиями. Если лента для резервного копирования перематывалась, а затем на нее производилась новая запись, то первоначальная информация не может затем быть восстановлена. Это также ограничивает возможности отката.

F.10.2 FDP_ROL.1 Базовый откат

F.10.2.1 Замечания по применению для пользователя

Компонент FDP_ROL.1 позволяет пользователю или субъекту отменять некоторую совокупность операций над предопределенным множеством объектов. Отмена возможна только в некоторых пределах, например, на некоторое число символов или в определенном интервале времени.

F.10.2.2 Операции

F.10.2.2.1 Назначение

В FDP_ROL.1.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления доступом и/или информационными потоками, которые будут осуществляться при выполнении операций отката. Необходимо удостовериться, что откат не используется для обхода специфицированных ПФБ.

В FDP_ROL.1.1 автору ПЗ/ЗБ следует специфицировать список операций, допускающих откат.

В FDP_ROL.1.1 автору ПЗ/ЗБ следует специфицировать типы информации и/или список объектов, к которым применима политика отката.

В FDP_ROL.1.2 автору ПЗ/ЗБ следует специфицировать ограничение, в рамках которого могут выполняться операции отката. Это может быть интервал времени, например, могут быть отменены операции, выполненные в течение последних двух минут. Другими возможными ограничениями могут быть максимальное число отменяемых операций или размер буфера.

F.10.3 FDP_ROL.2 Расширенный откат

F.10.3.1 Замечания по применению для пользователя

Компонент FDP_ROL.2 содержит требование, чтобы ФБО предоставляли возможность отката всех операций, однако пользователь может выбрать для отката только часть из них.

F.10.3.2 Операции

F.10.3.2.1 Назначение

В FDP_ROL.2.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления доступом и/или ПФБ управления информационными потоками, которые будут осуществляться при выполнении операций отката. Это необходимо для того, чтобы удостовериться, что откат не используется для обхода специфицированных ПФБ.

В FDP_ROL.2.1 автору ПЗ/ЗБ следует специфицировать список объектов, к которым применима политика отката.

В FDP_ROL.2.2 автору ПЗ/ЗБ следует специфицировать ограничение, в рамках которого могут выполняться операции отката. Это может быть интервал времени, например, могут быть отменены операции, выполненные в течение последних двух минут. Другими возможными ограничениями могут быть максимальное число отменяемых операций или размер буфера.

F.11 Целостность хранимых данных (FDP_SDI)

F.11.1 Замечания для пользователя

Семейство FDP_SDI содержит требования, связанные с защитой данных пользователя во время их хранения в пределах ОДФ.

Аппаратные сбои и ошибки могут воздействовать на данные, хранимые в памяти. Семейство содержит требования по обнаружению таких непреднамеренных ошибок. В этом семействе также рассматривается целостность данных во время их хранения в запоминающих устройствах в пределах ОДФ.

Для предотвращения модификации данных субъектом требуется вместо этого семейства использовать семейства FDP_IFF «Функции управления инфлормационными потоками» или FDP_ACF «Функции управления доступом».

FDP_SDI отличается от семейства FDP_ITT «Передача в пределах ОО», которое защищает данные пользователя от ошибок целостности во время их передачи в пределах ОО.

F.11.2 FDP_SDI.1 Мониторинг целостности хранимых данных

F.11.2.1 Замечания по применению для пользователя

Компонент FDP_SDI.1 контролирует появление ошибок целостности данных, хранимых на носителе. Автор ПЗ/ЗБ может специфицировать различные типы атрибутов данных пользователя, на которых будет основан мониторинг.

F.11.2.2 Операции

F.11.2.2.1 Назначение

В FDP_SDI.1.1 автору ПЗ/ЗБ следует специфицировать ошибки целостности, которые будут выявлять ФБО.

В FDP_SDI.1.1 автору ПЗ/ЗБ следует специфицировать атрибуты данных пользователя, которые будут использоваться как основа для мониторинга.

F.11.3 FDP_SDI.2 Мониторинг целостности хранимых данных и предпринимаемые действия

F.11.3.1 Замечания по применению для пользователя

Компонент FDP_SDI.2 контролирует появление ошибок целостности данных, хранимых на носителе. Автор ПЗ/ЗБ может специфицировать, какие действия следует предпринять при обнаружении ошибок целостности.

F.11.3.2 Операции

F.11.3.2.1 Назначение

В FDP_SDI.2.1 автору ПЗ/ЗБ следует специфицировать ошибки целостности, которые будут выявлять ФБО.

В FDP_SDI.2.1 автору ПЗ/ЗБ следует специфицировать атрибуты данных пользователя, которые будут использоваться как основа для мониторинга.

В FDP_SDI.2.2 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые при обнаружении ошибки целостности.

F.12 Защита конфиденциальности данных пользователя при передаче между ФБО (FDP_UCT)

F.12.1 Замечания для пользователя

Семейство FDP_UCT определяет требования по обеспечению конфиденциальности данных пользователя при их передаче по внешнему каналу между ОО и другим доверенным продуктом ИТ. Конфиденциальность осуществляется путем предотвращения несанкционированного раскрытия данных при их передаче между двумя оконечными точками. Оконечными точками могут быть ФБО или пользователь.

Это семейство содержит требование защиты данных пользователя при передаче, тогда как семейство FPT_ITC «Конфиденциальность экспортируемых данных ФБО» имеет дело с данными ФБО.

F.12.2 FDP_UCT.1 Базовая конфиденциальность обмена данными

F.12.2.1 Замечания по применению для пользователя:

ФБО имеют возможность защитить от раскрытия некоторые данные пользователя во время обмена.

F.12.2.2 Операции

E.12.2.2.1 Назначение

В FDP_UCT.1.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления доступом и/или информационными потоками, которые будут осуществляться при обмене данными пользователя. Указанные политики будут осуществляться для принятия решений о том, кто и какими данными может обмениваться.

F.12.2.2.2 Выбор

В FDP_UCT.1.1 автору ПЗ/ЗБ следует определить, применяется этот элемент к механизму отправления или получения данных пользователя.

F.13 Защита целостности данных пользователя при передаче между ФБО (FDP_UIT)

F.13.1 Замечания для пользователя

Семейство FDP_UIT определяет требования по обеспечению целостности данных пользователя при их передаче между ФБО и другим доверенным продуктом ИТ, а также для их восстановления при обнаруживаемых ошибках. Как минимум, данное семейство контролирует целостность данных пользователя на предмет модификации. Кроме того, данное семейство поддерживает различные способы исправления обнаруженных ошибок целостности.

Данное семейство определяет требования по обеспечению целостности данных пользователя при передаче, тогда как семейство FPT_ITI «Целостность экспортируемых данных ФБО» имеет дело с данными ФБО.

Семейства FDP_UIT «Защита целостности данных пользователя при передаче между ФБО» и FDP_UCT «Защита конфиденциальности данных пользователя при передаче между ФБО» сходны между собой, поскольку FDP_UCT «Защита конфиденциальности данных пользователя при передаче между ФБО» связано с конфиденциальностью данных пользователя. Поэтому тот же механизм, который реализует FDP_UIT «Защита целостности данных пользователя при передаче между ФБО», мог бы использоваться и для реализации других семейств, таких как FDP_UCT «Защита конфиденциальности данных пользователя при передаче между ФБО» или FDP_ITC «Импорт данных из-за пределов действия ФБО».

F.13.2 FDP_UIT.1 Целостность передаваемых данных

E.13.2.1 Замечания по применению для пользователя

ФБО имеют базовую способность отправлять и получать данные пользователя способом, позволяющим обнаружить модификацию. От ФБО не требуется попыток восстановления модифицированных данных.

F.13.2.2 Операции

F.13.2.2.1 Назначение

В FDP_UIT.1.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления доступом и/или информационными потоками, которые будут осуществляться при обмене данными пользователя. Указанные политики будут осуществляться для принятия решений о том, кто может отправлять или получать данные и какие именно данные могут быть отправлены или получены.

F.13.2.2.2 Выбор

В FDP_UIT.1.1 автору ПЗ/ЗБ следует определить, применять ли этот элемент к ФБО при отправлении или получении объектов.

В FDP_UIT.1.1 автору ПЗ/ЗБ следует определить, защищать ли данные от модификации, удаления, вставки или повторения.

В FDP_UIT.1.2 автору ПЗ/ЗБ следует определить, обнаруживать ли ошибки типа модификации, удаления, вставки или повторения.

F.13.3 FDP_UIT.2 Восстановление переданных данных источником

F.13.3.1 Замечания по применению для пользователя

Компонент FDP_UIT.2 предоставляет возможность исправления совокупности идентифицированных ошибок передачи, если требуется, то с помощью другого доверенного продукта ИТ. Поскольку другой доверенный продукт ИТ находится за пределами ОДФ, ФБО не могут управлять режимом его функционирования. Тем не менее

в целях восстановления возможно предоставление функций, обладающих способностью выполняться координировано с другим доверенным продуктом ИТ. ФБО, например, могут включать в себя функции, способные побудить доверенный продукт ИТ, являющийся источником, повторить передачу данных после обнаружения ошибки. Этот компонент связан с возможностью ФБО реализовать такое восстановление при ошибках.

F.13.3.2 Операции

F.13.3.2.1 Назначение

В FDP_UIT.2.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления доступом и/или информационными потоками, которые будут осуществляться при обмене данными пользователя. Указанные политики будут осуществляться для принятия решений о том, какие данные и каким образом могут восстанавливаться.

В FDP_UIT.2.1 автору ПЗ/ЗБ следует привести список ошибок целостности, после которых ФБО с помощью доверенного продукта ИТ, являющегося источником, в состоянии восстановить первоначальное содержание данных пользователя.

F.13.4 FDP_UIT.3 Восстановление переданных данных получателем

F.13.4.1 Замечания по применению для пользователя

Компонент FDP_UIT.3 предоставляет возможность исправления совокупности идентифицированных ошибок передачи. Исправление выполняется без помощи доверенного продукта ИТ, являющего источником. Например, если обнаружены определенные ошибки, то необходима достаточная устойчивость протокола передачи с тем, чтобы дать возможность ФБО выполнить восстановление на основании контрольных сумм и другой предусмотренной протоколом информации.

F.13.4.2 Операции

F.13.4.2.1 Назначение

В FDP_UIT.3.1 автору ПЗ/ЗБ следует специфицировать ПФБ управления доступом и/или информационными потоками, которые будут осуществляться при обмене данными пользователя. Указанные политики будут осуществляться для принятия решений о том, какие данные и каким образом могут восстанавливаться.

В FDP_UIT.3.1 автору ПЗ/ЗБ следует привести список ошибок целостности, после которых ФБО, получающие данные, в состоянии самостоятельно восстановить первоначальное содержание данных пользователя.

Федеральное агентство по техническому регулированию и метрологии

Приложение G
(обязательное)

Идентификация и аутентификация (FIA)

Общим требованием безопасности является однозначная идентификация лица и/или объекта, выполняющего в ОО определенные функции. Это требование предполагает не только установление заявленного идентификатора каждого пользователя, но также и верификацию того, что каждый пользователь действительно тот, за кого себя выдает. Это достигается тем, что от пользователей требуется предоставлять ФБО некоторую информацию, которая, по сведениям ФБО, действительно ассоциирована с ними.

Семейства класса FIA определяют требования к функциям, устанавливающим и верифицирующим заявленный идентификатор каждого пользователя. Идентификация и аутентификация требуются для обеспечения ассоциации пользователей с соответствующими атрибутами безопасности (например, идентификаторами, группами, ролями, уровнями безопасности или целостности).

Однозначная идентификация уполномоченных пользователей и правильная ассоциация атрибутов безопасности с пользователями и субъектами критичны для осуществления определенных политик безопасности.

Семейство FIA_UID «Идентификация пользователя» предназначено для определения идентификатора пользователя.

Семейство FIA_UAU «Аутентификация пользователя» предназначено для верификации идентификатора пользователя.

Семейство FIA_AFL «Отказы аутентификации» предназначено для определения ограничений на число повторных неуспешных попыток аутентификации.

Семейство FIA_ATD «Определение атрибутов пользователя» предназначено для определения атрибутов пользователей, применяемых при осуществлении ПБО.

Семейство FIA_USB «Связывание пользователь-субъект» предназначено для корректной ассоциации атрибутов безопасности для каждого уполномоченного пользователя.

Семейство FIA_SOS «Спецификация секретов» предназначено для генерации и верификации секретов, соответствующих установленной метрике.

Декомпозиция класса FIA «Идентификация и аутентификация» на составляющие его компоненты показана на рисунке G.1.

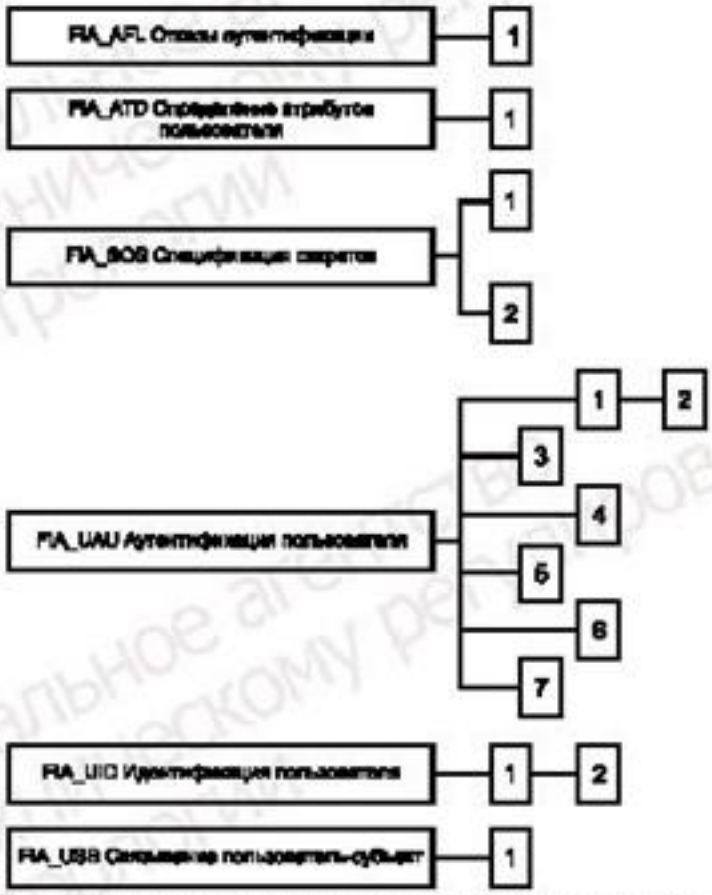

Рисунок G.1 — Декомпозиция класса FIA «Идентификация и аутентификация»

G.1 Отказы аутентификации (FIA_AFL)

G.1.1 Замечания для пользователя

Семейство FIA_AFL содержит требования по определению числа попыток аутентификации и действиям ФБО в случае их неудачи. Параметрами, определяющими возможное число попыток аутентификации, среди прочих могут быть число попыток и допустимый интервал времени.

Процесс открытия сеанса пользователя предусматривает взаимодействие с пользователем, позволяющее открыть сеанс и независимое от фактической реализации. Если число неуспешных попыток аутентификации превысило установленное значение, то блокируются учетные данные пользователя и/или терминал, с которого выполнялись запросы. Если учетные данные пользователя заблокированы, то он не может войти в систему. Если заблокирован терминал, то он (или его адрес) не может быть использован для входа в систему. Эта ситуация сохранится, пока условия для повторения попыток открытия сеанса не будут удовлетворены.

G.1.2 FIA_AFL.1 Обработка отказов аутентификации

G.1.2.1 Замечания по применению для пользователя

Автор ПЗ/ЗБ может установить число неуспешных попыток аутентификации либо доверить это разработчику ОО или уполномоченному пользователю. Подсчет неуспешных попыток аутентификации должен быть связан не с последовательностью их возникновения, а с каким-либо событием аутентификации. Таким событием может быть число неуспешных попыток с момента последнего сеанса, успешно открытого с данного терминала.

Автор ПЗ/ЗБ может определить список действий, которые должны предприниматься ФБО в случае отказа аутентификации. Уполномоченному администратору также может быть разрешено управлять этими событиями, если такую возможность предусмотрел автор ПЗ/ЗБ. Такими действиями, среди прочих, могут быть: отключение терминала, отключение учетных данных пользователя или подача сигнала тревоги администратору. Условия, при которых произойдет возвращение к обычному режиму работы, необходимо специфицировать через действия.

Для того, чтобы предотвратить полную невозможность обслуживания, в ОО обычно обеспечивается невозможность блокирования учетных данных, по меньшей мере, одного пользователя.

Автор ПЗ/ЗБ может устанавливать иные действия для ФБО, относящиеся в том числе к правилам деблокирования процесса открытия сеанса пользователя или подаче сигнала тревоги администратору. Примерами таких действий (правил) являются: до истечения установленного времени; пока уполномоченный администратор вновь не деблокирует терминал или учетные данные пользователя; до истечения времени, связанного с предыдущими неуспешными попытками (например, после каждой неуспешной попытки время блокирования удваивается).

G.1.2.2 Операции

G.1.2.2.1 Выбор

В FIA_AFL.1.1 автор ПЗ/ЗБ должен выбрать или назначение положительного целого числа, или выражение «устанавливаемое администратором положительное целое число», определив диапазон допустимых значений.

G.1.2.2.2 Назначение

В FIA_AFL.1.1 автору ПЗ/ЗБ следует специфицировать события аутентификации. Примерами являются: число неуспешных попыток аутентификации для данного идентификатора пользователя с момента последней успешной попытки; число неуспешных попыток аутентификации для данного терминала с момента последней успешной попытки; число неуспешных попыток аутентификации за последние 10 мин. Необходимо указать, по меньшей мере, одно событие аутентификации.

В FIA_AFL.1.1, если выбрано назначение положительного целого числа, автору ПЗ/ЗБ следует специфицировать задаваемое по умолчанию число (положительное целое) неуспешных попыток аутентификации, при достижении или превышении которого будут инициироваться определенные действия.

В FIA_AFL.1.1 если выбрано «устанавливаемое администратором положительное целое число», то автору ПЗ/ЗБ следует специфицировать диапазон допустимых значений, из которого администратор ОО может установить число неудачных попыток аутентификации. Число неудачных попыток аутентификации должно быть меньше или равняться значению верхней границы и больше или равняться значению нижней границы диапазона.

В FIA_AFL.1.2 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые в случае достижения или превышения предельного значения числа попыток. Такими действиями могут быть: блокирование учетных данных на 5 мин, блокирование терминала на увеличивающийся интервал времени (число секунд, равное 2^n, где n — число неуспешных попыток) или блокирование (с уведомлением администратора) учетных данных вплоть до его снятия администратором. В описании действий следует указать принимаемые меры и срок их действия (или условия прекращения действия этих мер).

G.2 Определение атрибутов пользователя (FIA_ATD)

G.2.1 Замечания для пользователя

Все уполномоченные пользователи могут, помимо идентификатора пользователя, иметь другие атрибуты безопасности, применяемые при осуществлении ПБО. Семейство FIA_ATD определяет требования для ассоциации атрибутов безопасности с пользователями в соответствии с необходимостью поддержки ПБО.

Существуют зависимости от определений отдельных политик безопасности. Следует, чтобы такие определения содержали списки атрибутов, необходимых для осуществления политики.

G.2.2 FIA_ATD.1 Определение атрибутов пользователя

G.2.2.1 Замечания по применению для пользователя

Компонент FIA_ATD.1 специфицирует атрибуты безопасности, которые следует поддерживать на уровне пользователя. Это означает, что назначение и возможное изменение атрибутов безопасности, указанных в списке, осуществляется на уровне пользователя (то есть для каждого пользователя индивидуально). Иными словами, изменение атрибутов из списка, ассоциированного с каким-либо пользователем, не должно влиять на атрибуты безопасности других пользователей.

Если атрибуты безопасности принадлежат группе пользователей (например список возможностей группы), пользователю потребуется иметь ссылку (как атрибут безопасности) на соответствующую группу.

G.2.2.2 Операции

G.2.2.2.1 Назначение

В FIA_ATD.1.1 автору ПЗ/ЗБ следует специфицировать атрибуты безопасности, ассоциируемые с каждым отдельным пользователем. Примером может служить список, включающий в себя атрибуты «уровень допуска», «идентификатор группы», «права».

G.3 Спецификация секретов (FIA_SOS)

G.3.1 Замечания для пользователя

Семейство FIA_SOS определяет требования к механизмам, которые реализуют определенную метрику качества для предоставляемых секретов и генерируют секреты, удовлетворяющие определенной метрике. Примерами таких механизмов могут быть автоматическая проверка предоставляемых пользователями паролей или автоматическая генерация паролей.

Секреты могут генерироваться вне ОО, например, выбираться пользователями и вводиться в систему. При этом может быть использован компонент FIA_SOS.1 «Верификация секретов» для обеспечения соответствия секретов, сгенерированных вне системы, конкретным условиям, таким как минимально допустимый размер, отсутствие в словаре и/или неприменение ранее.

Секреты могут также генерироваться самим ОО. В этом случае требование, чтобы сгенерированные ОО секреты соответствовали специфицированной метрике, обеспечивается компонентом FIA_SOS.2 «Генерация секретов ФБО».

Секреты, рассматриваемые в данном семействе, содержат аутентификационные данные, предъявляемые пользователем механизму аутентификации, основанному на сведениях, которыми располагает пользователь. Если используются криптографические ключи, вместо этого семейства следует использовать семейства класса FCS «Криптографическая поддержка».

G.3.2 FIA_SOS.1 Верификация секретов

G.3.2.1 Замечания по применению для пользователя

Секреты могут создаваться пользователем. Компонент FIA_SOS.1 обеспечивает возможность верификации соответствия секретов, созданных пользователем, определенной метрике качества.

G.3.2.2 Операции

G.3.2.2.1 Назначение

В FIA_SOS.1.1 автору ПЗ/ЗБ следует предоставить определенную метрику качества. Эта метрика может быть специфицирована как собственно описание проверки качества или как ссылка на нормативный документ, определяющий метрики качества, соответствие которым необходимо для секретов. К примерам метрик качества можно отнести описание допустимых символьных структур секретов и/или описание допустимых размеров секретов.

G.3.3 FIA_SOS.2 Генерация секретов ФБО

G.3.3.1 Замечания по применению для пользователя

Компонент FIA_SOS.2 позволяет ФБО генерировать секреты для специальных функций, таких как аутентификация по паролю.

Если в алгоритме генерации секретов используется генератор псевдослучайных чисел, то на его вход следует подавать произвольные величины, что будет обеспечивать высокую степень непредсказуемости выходных данных. Эти произвольные величины могут быть получены из таких доступных параметров системы, как системные часы, значения системных регистров, дата, время и т. д. Эти параметры следует выбирать с таким расчетом, чтобы число произвольных величин, которое можно из них получить, было бы не меньше минимального числа секретов, которые необходимо сгенерировать.

G.3.3.2 Операции

G.3.3.2.1 Назначение

В FIA_SOS.2.1 автору ПЗ/ЗБ следует обеспечить определенную метрику качества. Эта метрика может быть специфицирована как собственно описание проверки качества или как ссылка на нормативный документ, определяющий метрики качества, соответствие которым необходимо для секретов. К примерам метрик качества относятся описание допустимых символьных структур секретов и/или допустимых размеров секретов.

В FIA_SOS.2.2 автору ПЗ/ЗБ следует представить список функций из числа ФБО, для которых необходимо использовать секреты, генерируемые ФБО. Примером такой функции может служить механизм аутентификации по паролю.

G.4 Аутентификация пользователя (FIA_UAU)

G.4.1 Замечания для пользователя

Семейство FIA_UAU определяет типы механизмов аутентификации пользователя, предоставляемые ФБО. Оно также определяет те атрибуты, на которых необходимо базировать механизмы аутентификации пользователя.

G.4.2 FIA_UAU.1 Выбор момента аутентификации

G.4.2.1 Замечания по применению для пользователя

Компонент FIA_UAU.1 содержит требование, чтобы автор ПЗ/ЗБ определил список действий, которые выполняются при посредничестве ФБО и допускаются ФБО от имени пользователя до того, как будет произведена аутентификация пользователя. Эти действия, выполняемые при посредничестве ФБО, с точки зрения безопасности не имеют отношения к пользователям, неверно идентифицировавшим себя до аутентификации. Все прочие действия, выполняемые при посредничестве ФБО и не включенные в этот список, разрешаются пользователю только после завершения аутентификации.

Этот компонент не применим для разрешения каких-либо действий до выполнения идентификации. Для этого необходимо использовать FIA_UID.1 «Выбор момента идентификации» либо FIA_UID.2 «Идентификация до любого действия пользователя» с соответствующими назначениями.

G.4.2.2 Операции

G.4.2.2.1 Назначение

В FIA_UAU.1.1 автору ПЗ/ЗБ следует специфицировать список действий, выполняемых при посредничестве ФБО от имени пользователя прежде, чем завершится аутентификация пользователя. Этот список не может быть пустым. Если таких действий нет, следует вместо этого компонента использовать компонент FIA_UAU.2 «Аутентификация до любых действий пользователя». Примером таких действий может служить запрос о помощи при выполнении процедуры логического входа в систему.

G.4.3 FIA_UAU.2 Аутентификация до любых действий пользователя

G.4.3.1 Замечания по применению для пользователя

Компонент FIA_UAU.2 содержит требование завершения аутентификации пользователя до выполнения любых действий при посредничестве ФБО от имени этого пользователя.

G.4.4 FIA_UAU.3 Аутентификация, защищенная от подделок

G.4.4.1 Замечания по применению для пользователя

Компонент FIA_UAU.3 содержит требования к механизмам, предоставляющим защиту аутентификационных данных. Аутентификационные данные, заимствованные у другого пользователя или полученные незаконным способом, следует обнаружить и/или отвергнуть. Данные механизмы предоставляют уверенность, что пользователи, аутентифицированные ФБО, являются действительно теми, кем они представляются.

Этот компонент применим только для механизмов аутентификации, основанных на уникальных аутентификационных данных (например, биометрических). ФБО не смогут обнаружить и предотвратить тиражирование пароля за пределами ОДФ.

G.4.4.2 Операции

G.4.4.2.1 Выбор

В FIA_UAU.3.1 автору ПЗ/ЗБ следует специфицировать, будут ли ФБО обнаруживать и/или предотвращать подделку данных аутентификации.

В FIA_UAU.3.2 автору ПЗ/ЗБ следует специфицировать, будут ли ФБО обнаруживать и/или предотвращать копирование данных аутентификации.

G.4.5 FIA_UAU.4 Механизмы одноразовой аутентификации

G.4.5.1 Замечания по применению для пользователя

Компонент FIA_UAU.4 содержит требования к механизмам аутентификации, основанным на аутентификационных данных одноразового использования. В качестве таких данных может использоваться то, что пользователь имеет или знает, но не свойства самого пользователя. Примеры одноразовых данных аутентификации пользователя: одноразовые пароли, зашифрованные метки времени, случайные числа секретной таблицы преобразований.

Автор ПЗ/ЗБ может определить, к какому механизму(ам) аутентификации применимы эти требования.

G.4.5.2 Операции

G.4.5.2.1 Назначение

В FIA_UAU.4.1 автору ПЗ/ЗБ следует привести список механизмов аутентификации, к которым применяется это требование. Назначением может быть: «все механизмы аутентификации». Примером назначения может быть также следующее: «механизмы аутентификации, используемые для аутентификации пользователей во внешней сети».

G.4.6 FIA_UAU.5 Сочетание механизмов аутентификации

G.4.6.1 Замечания по применению для пользователя

Применение компонента FIA_UAU.5 позволяет специфицировать требования к применению нескольких механизмов аутентификации в ОО. Требования, применяемые к каждому отдельному механизму, необходимо выбирать из класса FIA «Идентификация и аутентификация». Чтобы отразить разные требования к разным механизмам аутентификации, можно многократно использовать один и тот же выбранный компонент.

Для обеспечения возможностей механизмов аутентификации, а также правил, определяющих успешность аутентификации, можно привлекать функции управления из класса FMT.

Для допуска в систему анонимных пользователей можно ввести механизм аутентификации типа «отсутствие аутентификации». Использование доступа такого типа следует четко разъяснить в правилах FIA_UAU.5.2.

G.4.6.2 Операции

G.4.6.2.1 Назначение

В FIA_UAU.5.1 автору ПЗ/ЗБ следует определить предоставляемые механизмы аутентификации. Примером списка механизмов может быть следующий: «отсутствие аутентификации, механизм пароля, биометрия (сканирование сетчатки), механизм ключа шифрования».

В FIA_UAU.5.2 автору ПЗ/ЗБ следует специфицировать правила, описывающие, как механизмы аутентификации обеспечивают аутентификацию и когда используется каждый из них. Это значит, что для любой возможной ситуации необходимо указать совокупность механизмов, которые могли бы использоваться для аутентификации. Пример такого правила: «для аутентификации пользователей, имеющих особые права доступа, должны совместно использоваться механизм пароля и биометрия, причем аутентификация успешна при успешной аутентификации каждым механизмом; для аутентификации остальных пользователей должен использоваться только механизм пароля».

Автор ПЗ/ЗБ может задать ограничения, в пределах которых уполномоченному администратору разрешено специфицировать конкретные правила. Пример правила: «аутентификация пользователя всегда должна производиться посредством аппаратного ключа; администратор может специфицировать дополнительные механизмы аутентификации, которые также необходимо использовать». Автор ПЗ/ЗБ может и не специфицировать ограничения, а оставить выбор механизмов аутентификации и их правил полностью на усмотрение уполномоченного администратора.

G.4.7 FIA_UAU.6 Повторная аутентификация

G.4.7.1 Замечания по применению для пользователя

В компоненте FIA_UAU.6 рассматривается потенциальная потребность повторной аутентификации пользователей в определенные моменты времени. Такая потребность может возникнуть при обращении пользователя к ФБО с запросом о выполнении действий, критичных по безопасности, а также при запросах о повторной аутентификации, исходящих от сущностей, не связанных с ФБО, например, от серверного приложения, которое запрашивает от ФБО повторную аутентификацию обслуживаемого клиента.

G.4.7.2 Операции

G.4.7.2.1 Назначение

В FIA_UAU.6.1 автору ПЗ/ЗБ следует привести список условий, требующих повторной аутентификации. Этот список может включать в себя завершение периода времени, выделенного пользователю, запрос пользователя с целью изменения действующих атрибутов безопасности или запрос пользователя к ФБО с целью выполнения некоторых критичных функций безопасности.

Автор ПЗ/ЗБ может задать пределы, в которых следует допускать повторную аутентификацию, оставив их детализацию на усмотрение уполномоченного администратора. Пример подобного правила: «пользователь должен проходить повторную аутентификацию не реже одного раза в сутки; администратор может потребовать более частую повторную аутентификацию, но не чаще одного раза в 10 мин».

G.4.8 FIA_UAU.7 Аутентификация с защищенной обратной связью

G.4.8.1 Замечания по применению для пользователя

В компоненте FIA_UAU.7 рассматривается обратная связь с пользователем в процессе аутентификации. В некоторых системах обратная связь выражается в том, что пользователю сообщается число набранных им символов, но сами символы скрываются, в других системах даже эта информация может считаться неприемлемой.

Этот компонент содержит требование, чтобы аутентификационные данные не возвращались пользователю в первоначальном виде. В рабочих станциях принято представлять набранные символы пароля условными знаками (например, звездочками).

G.4.8.2 Операции

G.4.8.2.1 Назначение

В FIA_UAU.7.1 автору ПЗ/ЗБ следует определить вид обратной связи с пользователем при проведении аутентификации. Примером такого назначения может служить «число набранных символов», другой тип обратной связи — «механизм аутентификации, через который не удалось осуществить аутентификацию».

G.5 Идентификация пользователя (FIA_UID)

G.5.1 Замечания для пользователя

Семейство FIA_UID определяет условия, при которых от пользователей требуется собственная идентификация до выполнения при посредничестве ФБО каких-либо иных действий, требующих идентификации пользователя.

G.5.2 FIA_UID.1 Выбор момента идентификации

G.5.2.1 Замечания по применению для пользователя

Компонент FIA_UID.1 устанавливает требования по идентификации пользователей. Автор ПЗ/ЗБ может указать конкретные действия, которые могут быть выполнены до завершения идентификации.

При использовании компонента упоминаемые в нем действия, которые допускается выполнять при посредничестве ФБО до идентификации, следует также привести и в компоненте FIA_UAU.1 «Выбор момента аутентификации».

G.5.2.2 Операции

G.5.2.2.1 Назначение

В FIA_UID.1.1 автору ПЗ/ЗБ следует специфицировать список действий, выполняемых при посредничестве ФБО от имени пользователя до его собственной идентификации. Этот список не может быть пустым. Если приемлемых действий нет, следует вместо этого компонента использовать компонент FIA_UID.2 «Идентификация до любого действия пользователя». Примером таких действий может служить запрос о помощи при выполнении процедуры логического входа в систему.

G.5.3 FIA_UID.2 Идентификация до любых действий пользователя

G.5.3.1 Замечания по применению для пользователя

Компонент FIA_UID.2 содержит требование идентификации пользователей. До идентификации пользователя ФБО не допускают выполнение им никаких действий.

G.6 Связывание пользователь-субъект (FIA_USB)

G.6.1 Замечания для пользователя

Для работы с ОО аутентифицированный пользователь обычно активизирует какой-либо субъект. Тогда атрибуты безопасности этого пользователя ассоциируются (полностью или частично) с этим субъектом. Семейство FIA_USB определяет требования по созданию и сопровождению ассоциации атрибутов безопасности пользователя с субъектом, действующим от имени пользователя.

G.6.2 FIA_USB.1 Связывание пользователь-субъект

G.6.2.1 Замечания по применению для пользователя

Выражение «действующий от имени», использовавшееся и ранее, требует некоторых пояснений. Установлено, что субъект действует от имени пользователя, создавшего субъект или активизировавшего его для решения некоторой задачи. Поэтому, когда субъект создается, то он действует от имени пользователя, инициировавшего его создание. Если пользователь предпочитает анонимность, субъект также действует от его имени, но идентификатор этого пользователя неизвестен. Особую категорию составляют субъекты, которые обслуживают нескольких пользователей (например серверный процесс). Тогда «владельцем» этого субъекта считается пользователь, создавший его.

G.6.2.2 Операции

G.6.2.2.1 Назначение

В FIA_USB.1 автору ПЗ/ЗБ следует специфицировать список атрибутов безопасности пользователя, которые должны быть связаны с субъектами.

В FIA_USB.1.2 автору ПЗ/ЗБ следует специфицировать какие-либо правила, которые должны применяться по отношению к исходной ассоциации атрибутов с субъектами, или слово «нет».

В FIA_USB.1.3 автору ПЗ/ЗБ следует специфицировать какие-либо правила, которые должны применяться при внесении изменений в атрибуты безопасности пользователей, связанные с субъектами, действующими от имени пользователей, или слово «нет».

Федеральное агентство по техническому регулированию и метрологии

Приложение Н
(обязательное)

Управление безопасностью (FMT)

Класс FMT предназначен для спецификации управления некоторыми аспектами ФБО: атрибутами безопасности, данными и отдельными функциями. Могут быть также установлены различные роли управления и определено их взаимодействие, например распределение обязанностей.

Если ОО состоит из нескольких физически разделенных частей, образующих распределенную систему, то проблемы синхронизации, относящиеся к распространению атрибутов безопасности, данных ФБО и модификации функций, становятся очень сложными, особенно, если требуется дублирование информации в различных частях ОО. Эти проблемы следует принять во внимание при выборе компонентов FMT_REV.1 «Отмена» и FMT_SAE.1 «Ограниченная по времени авторизация», поскольку при этом возможно нарушение нормального выполнения ФБО. В такой ситуации рекомендуется воспользоваться компонентами семейства FPT_TRC «Согласованность данных ФБО при дублировании в пределах ОО».

Декомпозиция класса FMT «Управление безопасностью» на составляющие его компоненты показана на рисунке Н.1.

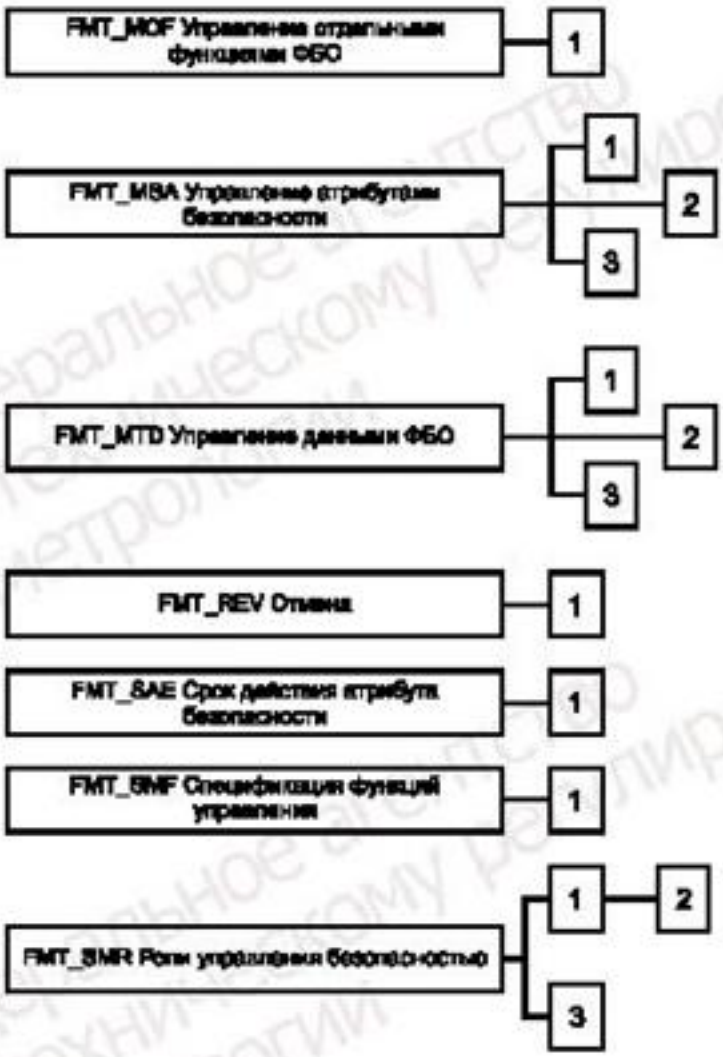

Рисунок Н.1 — Декомпозиция класса FMT «Управление безопасностью»

H.1 Управление отдельными функциями ФБО (FMT_MOF)

H.1.1 Замечания для пользователя

Функции управления из числа ФБО дают уполномоченным пользователям возможность устанавливать операции безопасности ОО и управлять ими. Эти административные функции обычно подразделяют на несколько категорий:

a) функции управления, относящиеся к управлению доступом, учету пользователей и аутентификации, реализованные в ОО, например определение и обновление характеристик безопасности пользователей (таких, как уникальные идентификаторы, ассоциированные с именами пользователей, учетные данные пользователей, параметры входа в систему), определение и обновление средств управления аудитом системы (выбор событий аудита, управление журналами аудита, анализ журнала аудита и генерация отчетов аудита), определение и обновление атрибутов политики, назначенных пользователю (таких, как уровень допуска), определение системных меток управления доступом, управление группами пользователей;

b) функции управления, относящиеся к контролю доступности, например определение и модификация параметров доступности или квот ресурсов;

c) функции управления, связанные в основном с инсталляцией и конфигурацией, например конфигурация ОО, ручное восстановление, инсталляция исправлений, относящихся к безопасности ОО (при их наличии), восстановление и реинсталляция аппаратных средств;

d) функции управления, связанные с текущим управлением и сопровождением ресурсов ОО, например подключение и отключение периферийных устройств, установка съемных носителей памяти, резервное копирование и восстановление объектов пользователей и системы.

Следует отметить, что эти функции требуется представить в ОО на основе семейств, включенных в ПЗ или ЗБ. Автор ПЗ/ЗБ должен предусмотреть необходимые функции, обеспечивающие безопасное управления системой.

Допускается включение в число ФБО функций, которыми может управлять администратор. Например, могут быть предусмотрены отключение функций аудита, переключение синхронизации времени, модификация механизма аутентификации.

H.1.2 FMT_MOF.1 Управление режимом выполнения функций безопасности

H.1.2.1 Замечания по применению для пользователя

Компонент FMT_MOF.1 предоставляет идентифицированным ролям возможность управления функциями из числа ФБО. Может потребоваться выяснить текущее состояние функции безопасности, отключить или подключить функцию безопасности, модифицировать режим ее выполнения. Примером модификации режима выполнения является изменение механизмов аутентификации.

H.1.2.2 Операции

H.1.2.2.1 Выбор

В FMT_MOF.1.1 автору ПЗ/ЗБ следует выбрать для роли возможность следующих действий: определение режима выполнения функций безопасности, отключение функций безопасности, подключение функций безопасности и/или модификация режима выполнения функций безопасности.

H.1.2.2.2 Назначение

В FMT_MOF.1.1 автору ПЗ/ЗБ следует специфицировать функции, которые могут быть модифицированы идентифицированными ролями. Примерами таких функций являются функции аудита или определения времени.

В FMT_MOF.1.1 автору ПЗ/ЗБ следует специфицировать роли, которые допускаются к модификации функций из числа ФБО. Все возможные роли специфицированы в FMT_SMR.1 «Роли безопасности».

H.2 Управление атрибутами безопасности (FMT_MSA)

H.2.1 Замечания для пользователя

Семейство FMT_MSA определяет требования по управлению атрибутами безопасности.

У пользователей, субъектов и объектов есть ассоциированные атрибуты безопасности, которые оказывают влияние на режим выполнения ФБО. Примерами атрибутов безопасности являются группы, в которые входит пользователь, роли, которые он может принимать, приоритет процесса (субъекта), а также права, которыми наделены роль или пользователь. Может возникнуть необходимость в управлении этими атрибутами безопасности со стороны пользователя, субъекта или специально уполномоченного пользователя (пользователя с явно предоставленными правами для такого управления).

Следует отметить, что право на назначение прав пользователям само по себе является атрибутом безопасности и/или потенциальным субъектом управления в компоненте FMT_MSA.1 «Управление атрибутами безопасности».

Компонент FMT_MSA.2 «Безопасные значения атрибутов безопасности» можно использовать для обеспечения того, что выбранное сочетание атрибутов безопасности находится в рамках безопасного состояния. Определение, что понимать как «безопасное», возлагается на руководства ОО и модель ПБО. Если разработчик предоставил четкое определение безопасных значений и доводы, почему их следует считать безопасными, зависимостью FMT_MSA.2 «Безопасные значения атрибутов безопасности» от ADV_SPM.1 «Неформальная модель политики безопасности ОО» можно пренебречь.

В некоторых случаях субъекты, объекты или учетные данные пользователей создаются заново. Если при этом не заданы явно значения атрибутов безопасности, связанные с субъектами, объектами или пользователя-

ми, то необходимо использовать значения по умолчанию. Компонент FMT_MSA.1 можно использовать для определения того, что этими значениями, задаваемыми по умолчанию, можно управлять.

Н.2.2 FMT_MSA.1 Управление атрибутами безопасности

Н.2.2.1 Замечания по применению для пользователя

Компонент FMT_MSA.1 допускает пользователей, исполняющих некоторые роли, к управлению идентифицированными атрибутами безопасности. Принятие роли пользователем осуществляется в компоненте FMT_SMR.1 «Роли безопасности».

Задаваемым по умолчанию называется значение параметра, которое он принимает, когда отображается без специально указанного значения. Начальное же значение предоставляется при отображении (создании) параметра, замещая заданное по умолчанию.

Н.2.2.2 Операции

Н.2.2.2.1 Назначение

В FMT_MSA.1.1 автору ПЗ/ЗБ следует указать ПФБ управления доступом или информационными потоками, для которой применимы атрибуты безопасности.

Н.2.2.2.2 Выбор

В FMT_MSA.1.1 автору ПЗ/ЗБ следует специфицировать операции, которые можно применять к идентифицированным атрибутам безопасности. Автор ПЗ/ЗБ может специфицировать, что роль допускается к изменению задаваемых по умолчанию значений атрибутов безопасности, запросу и модификации значений атрибутов безопасности, полному удалению атрибутов безопасности, а также определить собственные операции с ними.

Н.2.2.2.3 Назначение

В FMT_MSA.1.1 автору ПЗ/ЗБ следует специфицировать атрибуты безопасности, которыми могут оперировать идентифицированные роли. Допускается, чтобы автор ПЗ/ЗБ специфицировал возможность управления задаваемыми по умолчанию величинами, например, задаваемыми по умолчанию правами доступа. Примерами данных атрибутов безопасности являются: уровень допуска, приоритет уровня обслуживания, список управления доступом, права доступа по умолчанию.

В FMT_MSA.1.1 автору ПЗ/ЗБ следует специфицировать роли, допущенные к операциям с атрибутами безопасности. Все возможные роли специфицируют в FMT_SMR.1.

В FMT_MSA.1.1, если сделан соответствующий выбор, автору ПЗ/ЗБ следует специфицировать, какие дополнительные операции может выполнять роль. Примером такой операции может служить операция «создать».

Н.2.3 FMT_MSA.2 Безопасные значения атрибутов безопасности

Н.2.3.1 Замечания по применению для пользователя

Компонент FMT_MSA.2 содержит требования к значениям, которые могут присваиваться атрибутам безопасности. Следует присваивать такие значения, чтобы ОО оставался в безопасном состоянии.

Определение «безопасных» значений в этом компоненте не раскрывается и оставлено для разработчика ОО (конкретно для компонента ADV_SPM.1 «Неформальная модель политики безопасности ОО») и руководств. Примером может служить нетривиальный пароль, назначаемый пользователю при регистрации.

Н.2.4 FMT_MSA.3 Инициализация статических атрибутов

Н.2.4.1 Замечания по применению для пользователя

Компонент FMT_MSA.3 содержит требования, чтобы ФБО предоставлял возможность как присвоения атрибутам безопасности объектов значений по умолчанию, так и их замены начальными значениями. Действительно, при создании новых объектов возможно иметь различающиеся значения атрибутов безопасности, если существует механизм спецификации полномочий во время создания объекта.

Н.2.4.2 Операции

Н.2.4.2.1 Назначение

В FMT_MSA.3.1 автору ПЗ/ЗБ следует указать ПФБ управления доступом или информационными потоками, для которой применимы атрибуты безопасности.

Н.2.4.2.2 Выбор

В FMT_MSA.3.1 автору ПЗ/ЗБ следует специфицировать, будут ли заданные по умолчанию свойства атрибутов управления доступом ограничивающими, разрешающими или иного характера. В последнем случае автору ПЗ/ЗБ следует уточнить характер этих свойств. Может быть выбран только один из представленных вариантов.

Н.2.4.2.3 Назначение

В FMT_MSA.3.1, если автор ПЗ/ЗБ выбирает другое свойство, то ему следует специфицировать требуемые характеристики значений по умолчанию.

В FMT_MSA.3.2 автору ПЗ/ЗБ следует специфицировать роли, допущенные к модификации значений атрибутов безопасности. Все возможные роли специфицируют в FMT_SMR.1 «Роли безопасности».

Н.3 Управление данными ФБО (FMT_MTD)

Н.3.1 Замечания для пользователя

Семейство FMT_MTD устанавливает требования по управлению данными ФБО. Примерами данных ФБО являются текущее время и журнал аудита. Например, данное семейство дает возможность специфицировать, кому разрешено читать, удалять или создавать журнал аудита.

Н.3.2 FMT_MTD.1 Управление данными ФБО

Н.3.2.1 Замечания по применению для пользователя

Компонент FMT_MTD.1 позволяет пользователям, которым присвоены определенные роли, управлять значениями данных ФБО. Назначение пользователей на роль рассмотрено в компоненте FMT_SMR.1 «Роли безопасности».

«Задаваемым по умолчанию» называется значение параметра, которое он принимает, если отображается без специально указанного значения. Начальное же значение предоставляется при отображении (создании) параметра, замещая заданное по умолчанию.

Н.3.2.2 Операции

Н.3.2.2.1 Выбор

В FMT_MTD.1.1 автору ПЗ/ЗБ следует специфицировать операции, которые могут быть применены к идентифицированным данным ФБО. Автор ПЗ/ЗБ может специфицировать, что роль может изменять заданные по умолчанию значения, выполнять очистку, чтение, модификацию или полное удаление данных ФБО. По желанию автор ПЗ/ЗБ может специфицировать какой-либо тип операции. «Очистка данных ФБО» означает, что содержание данных удаляется, но категория данных остается в системе.

Н.3.2.2.2 Назначение

В FMT_MTD.1.1 автору ПЗ/ЗБ следует специфицировать, какими данными ФБО могут оперировать идентифицированные роли. Допускается, что автор ПЗ/ЗБ специфицирует возможность управления значениями, задаваемыми по умолчанию.

В FMT_MTD.1.1 автору ПЗ/ЗБ следует специфицировать роли, допущенные к операциям с данными ФБО. Все возможные роли специфицируют в FMT_SMR.1 «Роли безопасности».

В FMT_MTD.1.1, если сделан соответствующий выбор, автору ПЗ/ЗБ следует специфицировать, какие дополнительные операции может выполнять роль. Примером такой операции может быть операция «создать».

Н.3.3 FMT_MTD.2 Управление ограничениями данных ФБО

Н.3.3.1 Замечания по применению для пользователя

Компонент FMT_MTD.2 специфицирует граничные значения для данных ФБО и действия, предпринимаемые в случае их превышения. Могут быть указаны, например, допустимый объем журнала аудита и действия при его переполнении.

Н.3.3.2 Операции

Н.3.3.2.1 Назначение

В FMT_MTD.2.1 автору ПЗ/ЗБ следует специфицировать данные ФБО, имеющие ограничения, и значения этих ограничений. Примером таких данных ФБО является число пользователей, осуществивших вход в систему.

В FMT_MTD.2.1 автору ПЗ/ЗБ следует специфицировать роли, допущенные к модификации как ограничений данных ФБО, так и действий в случае нарушения ограничений. Все возможные роли специфицированы в FMT_SMR.1 «Роли безопасности».

В FMT_MTD.2.2 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые в случае превышения предельных значений специфицированных данных ФБО. Примером таких действий, выполняемых ФБО, является информирование уполномоченного администратора и генерация записи аудита.

Н.3.4 FMT_MTD.3 Безопасные данные ФБО

Н.3.4.1 Замечания по применению для пользователя

Компонент FMT_MTD.3 распространяется на требования к значениям, которые могут присваиваться данным ФБО. Следует присваивать такие значения, чтобы ОО оставался в безопасном состоянии.

Определение «безопасных» значений в этом компоненте не раскрывается и оставлено для разработчика ОО (конкретно для компонента ADV_SPM.1 «Неформальная модель политики безопасности ОО») и руководств. Если разработчик предоставил четкое определение безопасных значений и объяснение, почему их следует считать безопасными, зависимостью FMT_MTD.3 «Безопасные данные ФБО» от ADV_SPM.1 «Неформальная модель политики безопасности ОО» можно пренебречь.

Н.4 Отмена (FMT_REV)

Н.4.1 Замечания для пользователя

Семейство FMT_REV связано с отменой атрибутов безопасности различных сущностей в пределах ОО.

Н.4.2 FMT_REV.1 Отмена

Н.4.2.1 Замечания по применению для пользователя

В компоненте FMT_REV.1 специфицируются требования по отмене прав. Он содержит требование спецификации правил отмены, например:

a) отмена произойдет при следующем входе пользователя в систему;

b) отмена произойдет при следующей попытке открыть файл;

c) отмена произойдет по истечении установленного времени, что может означать пересмотр всех открытых соединений через каждые X минут.

Н.4.2.2 Операции

Н.4.2.2.1 Выбор

В FMT_REV.1.1 автору ПЗ/ЗБ следует специфицировать, должна ли быть предоставлена возможность отменять с использованием ФБО атрибуты безопасности пользователей, субъектов, объектов или каких-либо дополнительных ресурсов.

H.4.2.2.2 Назначение

В FMT_REV.1.1 автору ПЗ/ЗБ следует указать роли, допущенные к отмене атрибутов безопасности. Все возможные роли специфицируют в FMT_SMR.1 «Роли безопасности».

В FMT_REV.1.1 автору ПЗ/ЗБ следует, если выбраны дополнительные ресурсы, специфицировать, должна ли быть предоставлена возможность отменять атрибуты безопасности с использованием ФБО.

В FMT_REV.1.2 автору ПЗ/ЗБ следует специфицировать правила отмены. К правилам, в частности, могут быть отнесены: «перед следующей операцией над ассоциированным ресурсом» или «при создании каждого нового субъекта».

H.5 Срок действия атрибутов безопасности (FMT_SAE)

H.5.1 Замечания для пользователя

Семейство FMT_SAE связано с возможностью установления срока действия атрибутов безопасности. Оно может применяться при спецификации требований к сроку действия атрибутов управления доступом, атрибутов идентификации и аутентификации, сертификатов (например, сертификатов ключей по X509), атрибутов аудита и т. д.

H.5.2 FMT_SAE.1 Ограниченная по времени авторизация

H.5.2.1 Операции

H.5.2.1.1 Назначение

В FMT_SAE.1.1 автору ПЗ/ЗБ следует представить список атрибутов безопасности, для которых поддерживается ограничение срока действия. Примером такого атрибута является уровень допуска пользователя.

В FMT_SAE.1.1 автору ПЗ/ЗБ следует указать роли, допущенные к назначению срока действия атрибутов безопасности. Все возможные роли специфицируют в FMT_SMR.1 «Роли безопасности».

В FMT_SAE.1.2 автору ПЗ/ЗБ следует представить список действий, предпринимаемых по отношению к каждому атрибуту безопасности по истечении срока его действия. Примером является назначение уровню допуска пользователя, по истечении срока его действия, значения, минимального для данного ОО. Если в ПЗ/ЗБ предусматривается немедленная отмена, то следует специфицировать действие «немедленная отмена».

H.6 Спецификация функций управления (FMT_SMF)

H.6.1 Замечания для пользователя

Данное семейство позволяет специфицировать функции управления, предоставляемые ОО. Каждая функция управления безопасностью, внесенная в список выполнения назначения, является функцией управления атрибутами безопасности либо функцией управления данными ФБО, либо функцией управления функциями безопасности.

H.6.2 FMT_SMF.1 Спецификация функций управления

H.6.2.1 Замечания по применению для пользователя

Данный компонент специфицирует функции управления, которые должны быть предоставлены.

Авторам ПЗ/ЗБ следует принять во внимание пункты «Управление» для компонентов, включенных в их ПЗ/ЗБ, чтобы обеспечить основу для функций управления, которые будут перечислены в данном компоненте.

H.6.2.2 Операции

H.6.2.2.1 Назначение

В FMT_SMF.1 автору ПЗ/ЗБ следует специфицировать функции управления, предоставляемые ФБО для управления атрибутами безопасности либо для управления данными ФБО, либо для управления функциями безопасности.

H.7 Роли управления безопасностью (FMT_SMR)

H.7.1 Замечания для пользователя

Семейство FMT_SMR уменьшает вероятность ущерба, который могут нанести пользователи действиями, выходящими за рамки назначенных им функциональных обязанностей. В семействе также рассматривается противодействие угрозе применения неадекватных механизмов, предоставляемых для безопасного управления ФБО.

Данное семейство содержит требования к предоставлению информации по поддержке идентификации полномочий пользователя на применение отдельных административных функций, относящихся к безопасности.

Некоторые действия управления могут выполнять пользователи, другие — только специально назначенные лица конкретной организации. Данное семейство позволяет определять различные роли, такие как владелец, аудитор, администратор, дежурный администратор.

Все роли данного семейства связаны с безопасностью. Каждая роль может предоставлять широкие возможности (например доступ ко всей структуре UNIX) или незначительные права (например право чтения объектов единственного типа, таких как файл помощи). Все роли определяют в этом семействе. Возможности ролей определяют в семействах FMT_MOF «Управление отдельными функциями ФБО», FMT_MSA «Управление атрибутами безопасности» и FMT_MTD «Управление данными ФБО».

Некоторые типы ролей могут быть взаимно исключающими. Например, дежурный администратор может быть способен определять и активизировать пользователей, но не удалять их (эта возможность закреплена за ролью администратора). Данное семейство допускает спецификацию политик двойного управления.

Н.7.2 FMT_SMR.1 Роли безопасности

Н.7.2.1 Замечания по применению для пользователя

Компонент FMT_SMR.1 определяет различные роли, которые ФБО следует распознавать. В системах часто проводится различие между владельцем сущности, администратором и остальными пользователями.

Н.7.2.2 Операции

Н.7.2.2.1 Назначение

В FMT_SMR.1.1 автору ПЗ/ЗБ следует специфицировать роли, которые распознаются системой. Это роли, которые могут исполнять пользователи относительно безопасности. Примеры ролей: владелец, аудитор, администратор.

Н.7.3 FMT_SMR.2 Ограничения на роли безопасности

Н.7.3.1 Замечания по применению для пользователя

Компонент FMT_SMR.2 специфицирует различные роли, которые ФБО следует распознавать, и условия, при которых этими ролями можно управлять. В системах часто проводится различие между владельцем сущности, администратором и другими пользователями.

Условия, налагаемые на роли, определяют взаимоотношения различных ролей, а также ограничения на принятие роли пользователем.

Н.7.3.2 Операции

Н.7.3.2.1 Назначение

В FMT_SMR.2.1 автору ПЗ/ЗБ следует специфицировать роли, которые распознаются системой. Это роли, которые могут исполнять пользователи относительно безопасности. Примеры ролей: владелец, аудитор, администратор.

В FMT_SMR.2.3 автору ПЗ/ЗБ следует специфицировать условия, которым необходимо следовать при управлении назначением роли. Примерами таких условий являются: «заказчик не может исполнять роль аудитора или администратора» или «пользователю, исполняющему роль ассистента, необходимо также исполнять роль владельца».

Н.7.4 FMT_SMR.3 Принятие ролей

Н.7.4.1 Замечания по применению для пользователя

Компонент FMT_SMR.3 определяет, что для принятия некоторых ролей необходим явный запрос.

Н.7.4.2 Операции

Н.7.4.2.1 Назначение

В FMT_SMR.3.1 автору ПЗ/ЗБ следует специфицировать роли, для принятия которых требуется явный запрос. Примеры: аудитор и администратор.

Федеральное агентство по техническому регулированию и метрологии

Приложение I
(обязательное)

Приватность (FPR)

Класс FPR описывает требования, которые могут накладываться для удовлетворения потребности пользователя в приватности, допуская максимально возможную гибкость системы, но оставляя в то же время возможной поддержку достаточного управления функционированием системы.

Компоненты этого класса достаточно гибки, чтобы учитывать, распространяется ли действие затребованных функций безопасности на уполномоченных пользователей. Например, автор ПЗ/ЗБ может посчитать, что не потребуется защита приватности пользователя от пользователей, наделенных специальными полномочиями.

Класс FPR вместе с другими классами (содержащими требования аудита, управления доступом, предоставления доверенного маршрута и неотказуемости) обеспечивает гибкость при спецификации желательного режима приватности. В то же время требования этого класса могут налагать ограничения на использование компонентов других классов, таких как FIA «Идентификация и аутентификация» или FAU «Аудит безопасности». Например, если уполномоченным пользователям не разрешено знать идентификатор пользователя (например, в семействах «Анонимность» или «Псевдонимность»), то, очевидно, невозможно будет оставить отдельных пользователей ответственными за выполняемые ими относящиеся к безопасности действия, на которые распространяются требования приватности. Тем не менее и в этом случае возможно включение в ПЗ/ЗБ требований аудита, если возникновение некоторых событий, связанных с безопасностью, важнее, чем знание о том, кто был их инициатором.

Дополнительная информация по этому вопросу представлена в замечаниях по применению класса FAU, где разъясняется, что вместо идентификатора в контексте аудита может применяться псевдоним или другая информация, которая могла бы идентифицировать пользователя.

Данный класс содержит четыре семейства: «Анонимность», «Псевдонимность», «Невозможность ассоциации» и «Скрытность». Три первых семейства имеют сложные взаимосвязи. При выборе семейства для применения следует учитывать выявленные угрозы. Для некоторых типов угроз приватности «Псевдонимность» подойдет больше, чем «Анонимность» (например, при требовании проведения аудита). Кроме того, некоторым видам угроз приватности наилучшим образом противостоит сочетание компонентов из нескольких семейств.

Во всех семействах предполагается, что пользователь явно не выполняет действий, раскрывающих его собственный идентификатор. Например, ФБО, как ожидают, не покажут на экране имя пользователя в сообщениях электронной почты или базах данных.

Все семейства этого класса имеют компоненты, область действия которых может быть задана операциями. Эти операции позволяют автору ПЗ/ЗБ указать действия, общие для пользователей/субъектов, которым необходимо противодействовать с использованием ФБО. Возможный пример отображения анонимности: «ФБО должны обеспечивать, чтобы пользователи и/или субъекты были не способны определить идентификатор пользователя, обратившегося за телеконсультацией».

Необходимо, чтобы ФБО предоставляли защиту от действий не только отдельных пользователей, но и пользователей, объединившихся для получения определенной информации. Стойкость защиты, предоставляемой этим классом, следует описать как стойкость функции в соответствии с ИСО/МЭК 15408-1, приложения А и В.

Декомпозиция класса FPR «Приватность» на составляющие его компоненты показана на рисунке I.1.

I.1 Анонимность (FPR_ANO)

I.1.1 Замечания для пользователя

Семейство FPR_ANO обеспечивает возможность использования субъектом ресурсов или услуг без раскрытия идентификатора его пользователя.

Данное семейство предназначено для определения того, что пользователь или субъект сможет предпринимать действия, не раскрывая идентификатора пользователя другим пользователям, субъектам или объектам. Это семейство предоставляет автору ПЗ/ЗБ способ идентификации совокупности пользователей, которые не смогут узнать идентификатор исполнителя некоторых действий.

Следовательно, если субъект, пользуясь анонимностью, выполняет некоторое действие, другой субъект будет не в состоянии определить ни идентификатор, ни даже ссылку на идентификатор пользователя, использовавшего первый субъект. Анонимность сфокусирована на защите идентификатора пользователя, а не на защите идентификатора субъекта. Поэтому идентификатор субъекта не защищен от раскрытия.

Хотя идентификатор пользователя не разглашается другим субъектам или пользователям, ФБО прямо не запрещено узнавать идентификатор пользователя. Если не допускается, чтобы ФБО был известен идентификатор пользователя, то можно прибегнуть к компоненту FPR_ANO.2 «Анонимность». В этом случае ФБО не разрешается запрашивать информацию о пользователе.

Термин «определить» следует понимать в самом широком смысле слова. Для конкретизации требований к строгости автор ПЗ/ЗБ может воспользоваться понятием стойкости функций.

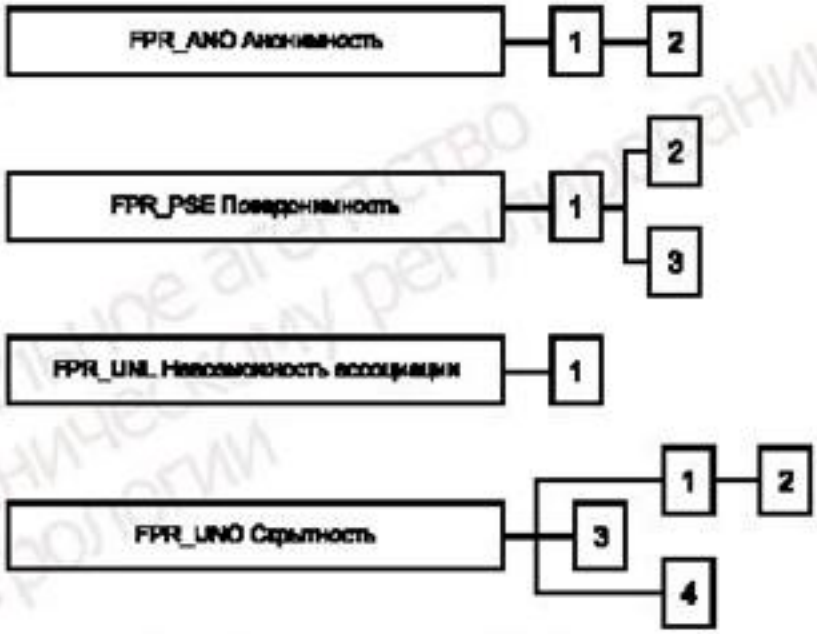

Рисунок I.1 — Декомпозиция класса FPR «Приватность»

В этом компоненте проводится различие между пользователями и уполномоченными пользователями. Уполномоченный пользователь часто не упоминается в компонентах и тогда ему не запрещается знать идентификатор пользователя. Однако нет и явного требования, чтобы уполномоченный пользователь обязательно имел возможность определить идентификатор пользователя. Для достижения максимальной приватности в компоненте необходимо указать, что ни пользователь, ни уполномоченный пользователь не смогут узнать чей-либо идентификатор при выполнении какого-либо действия.

В то время как некоторые системы обеспечат анонимность всех предоставляемых услуг, в других системах она предоставляется только для некоторых субъектов/операций. Для необходимой гибкости включена операция, в которой задается область действия требования. Если автор ПЗ/ЗБ захочет охватить все субъекты/операции, можно воспользоваться выражением «все субъекты и операции».

Возможные применения анонимности включают в себя запросы конфиденциального характера к общедоступным базам данных, ответы на опросы, проводимые через телекоммуникации, или осуществление анонимных выплат или пожертвований.

Примерами потенциально враждебных пользователей или субъектов являются провайдеры, системные операторы, абоненты связи и пользователи, скрытно вводящие в систему опасные элементы (например, «троянских коней»). Все они могут изучать образ действия пользователей (например, какие пользователи какие услуги заказывают) и злоупотреблять этой информацией.

I.1.2 FPR_ANO.1 Анонимность

I.1.2.1 Замечания по применению для пользователя

Компонент FPR_ANO.1 обеспечивает, чтобы идентификатор пользователя был защищен от раскрытия. Однако в некоторых случаях уполномоченный пользователь может определять, кто произвел определенные действия. Этот компонент дает возможность гибкого подхода, позволяя выбирать политику как ограниченной, так и полной приватности.

I.1.2.2 Операции

I.1.2.2.1 Назначение

В FPR_ANO.1.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, от которых ФБО необходимо предоставить защиту. Например, даже если автор ПЗ/ЗБ специфицирует единственную роль пользователя или субъекта, ФБО необходимо предоставить защиту не только от отдельного пользователя или субъекта, но и от совместно действующих пользователей и/или субъектов. Например, совокупность пользователей может являться группой пользователей, выступающих в одной и той же роли или использующих одни и те же процессы.

В FPR_ANO.1.1 автору ПЗ/ЗБ следует идентифицировать список субъектов и/или операций, и/или объектов, для которых подлинное имя пользователя данного субъекта следует защитить, например «голосование».

I.1.3 FPR_ANO.2 Анонимность без запроса информации

I.1.3.1 Замечания по применению для пользователя

Компонент FPR_ANO.2 используется для обеспечения того, что ФБО не будет разрешено знать идентификатор пользователя.

I.1.3.2 Операции

I.1.3.2.1 Назначение

В FPR_ANO.2.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, от которых ФБО необходимо предоставить защиту. Например, даже если автор ПЗ/ЗБ специфицирует единственную роль пользователя или субъекта, ФБО необходимо предоставить защиту не только от отдельного пользователя или субъекта, но и от совместно действующих пользователей и/или субъектов. Совокупность пользователей, например, может являться группой пользователей, выступающих в одной и той же роли или использующих одни и те же процессы.

В FPR_ANO.2.1 автору ПЗ/ЗБ следует идентифицировать список субъектов и/или операций, и/или объектов, для которых подлинное имя пользователя данного субъекта следует защитить, например «голосование».

В FPR_ANO.2.2 автору ПЗ/ЗБ следует идентифицировать список услуг, на которые распространяется требование анонимности, например «доступ к описанию работ».

В FPR_ANO.2.2 автору ПЗ/ЗБ следует идентифицировать список субъектов, для которых подлинные имена пользователей необходимо защитить при предоставлении специфицированных услуг.

I.2 Псевдонимность (FPR_PSE)

I.2.1 Замечания для пользователя

Семейство FPR_PSE обеспечивает, чтобы пользователь мог использовать ресурс или услугу без раскрытия своего идентификатора, оставаясь в то же время ответственным за это использование. Пользователь может быть ответственным, будучи прямо связан со ссылкой (псевдонимом), предоставляемой ФБО, или с псевдонимом, таким как номер банковского счета, используемым для целей обслуживания.

В некотором отношении псевдонимность походит на анонимность. В обоих случаях защищается идентификатор пользователя, но в псевдонимности поддерживается ссылка на идентификатор пользователя как для сохранения его ответственности, так и для других целей.

Компонент FPR_PSE.1 «Псевдонимность» не специфицирует требований, относящихся к ссылке на идентификатор пользователя. Эти требования имеются в компонентах FPR_PSE.2 «Обратимая псевдонимность» и FPR_PSE.3 «Альтернативная псевдонимность».

Одним из путей использования этой ссылки является возможность получения первоначального идентификатора пользователя. Например, если компьютеризованная касса несколько раз выдает абсолютно одинаковые чеки (то есть происходит мошенничество), было бы предпочтительно иметь возможность отследить идентификатор пользователя. В общем случае необходимость восстановления идентификаторов пользователей определяется конкретными условиями. Для описания такой услуги автору ПЗ/ЗБ можно воспользоваться компонентом FPR_PSE.2 «Обратимая псевдонимность».

Ссылка может также использоваться в качестве псевдонима пользователя. Например, пользователь, не желающий быть идентифицированным, может предоставить номер счета, с которого следует оплачивать использование ресурсов. В таком случае ссылка на идентификатор пользователя - это его псевдоним, который другие пользователи или субъекты могут использовать для выполнения своих функций, без получения при любых обстоятельствах идентификатора пользователя (например, при сборе статистических данных использования системы). В этом случае для определения правил, которым ссылки должны удовлетворять, автор ПЗ/ЗБ может воспользоваться компонентом FPR_PSE.3 «Альтернативная псевдонимность».

Применяя упомянутые выше конструкции, с помощью FPR_PSE.2 можно ввести электронные деньги, установив требование защиты идентификатора пользователя от наблюдения при условии, что одна и та же электронная сумма не тратится дважды. В последнем случае идентификатор пользователя будет отслеживаться. Следовательно, если пользователь ведет себя честно, его идентификатор защищен, если же он пытается мошенничать, его идентификатор может быть отслежен.

Другим видом системы электронных платежей являются электронные кредитные карточки, с помощью которых пользователь предоставляет псевдоним, указывающий на счет, с которого могут быть сняты деньги. В подобном случае можно использовать, например компонент FPR_PSE.3, определив, что идентификатор пользователя будет защищен и пользователь получит требуемую сумму, только если на его счете есть деньги (если так оговорено в условиях).

Следует иметь в виду, что наиболее строгие компоненты данного семейства могут потенциально не сочетаться с другими возможными требованиями, такими как идентификация и аутентификация или аудит. Выражение «определить идентификатор» следует понимать в широком смысле, а именно: ФБО не предоставляют информацию при выполнении операции; нельзя определить создателя субъекта или владельца субъекта, вызвавшего операцию; ФБО не будут записывать такую информацию, доступную пользователям или субъектам, по которой в дальнейшем можно бы было узнать идентификатор пользователя.

Смысл заключается в том, чтобы ФБО не раскрывали без необходимости любую информацию, с помощью которой можно определить идентификатор пользователя, например идентификаторы субъектов, действующих от имени пользователя. Степень сохранности этой информации зависит от усилий, которые потребуются нарушителю для ее раскрытия. Следовательно, в компонентах семейства FPR_PSE «Псевдонимность» необходимо учитывать требования стойкости функций.

Возможные применения включают в себя оплату телефонных услуг по льготному тарифу без раскрытия идентификатора абонента или оплату анонимного использования системы электронных платежей.

Примерами потенциально враждебных пользователей являются провайдеры, системные операторы, абоненты связи и пользователи, скрытно вводящие в систему опасные элементы (например «троянские кони»). Все эти нарушители могут изучать, какие пользователи какие услуги заказывают, и злоупотреблять этой информацией. В дополнение к семейству «Анонимность» услуги, предоставляемые семейством «Псевдонимность», содержат методы авторизации без идентификации, особенно при анонимной оплате («электронные деньги»). Это помогает провайдерам получать платежи безопасным способом, поддерживая при этом анонимность клиентов.

I.2.2 FPR_PSE.1 Псевдонимность

I.2.2.1 Замечания по применению для пользователя

Компонент FPR_PSE.1 обеспечивает защиту пользователя от раскрытия его идентификатора другими пользователями. При этом пользователь останется ответственным за свои действия.

I.2.2.2 Операции

I.2.2.2.1 Назначение

В FPR_PSE.1.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, от которых ФБО необходимо предоставить защиту. Например, даже если автор ПЗ/ЗБ специфицирует единственную роль пользователя или субъекта, ФБО необходимо предоставить защиту не только от отдельного пользователя или субъекта, но и от совместно действующих пользователей и/или субъектов. Например, совокупность пользователей может являться группой пользователей, выступающих в одной и той же роли или использующих одни и те же процессы.

В FPR_PSE.1.1 автору ПЗ/ЗБ следует идентифицировать список субъектов и/или операций, и/или объектов, для которых подлинное имя пользователя данного субъекта следует защитить, например, «доступ к предложениям трудоустройства». Следует отметить, что к «объектам» относят любые атрибуты, позволяющие другим пользователям или субъектам раскрыть действительный идентификатор данного пользователя.

В FPR_PSE.1.2 автору ПЗ/ЗБ следует идентифицировать число псевдонимов (один или более), которое ФБО способны предоставить.

В FPR_PSE.1.2 автору ПЗ/ЗБ следует идентифицировать список субъектов, которым ФБО способны предоставлять псевдонимы.

I.2.2.2.2 Выбор

В FPR_PSE.1.3 автору ПЗ/ЗБ следует специфицировать, создаются псевдонимы функциями безопасности ОО или выбираются самими пользователями. Может быть выбран только один из этих вариантов.

I.2.2.2.3 Назначение

В FPR_PSE.1.3 автору ПЗ/ЗБ следует идентифицировать метрику, которой удовлетворял бы псевдоним, созданный ФБО или выбранный пользователем.

I.2.3 FPR_PSE.2 Обратимая псевдонимность

I.2.3.1 Замечания по применению для пользователя

В компоненте FPR_PSE.2 ФБО должны обеспечить, чтобы при специфицированных условиях по предоставленной ссылке мог быть определен идентификатор пользователя.

В этом компоненте ФБО должны вместо идентификатора пользователя предоставить его псевдоним. При удовлетворении специфицированных условий идентификатор пользователя, которому принадлежит псевдоним, может быть определен. Для электронных денег примером таких условий может служить: «ФБО должны предоставить нотариусу возможность определить идентификатор пользователя по представленному псевдониму только в том случае, если чек был выдан дважды».

I.2.3.2 Операции

I.2.3.2.1 Назначение

В FPR_PSE.2.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, от которых ФБО необходимо предоставить защиту. Например, даже если автор ПЗ/ЗБ специфицирует единственную роль пользователя или субъекта, ФБО необходимо предоставить защиту не только от отдельного пользователя или субъекта, но и от совместно действующих пользователей и/или субъектов. Например, совокупность пользователей может являться группой пользователей, выступающих в одной и той же роли или использующих одни и те же процессы.

В FPR_PSE.2.1 автору ПЗ/ЗБ следует идентифицировать список субъектов и/или операций, и/или объектов, для которых подлинное имя пользователя данного субъекта следует защитить, например «доступ к предложениям трудоустройства». Отметим, что к «объектам» относят любые атрибуты, позволяющие другим пользователям или субъектам раскрыть действительный идентификатор данного пользователя.

В FPR_PSE.2.2 автору ПЗ/ЗБ следует идентифицировать число псевдонимов (один или более), которое ФБО способны предоставить.

В FPR_PSE.2.2 автору ПЗ/ЗБ следует идентифицировать список субъектов, которым ФБО способны предоставлять псевдонимы.

I.2.3.2.2 Выбор

В FPR_PSE.2.3 автору ПЗ/ЗБ следует специфицировать, создаются псевдонимы функциями безопасности ОО или выбираются самими пользователями. Может быть выбран только один из этих вариантов.

I.2.3.2.3 Назначение

В FPR_PSE.2.3 автору ПЗ/ЗБ следует идентифицировать метрику, которой удовлетворял бы псевдоним, созданный ФБО или выбранный пользователем.

I.2.3.2.4 Выбор

В FPR_PSE.2.4 автору ПЗ/ЗБ следует идентифицировать, могут ли уполномоченный пользователь и/или доверенные субъекты определить подлинное имя пользователя.

I.2.3.2.5 Назначение

В FPR_PSE.2.4 автору ПЗ/ЗБ следует идентифицировать список условий, при которых доверенные субъекты и уполномоченный пользователь могут определить подлинное имя пользователя на основе предоставленной ссылки. Такими условиями может быть «время суток» или же правовое условие, например, предъявление судебного постановления.

В FPR_PSE.2.4 автору ПЗ/ЗБ следует идентифицировать список доверенных субъектов (например «нотариус» или «пользователь, имеющий специальное разрешение»), которые могут при определенных условиях узнать подлинное имя пользователя.

I.2.4 FPR_PSE.3 Альтернативная псевдонимность

I.2.4.1 Замечания по применению для пользователя

В компоненте FPR_PSE.3 ФБО должны обеспечить, чтобы предоставленная ссылка отвечала определенным правилам ее создания и вследствие этого могла использоваться потенциально опасными субъектами без нарушения безопасности.

Если пользователь хочет использовать ресурсы, не раскрывая свой идентификатор, то может применяться псевдонимность. Однако на всем протяжении доступа к системе пользователь обязан использовать один и тот же псевдоним. Такое условие можно специфицировать в этом компоненте.

I.2.4.2 Операции

I.2.4.2.1 Назначение

В FPR_PSE.3.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, от которых ФБО необходимо предоставить защиту. Например, даже если автор ПЗ/ЗБ специфицирует единственную роль пользователя или субъекта, ФБО необходимо предоставить защиту не только от отдельного пользователя или субъекта, но и от совместно действующих пользователей и/или субъектов. Например, совокупность пользователей может являться группой пользователей, выступающих в одной и той же роли или использующих один и тот же процесс.

В FPR_PSE.3.1 автору ПЗ/ЗБ следует идентифицировать список субъектов и/или операций, и/или объектов, для которых подлинное имя пользователя данного субъекта следует защитить, например «доступ к предложениям трудоустройства». Отметим, что к «объектам» относят любые атрибуты, позволяющие другим пользователям или субъектам раскрыть действительный идентификатор данного пользователя.

В FPR_PSE.3.2 автору ПЗ/ЗБ следует идентифицировать число псевдонимов (один или более), которое ФБО способны предоставить.

В FPR_PSE.3.2 автору ПЗ/ЗБ следует идентифицировать список субъектов, которым ФБО способны предоставлять псевдонимы.

I.2.4.2.2 Выбор

В FPR_PSE.3.3 автору ПЗ/ЗБ следует специфицировать, создаются псевдонимы функциями безопасности ОО или выбираются самими пользователями. Может быть выбран только один из этих вариантов.

I.2.4.2.3 Назначение

В FPR_PSE.3.3 автору ПЗ/ЗБ следует идентифицировать метрику, которой удовлетворял бы псевдоним, созданный ФБО или выбранный пользователем.

FPR_PSE.3.4 автору ПЗ/ЗБ следует идентифицировать список условий, указывающих, в каких случаях ссылки на подлинное имя пользователя должны быть одинаковы, а в каких должны быть различными, например, «если пользователь осуществляет многократный вход в узел сети, он будет использовать один и тот же псевдоним».

I.3 Невозможность ассоциации (FPR_UNL)

I.3.1 Замечания для пользователя

Семейство FPR_UNL обеспечивает, чтобы пользователь мог неоднократно использовать ресурсы или услуги, не давая никому возможности связать вместе их использование. Невозможность ассоциации отличается от псевдонимности тем, что хотя при псевдонимности сам пользователь также неизвестен, связи между его различными действиями не скрываются.

Требования невозможности ассоциации предназначены для защиты идентификатора пользователя от применения профиля операций. Например, телефонная компания может определить поведение пользователя телефонной карты, используемой с единственного номера. Если известны профили использования телефона группой пользователей, то карту можно связать с конкретным пользователем. Сокрытие связи между различными обращениями за услугой или за доступом к ресурсу предотвратит накопление подобной информации.

В результате, требования невозможности ассоциации могут означать защиту идентификатора субъекта и пользователя для некоторой операции. В противном случае эта информация может быть использована для связывания операций.

Семейство содержит требование исключить установление связи между различными операциями. Эта связь может приобретать различные формы. Например, с пользователем ассоциируется операция или терминал, с которого инициировано действие, или продолжительность выполнения действия. Автор ПЗ/ЗБ может специфицировать, раскрытию какого типа связей необходимо противодействовать.

Возможные приложения включают в себя возможность многократного использования псевдонима, исключающие создание шаблона использования, по которому можно раскрыть идентификатор пользователя.

Примерами потенциально враждебных субъектов или пользователей являются провайдеры, системные операторы, абоненты связи и пользователи, скрытно вводящие в систему опасные элементы (например «троянские кони»). Сами они не выполняют операции в системе, но стремятся получить информацию об операциях. Все эти нарушители могут изучать образ действий пользователей (например, какие пользователи какие услуги заказывают) и злоупотреблять этой информацией. Невозможность ассоциации защищает пользователей от сопоставления, которое может быть проведено между различными действиями потребителя. Например, серия телефонных вызовов, сделанных анонимным потребителем по различным номерам, может дать информацию для раскрытия его идентификатора по сочетанию номеров.

I.3.2 FPR_UNL.1 Невозможность ассоциации

I.3.2.1 Замечания по применению для пользователя

Компонент FPR_UNL.1 обеспечивает, чтобы пользователи не могли связывать между собой различные операции в системе и таким образом получать информацию.

I.3.2.2 Операции

I.3.2.2.1 Назначение

В FPR_UNL.1.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, от которых ФБО необходимо предоставить защиту. Например, даже если автор ПЗ/ЗБ специфицирует единственную роль пользователя или субъекта, ФБО необходимо предоставить защиту не только от отдельного пользователя или субъекта, но и от совместно действующих пользователей и/или субъектов. Например, совокупность пользователей может являться группой пользователей, выступающих в одной и той же роли или использующих один и тот же процесс.

В FPR_UNL.1.1 автору ПЗ/ЗБ следует идентифицировать список операций, на которые следует распространить требование невозможности ассоциации, например «отправка электронной почты».

I.3.2.2.2 Выбор

В FPR_UNL.1.1 автору ПЗ/ЗБ следует выбрать взаимосвязи, которые следует скрыть. Этот выбор позволяет специфицировать идентификатор пользователя либо операцию назначения списка соотношений.

I.3.2.2.3 Назначение

В FPR_UNL.1.1 автору ПЗ/ЗБ следует идентифицировать список соотношений, которые следует защищать, например «посланные с одного и того же терминала».

I.4 Скрытность (FPR_UNO)

I.4.1 Замечания для пользователя

Семейство FPR_UNO обеспечивает, чтобы пользователь мог использовать ресурс или услугу без предоставления кому-либо, в особенности третьей стороне, возможности знать об использовании ресурса или услуги.

Подход к защите идентификатора пользователя в этом семействе отличает его от остальных семейств данного класса. Скрывается факт использования ресурса или услуги, а не идентификатор пользователя.

Для реализации скрытности могут быть применены различные методы. Примеры некоторых из них:

a) размещение информации, влияющее на скрытность. Информацию, которую необходимо скрыть (например, указывающую на выполнение операции), можно разместить в ОО различными способами. Место ее размещения в ОО можно выбирать случайно, чтобы нарушитель не знал, какую именно часть ОО следует атаковать. Данную информацию можно распределить так, чтобы ни в одной части ОО ее не было достаточно для нарушения приватности пользователя. Этот способ рассматривается в компоненте FPR_UNO.2 «Распределение информации, влияющее на скрытность»;

b) массовое распространение информации (по локальной сети, по радио). Пользователи не могут определить, кто конкретно получил и использовал данную информацию. Этот метод особенно полезен в случае, если информацию следует довести до того, кто опасается показывать свою заинтересованность в данной информации (например, чувствительной медицинской информации);

c) криптографическая защита и дополнение сообщений незначащей информацией. Путем наблюдения за потоком сообщений можно извлечь информацию из самого факта передачи сообщения и его атрибутов. Защиту передаваемых сообщений и их атрибутов можно обеспечить посредством дополнения трафика и самих сообщений незначащей информацией или шифрования.

Иногда пользователей не следует допускать к наблюдению за использованием ресурсов, а уполномоченным пользователям такое наблюдение необходимо для исполнения своих обязанностей. В этом случае может применяться компонент FPR_UNO.4 «Открытость для уполномоченного пользователя», который предоставляет эту возможность одному или нескольким уполномоченным пользователям.

В данном семействе используется понятие «часть ОО». Под ней подразумевается какая-либо часть ОО, отделенная физически или логически от других частей ОО. В случае логического отделения может быть уместно применение семейства FPT_SEP «Разделение домена».

Скрытность связей может быть важным фактором во многих областях, таких как осуществление конституционных прав, политика организации или приложения, связанные с оборонными вопросами.

I.4.2 FPR_UNO.1 Скрытность

I.4.2.1 Замечания по применению для пользователя

Компонент FPR_UNO.1 содержит требования недопустимости наблюдения неуполномоченными пользователями за использованием услуги или ресурса. Дополнительно к этому компоненту автору ПЗ/ЗБ может потребоваться «Анализ скрытых каналов».

I.4.2.2 Операции

I.4.2.2.1 Назначение

В FPR_UNO.1.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, от которых ФБО необходимо предоставить защиту. Например, даже если автор ПЗ/ЗБ специфицирует единственную роль пользователя или субъекта, ФБО необходимо предоставить защиту не только от отдельного пользователя или субъекта, но и от совместно действующих пользователей и/или субъектов. Например, совокупность пользователей может являться группой пользователей, выступающих в одной и той же роли или использующих одни и те же процессы.

В FPR_UNO.1.1 автору ПЗ/ЗБ следует идентифицировать список операций, на которые распространяется требование скрытности. Тогда другие пользователи/субъекты не смогут наблюдать за указанными в списке операциями над специфицированными ниже объектами (например, за чтением и записью на объекте).

В FPR_UNO.1.1 автору ПЗ/ЗБ следует идентифицировать список объектов, на которые распространяется требование скрытности. Примером может быть конкретный сервер электронной почты или FTP-сайт.

В FPR_UNO.1.1 автору ПЗ/ЗБ следует специфицировать совокупность защищаемых пользователей и/или субъектов, скрытность информации которых будет обеспечиваться. Примером может быть: «пользователи, получившие доступ к системе через Интернет».

I.4.3 FPR_UNO.2 Распределение информации, влияющее на скрытность

I.4.3.1 Замечания по применению для пользователя

Компонент FPR_UNO.2 содержит требования недопустимости наблюдения определенными пользователями за использованием услуги или ресурса. Кроме того, в нем определяется, какая информация, связанная с приватностью пользователя, распределяется в ОО так, чтобы нарушитель не мог установить, в какой именно части ОО она содержится, или был вынужден атаковать несколько частей ОО.

Примером использования этого компонента является случайный выбор узла для предоставления услуги. В этом случае в компоненте может быть установлено требование, что информация, связанная с приватностью пользователя, должна быть доступна только в одной идентифицированной части ОО, не распространяясь за ее пределы.

Более сложный пример связан с некоторыми «алгоритмами голосования». В предоставлении услуги принимают участие несколько частей ОО, но никакая отдельная часть ОО не сможет нарушить принятую политику. Какое-либо лицо может принять (или не принять) участие в голосовании; при этом невозможно без использования ОО определить результат голосования и его участие в голосовании (если голосование не было единогласным).

В дополнение к этому компоненту автору ПЗ/ЗБ может потребоваться «Анализ скрытых каналов».

I.4.3.2 Операции

I.4.3.2.1 Назначение

В FPR_UNO.2.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, от которых ФБО необходимо предоставить защиту. Например, даже если автор ПЗ/ЗБ специфицирует единственную роль пользователя или субъекта, ФБО необходимо предоставить защиту не только от отдельного пользователя или субъекта, но и от совместно действующих пользователей и/или субъектов. Например, совокупность пользователей может являться группой пользователей, выступающих в одной и той же роли или использующих одни и те же процессы.

В FPR_UNO.2.1 автору ПЗ/ЗБ следует идентифицировать список операций, на которые распространяется требование скрытности. Тогда другие пользователи/субъекты не смогут наблюдать за операциями над объектом из специфицированного списка (например, за чтением и записью).

В FPR_UNO.2.1 автору ПЗ/ЗБ следует идентифицировать список объектов, на которые распространяется требование скрытности. Примером может быть конкретный сервер электронной почты или FTP-сайт.

В FPR_UNO.2.1 автору ПЗ/ЗБ следует специфицировать совокупность пользователей и/или субъектов, скрытность информации которых будет обеспечиваться, например «пользователи, получившие доступ к системе через Интернет».

В FPR_UNO.2.2 автору ПЗ/ЗБ следует идентифицировать, распределение какой информации, связанной с приватностью, следует контролировать. Примером такой информации являются IP-адрес субъекта, IP-адрес объекта, время, используемые криптографические ключи.

В FPR_UNO.2.2 автору ПЗ/ЗБ следует специфицировать условия распространения указанной информации. Эти условия следует поддерживать все время существования приватной информации пользователя в каждом случае. Примерами таких условий могут быть следующие: «информация должна быть представлена только в

одной из разделенных частей ОО и не должна передаваться за ее пределы»; «информация должна пребывать только в одной из разделенных частей ОО, но должна передаваться в другие его части периодически»; «информация должна распределяться между различными частями ОО так, чтобы нарушение защиты любых пяти отдельных частей ОО не приводило к нарушению политики безопасности в целом».

I.4.4 FPR_UNO.3 Скрытность без запроса информации

I.4.4.1 Замечания по применению для пользователя

Компонент FPR_UNO.3 применяется для требования, чтобы ФБО не стремились получить информацию, которая может нарушить скрытность при предоставлении определенных услуг. Поэтому ФБО не будут запрашивать (то есть стремиться получить из других источников) информацию, которая может быть использована для нарушения скрытности.

I.4.4.2 Операции

I.4.4.2.1 Назначение

В FPR_UNO.3.1 автору ПЗ/ЗБ следует идентифицировать список услуг, на которые распространяется требование скрытности, например «доступ к описанию работ».

В FPR_UNO.3.1 автору ПЗ/ЗБ следует идентифицировать список субъектов, от которых при получении специфицированных услуг следует защищать информацию, связанную с приватностью.

В FPR_UNO.3.1 автору ПЗ/ЗБ следует специфицировать информацию, связанную с приватностью, которая будет защищена от специфицированных субъектов. Это может быть идентификатор субъекта, получающего услугу, или характеристики полученной услуги, например использованный ресурс памяти.

I.4.5 FPR_UNO.4 Открытость для уполномоченного пользователя

I.4.5.1 Замечания по применению для пользователя

Компонент FPR_UNO.4 применяется для предоставления права наблюдения за использованием ресурсов одному или нескольким уполномоченным пользователям. Без этого компонента возможность наблюдения допускается, но не является обязательной.

I.4.5.2 Операции

I.4.5.2.1 Назначение

В FPR_UNO.4.1 автору ПЗ/ЗБ следует специфицировать совокупность уполномоченных пользователей, которым ФБО необходимо предоставить возможность наблюдения за использованием ресурсов. Это может быть, например группа уполномоченных пользователей, исполняющих одну и ту же роль или использующих одни и те же процессы.

В FPR_UNO.4.1 автору ПЗ/ЗБ следует специфицировать список ресурсов и/или услуг, возможность наблюдения за которыми необходима уполномоченному пользователю.

Федеральное агентство по техническому регулированию и метрологии

Приложение J
(обязательное)

Защита ФБО (FPT)

Класс FPT содержит семейства функциональных требований, которые связаны с целостностью и управлением механизмами, реализованными в ФБО, не завися при этом от особенностей ПБО, а также с целостностью данных ФБО, не завися от специфического содержания данных ПБО. В некотором смысле, компоненты семейств этого класса дублируют компоненты из класса FDP «Защита данных пользователя» и могут даже использовать одни и те же механизмы. Однако класс FDP «Защита данных пользователя» нацелен на защиту данных пользователя, в то время как класс FPT «Защита ФБО» — на защиту данных ФБО. Фактически, компоненты из класса FPT «Защита ФБО» необходимы для реализации требований невозможности нарушения и обхода политик ФБ данного ОО.

В рамках данного класса выделяются три важные составные части ФБО:

1) абстрактная машина ФБО, то есть виртуальная или физическая машина, на которой выполняется оцениваемая реализация ФБО;

2) реализация ФБО, которая выполняется на абстрактной машине и реализует механизмы, осуществляющие ПБО;

3) данные ФБО, которые являются административными базами данных, управляющими осуществлением ПБО.

Все семейства в классе FPT «Защита ФБО» можно связать с этими тремя частями и сгруппировать следующим образом:

a) FPT_PHP «Физическая защита ФБО» предоставляет уполномоченному пользователю возможность обнаружения внешних атак на те части ОО, которые реализуют ФБО;

b) FPT_AMT «Тестирование базовой абстрактной машины» и FPT_TST «Самотестирование ФБО» предоставляют уполномоченному пользователю возможность верифицировать правильность операций базовой абстрактной машины и ФБО, а также целостность данных и выполняемого кода ФБО;

c) FPT_SEP «Разделение домена» и FPT_RVM «Посредничество при обращениях» защищают ФБО во время их выполнения и обеспечивают невозможность обхода ФБО. Если соответствующие компоненты этих семейств сочетаются с соответствующими компонентами семейства ADV_INT «Внутренняя структура ФБО», можно говорить о наличии в ОО традиционного «монитора обращений»;

d) FPT_RCV «Надежное восстановление», FPT_FLS «Безопасность при сбое» и FPT_TRC «Согласованность данных ФБО при дублировании в пределах ОО» определяют режим выполнения ФБО при возникновении сбоя и непосредственно после него;

e) FPT_ITA «Доступность экспортируемых данных ФБО», FPT_ITC «Конфиденциальность экспортируемых данных ФБО» и FPT_ITI «Целостность экспортируемых данных ФБО» определяют защиту и доступность данных ФБО при их обмене между ФБО и удаленным доверенным продуктом ИТ;

f) FPT_ITT «Передача данных ФБО в пределах ОО» предназначено для защиты данных ФБО при их передаче между физически разделенными частями ОО;

g) FPT_RPL «Обнаружение повторного использования» содержит требование защиты от повторного использования различных типов информации и/или операций;

h) FPT_SSP «Протокол синхронизации состояний» определяет синхронизацию состояний между различными частями распределенных ФБО на основе данных ФБО;

i) FPT_STM «Метки времени» предоставляет надежные метки времени;

j) FPT_TDC «Согласованность данных ФБО между ФБО» предназначено для согласования данных между ФБО и удаленным доверенным продуктом ИТ.

Декомпозиция класса FPT «Защита ФБО» на составляющие его компоненты показана на рисунке J.1.

J.1 Тестирование базовой абстрактной машины (FPT_AMT)

J.1.1 Замечания для пользователя

Семейство FPT_AMT определяет требования к выполнению тестирования функциями безопасности ОО предположений безопасности, сделанных относительно базовой абстрактной машины, на которую полагаются ФБО. Данная «абстрактная» машина может быть как платформой аппаратных/программно-аппаратных средств, так и некоторым известным и прошедшим оценку сочетанием аппаратных/программных средств, действующим как виртуальная машина. В качестве примеров такого тестирования можно указать проверку аппаратной защиты, посылку типовых пакетов по сети для проверки получения, верификацию режима функционирования виртуального машинного интерфейса и т. д. Эти тесты могут выполняться при некотором поддерживаемом состоянии, при запуске, по запросу или постоянно. Действия, предпринимаемые с использованием ОО по результатам тестирования, определены в FPT_RCV «Надежное восстановление».

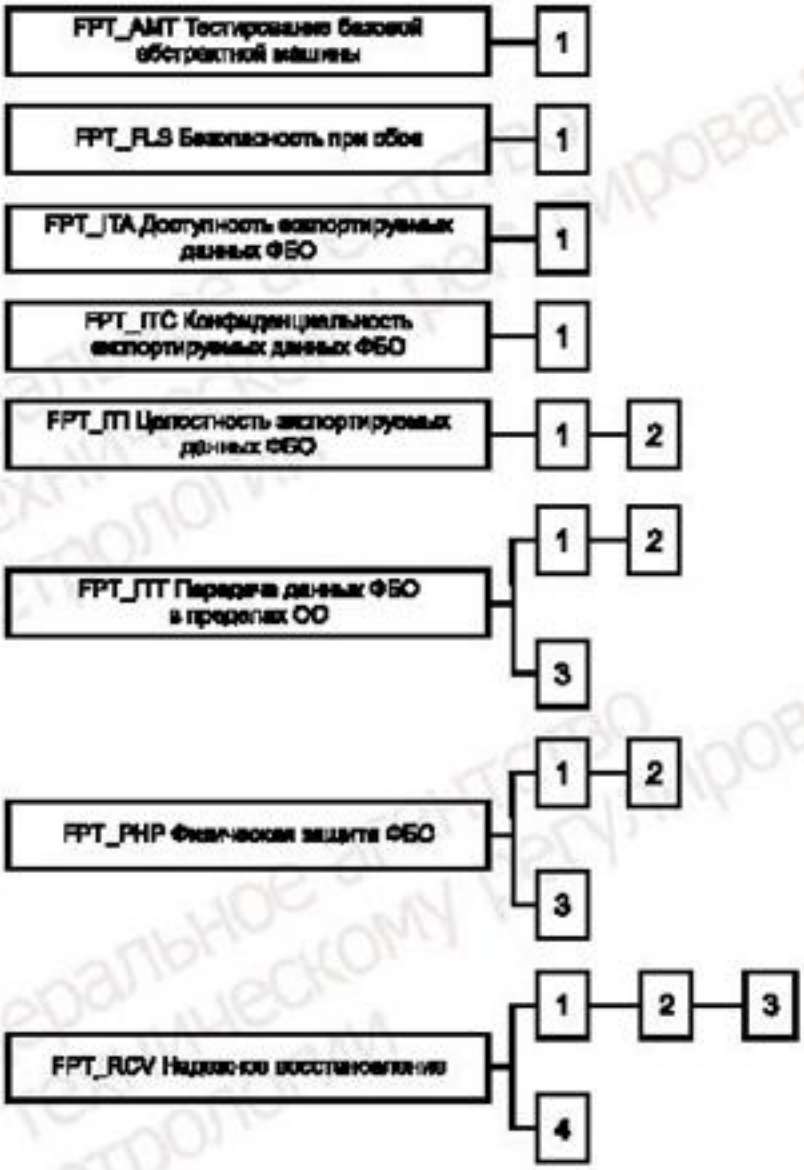

Рисунок J.1 — Декомпозиция класса FPT «Защита ФБО», лист 1

Термин «базовая абстрактная машина» относится главным образом к аппаратным компонентам, на базе которых выполняются ФБО. Однако его можно отнести и к предварительно оцененной базовой комбинации аппаратных средств и программного обеспечения, ведущей себя как виртуальная машина, на которую полагаются ФБО.

Тесты абстрактной машины могут иметь различные формы:

a) тесты при включении, которые проверяют правильность работы платформы. Для аппаратных и программно-аппаратных средств они могут включать в себя тесты таких элементов, как платы памяти, маршруты передачи данных, шины, управляющие элементы, регистры процессора, порты сообщений, интерфейсы консолей, звуковоспроизводящие и периферийные устройства. Для программных элементов (виртуальной машины) они включат в себя верификацию корректности инициализации и режима функционирования;

b) загружаемые тесты, которые могут загружаться и выполняться уполномоченным пользователем или активизироваться при определенных условиях. Они могут включать в себя тесты нагрузки элементов процессора (логических элементов, вычислительных элементов и т. д.) и управляемой памяти.

J.1.2 Замечания для оценщика

Необходимо, чтобы тесты базовой абстрактной машины были достаточны для проверки всех характеристик базовой абстрактной машины, на которой выполняются ФБО.

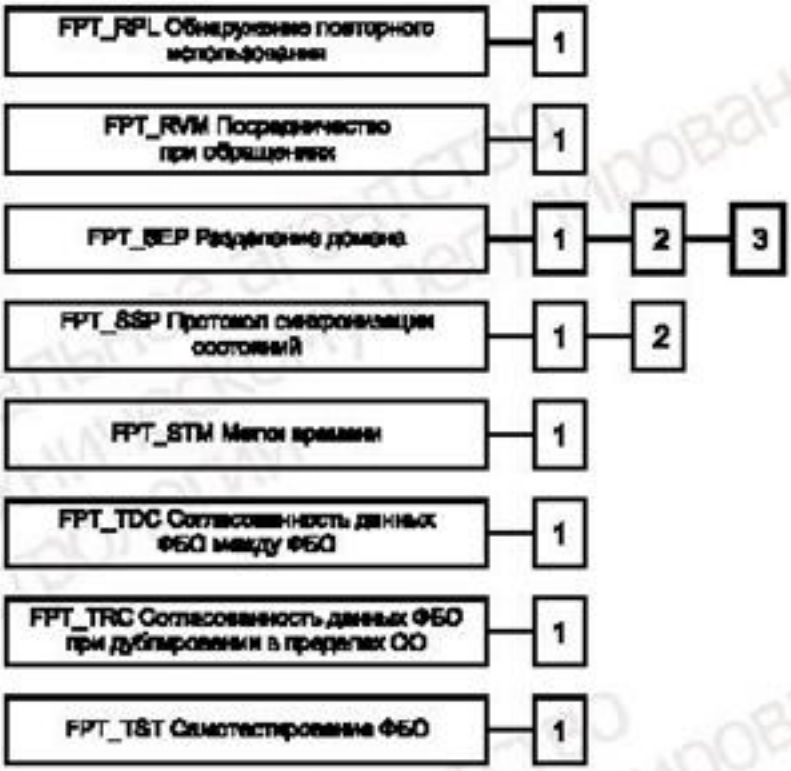

Рисунок J.1, лист 2

J.1.3 FPT_AMT.1 Тестирование абстрактной машины

J.1.3.1 Замечания по применению для пользователя

Компонент FPT_AMT.1 поддерживает периодическое тестирование предположений безопасности базовой абстрактной машины, от которых зависит выполнение ФБО, требуя обеспечения возможности периодического запуска тестирования функций.

При желании автор ПЗ/ЗБ может уточнить требование, указав, в каком режиме следует проводить тестирование: автономно, при обычном функционировании системы или в режиме аварийной поддержки.

J.1.3.2 Замечания для оценщика

Допускается, чтобы функции периодического тестирования были доступны только в автономном режиме или режиме аварийной поддержки. Следует иметь средства управления для предоставления доступа в режиме аварийной поддержки только уполномоченным пользователям.

J.1.3.3 Операции

J.1.3.3.1 Выбор

В FPT_AMT.1.1 автору ПЗ/ЗБ следует специфицировать, когда ФБО будут выполнять тестирование абстрактной машины: при запуске, периодически во время нормального функционирования, по запросу уполномоченного пользователя, при других условиях. В последнем случае следует уточнить эти условия. С помощью этой операции выбора автор ПЗ/ЗБ имеет возможность указать также периодичность выполнения самотестирования. Более частое тестирование даст пользователю большую уверенность в правильном функционировании ОО. Однако необходимо выбрать правильное соотношение между предоставлением уверенности и потенциальным уменьшением доступности ОО, поскольку слишком частое тестирование может замедлить нормальное функционирование ОО.

J.1.3.3.2 Назначение

В FPT_AMT.1.1 автору ПЗ/ЗБ следует (если другие условия выбраны) специфицировать частоту, с которой будет проходить самотестирование.

J.2 Безопасность при сбое (FPT_FLS)

J.2.1 Замечания для пользователя

Требования семейства FPT_FLS обеспечивают, чтобы ОО не нарушал свою политику безопасности при сбоях ФБО идентифицированных типов.

J.2.2 FPT_FLS.1 Сбой с сохранением безопасного состояния

J.2.2.1 Замечания по применению для пользователя

Термин «безопасное состояние» относится к состоянию, при котором данные ФБО непротиворечивы и ФБО продолжают корректное осуществление ПБО. «Безопасное состояние» определяют в модели ПБО. Если

разработчик предоставил четкое определение безопасного состояния и разъяснение, когда его следует считать таковым, зависимость FPT_FLS.1 «Сбой с сохранением безопасного состояния» от ADV_SPM.1 «Неформальная модель политики безопасности ОО» можно не учитывать.

Хотя при сбоях с сохранением безопасного состояния желательно проведение аудита, это возможно не во всех ситуациях. Автору ПЗ/ЗБ следует специфицировать те ситуации, при которых проведение аудита желательно и выполнимо.

Сбои ФБО могут включать в себя аппаратные отказы, которые указывают на нарушение режима работы оборудования и требуют аварийной поддержки или восстановления ФБО. Сбои ФБО могут включать в себя также устранимые программные отказы, после которых требуется только инициализация или повторный запуск ФБО.

J.2.2.2 Операции

J.2.2.2.1 Назначение

В FPT_FLS.1.1 автору ПЗ/ЗБ следует привести список типов сбоев ФБО, при которых должен быть «безопасный сбой» ФБО, то есть ФБО сохранили безопасное состояние и продолжали корректно осуществлять ПБО.

J.3 Доступность экспортируемых данных ФБО (FPT_ITA)

J.3.1 Замечания для пользователя

Семейство FPT_ITA определяет правила предотвращения потери доступности данных ФБО, передаваемых между ФБО и удаленным доверенным продуктом ИТ. Это могут быть, например, критичные данные ФБО, такие как пароли, ключи, данные аудита или выполняемый код ФБО.

Это семейство используют в распределенных системах, если ФБО предоставляют свои данные удаленному доверенному продукту ИТ. ФБО могут предпринять меры безопасности лишь со своей стороны и не могут нести ответственность за ФБО другого доверенного продукта ИТ.

Если имеется несколько различных метрик доступности для разных типов данных ФБО, этот компонент следует повторить для каждой отдельной пары «метрика — тип данных ФБО».

J.3.2 FPT_ITA.1 Доступность экспортируемых данных ФБО в пределах заданной метрики

J.3.2.1 Операции

J.3.2.1.1 Назначение

В FPT_ITA.1.1 автору ПЗ/ЗБ следует специфицировать типы данных ФБО, на которые распространяется метрика доступности.

В FPT_ITA.1.1 автору ПЗ/ЗБ следует специфицировать метрику доступности для соответствующих данных ФБО.

В FPT_ITA.1.1 автору ПЗ/ЗБ следует специфицировать условия, при которых необходимо обеспечить доступность. Это может быть, например наличие связи между ОО и удаленным доверенным продуктом ИТ.

J.4 Конфиденциальность экспортируемых данных ФБО (FPT_ITC)

J.4.1 Замечания для пользователя

Семейство FPT_ITC определяет правила защиты данных ФБО от несанкционированного раскрытия при передаче между ФБО и удаленным доверенным продуктом ИТ. Это могут быть, например критичные данные ФБО, такие как пароли, ключи, данные аудита или выполняемый код ФБО.

Данное семейство используют в распределенных системах, если ФБО предоставляют свои данные удаленному доверенному продукту ИТ. ФБО могут предпринять меры безопасности лишь в своей области действия и не могут нести ответственность за ФБО другого доверенного продукта ИТ.

J.4.2 FPT_ITC.1 Конфиденциальность экспортируемых данных ФБО при передаче

J.4.2.1 Замечания для оценщика

Конфиденциальность данных ФБО во время передачи необходима для их защиты от раскрытия. Возможные способы обеспечения конфиденциальности включают в себя применение криптографии, а также других методов, выбор которых постоянно расширяется.

J.5 Целостность экспортируемых данных ФБО (FPT_ITI)

J.5.1 Замечания для пользователя

Семейство FPT_ITI определяет правила защиты данных ФБО от несанкционированной модификации при передаче между ФБО и удаленным доверенным продуктом ИТ. Это могут быть, например, критичные данные ФБО типа паролей, ключей, данных аудита или выполняемого кода ФБО.

Данное семейство используется в распределенных системах, если ФБО предоставляют свои данные удаленному доверенному продукту ИТ. Отметим, что требования, связанные с модификацией, обнаружением или восстановлением и относящиеся к удаленному доверенному продукту ИТ, невозможно специфицировать, поскольку заранее не известны механизмы, которые будут использованы в удаленном доверенном продукте ИТ. Поэтому эти требования выражены в терминах «предоставления ФБО возможности», которую может использовать удаленный доверенный продукт ИТ.

J.5.2 FPT_ITI.1 Обнаружение модификации экспортируемых данных ФБО

J.5.2.1 Замечания по применению для пользователя

Компонент FPT_ITI.1 следует использовать в ситуациях, когда достаточно обнаружить факт модификации данных. Примером является ситуация, когда у удаленного доверенного продукта ИТ имеется возможность запросить ФБО о повторении передачи данных при обнаружении их модификации или удовлетворить аналогичный запрос.

Желательная стойкость функции обнаружения модификации основана на определенной метрике модификации, которая зависит от используемого алгоритма и может находиться в диапазоне от простых контрольных сумм и проверки на четность, которые не обнаруживают простые комбинации изменений в нескольких разрядах, до более сложных криптографических контрольных сумм.

J.5.2.2 Операции

J.5.2.2.1 Назначение

В FPT_ITI.1.1 автору ПЗ/ЗБ следует специфицировать метрику модификации, удовлетворение которой необходимо для механизма обнаружения. Эта метрика должна определить желательную стойкость функции обнаружения модификации.

В FPT_ITI.1.2 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые при обнаружении модификации данных ФБО. Примером таких действий может служить: «игнорировать полученные данные ФБО и запросить у доверенного продукта, являющегося отправителем, повторную передачу данных ФБО».

J.5.3 FPT_ITI.2 Обнаружение и исправление модификации экспортируемых данных ФБО

J.5.3.1 Замечания по применению для пользователя

Компонент FPT_ITI.2 следует использовать в ситуациях, когда требуется обнаружить или исправить модификации критичных данных ФБО.

Желательная стойкость функции обнаружения модификации основана на определенной метрике модификаций, которая зависит от используемого алгоритма и может находиться в диапазоне от контрольных сумм и проверки на четность, которые могут не обнаружить простые комбинации изменений в нескольких разрядах, до более сложных криптографических контрольных сумм. Метрику, которую требуется определить, можно связать с отражением атак (например, будет пропускаться только одно из тысячи случайных сообщений) либо с приведенным в открытой литературе механизмом (например, необходимо, чтобы требуемая стойкость соответствовала стойкости алгоритма безопасного хэширования).

Подход к исправлению модификаций может быть основан на использовании некоторых видов контрольных сумм, позволяющих корректировать ошибки.

J.5.3.2 Замечания для оценщика

Возможные способы удовлетворения этих требований состоят в использовании криптографических функций или некоторых видов контрольных сумм.

J.5.3.3 Операции

J.5.3.3.1 Назначение

В FPT_ITI.2.1 автору ПЗ/ЗБ следует специфицировать метрику модификации, удовлетворение которой необходимо для механизма обнаружения. Эта метрика должна определить желательную стойкость функции обнаружения модификации.

В FPT_ITI.2.2 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые при обнаружении модификации данных ФБО. Примером таких действий может служить: «игнорировать полученные данные ФБО и запросить у доверенного продукта, являющегося отправителем, повторную передачу данных ФБО».

В FPT_ITI.2.3 автору ПЗ/ЗБ следует определить типы модификаций, после которых ФБО следует предоставить возможность восстановления.

J.6 Передача данных ФБО в пределах ОО (FPT_ITT)

J.6.1 Замечания для пользователя

Семейство FPT_ITT содержит требования защиты данных ФБО при их передаче между разделенными частями ОО по внутреннему каналу.

Принятие решения о степени физического или логического разделения, в условиях которого могло бы применяться это семейство, зависит от предполагаемой среды эксплуатации. В неблагоприятной среде могут возникать риски, связанные с передачей между частями ОО, разделенными всего лишь системной шиной. В более благоприятной среде для передачи можно использовать обычные сетевые средства.

J.6.2 Замечания для оценщика

Один из механизмов, практически применяемых для реализации функциями безопасности ОО этого вида защиты, основан на применении криптографических методов.

J.6.3 FPT_ITT.1 Базовая защита внутренней передачи данных ФБО

J.6.3.1 Операции

J.6.3.1.1 Выбор

В FPT_ITT.1.1 автору ПЗ/ЗБ следует специфицировать требуемый тип защиты от раскрытия или модификации.

J.6.4 FPT_ITT.2 Разделение данных ФБО при передаче

J.6.4.1 Замечания по применению для пользователя

Одним из путей выполнения разделения каналов, основанного на атрибутах, относящихся к ПФБ, является использование разделенных логических или физических каналов.

J.6.4.2 Операции

J.6.4.2.1 Выбор

В FPT_ITT.2.1 автору ПЗ/ЗБ следует специфицировать требуемый тип защиты: от раскрытия или от модификации.

J.6.5 FPT_ITT.3 Мониторинг целостности данных ФБО

J.6.5.1 Операции

J.6.5.1.1 Выбор

В FPT_ITT.3.1 автору ПЗ/ЗБ следует специфицировать, какой тип модификации должны быть способны обнаруживать ФБО, выбирая из следующих типов: модификация данных, подмена данных, перестановка данных, удаление данных или какие-либо иные ошибки целостности.

J.6.5.1.2 Назначение

В FPT_ITT.3.1 в случае выбора автором ПЗ/ЗБ последнего варианта из предыдущего абзаца ему следует также специфицировать, какие иные ошибки целостности ФБО следует обнаруживать.

В FPT_ITT.3.2 автору ПЗ/ЗБ следует специфицировать действия, предпринимаемые при обнаружении ошибки целостности.

J.7 Физическая защита ФБО (FPT_PHP)

J.7.1 Замечания для пользователя

Компоненты семейства FPT_PHP «Физическая защита ФБО» дают возможность ограничивать физический доступ к ФБО, а также удерживать от несанкционированной физической модификации или подмены реализации ФБО и противодействовать им.

Требования компонентов в этом семействе обеспечивают защиту ФБО от физического воздействия и вмешательства. Удовлетворение требований этих компонентов позволяет получить реализацию ФБО, компонуемую и используемую способом, предусматривающим обнаружение физического воздействия или противодействие ему. Без этих компонентов защита ФБО теряет свою эффективность в среде, где не может быть предотвращено физическое повреждение. Это семейство также содержит требования к реакции ФБО на попытки физического воздействия на их реализацию.

Примерами сценариев физического воздействия являются нападения с использованием механических средств, радиоактивного излучения, изменения температуры.

Допускается, чтобы функции обнаружения физических нападений были доступны уполномоченному пользователю только в автономном режиме или режиме аварийной поддержки. Следует предусмотреть средства ограничения доступа в этих режимах, предоставляя его только уполномоченным пользователям. Поскольку в этих режимах ФБО могут оказаться «невыполнимыми», это может помешать нормальному осуществлению доступа уполномоченных пользователей. Физически ОО может состоять из устройств различного типа, например, из экранирующего корпуса, плат и микросхем. Необходимо, чтобы эта совокупность «элементов» защищала ФБО от физического воздействия (а также оповещала о нем и противодействовала ему). Это не означает, что эти качества необходимы всем устройствам по отдельности, но следует, чтобы их имело физическое воплощение ОО в целом.

Хотя с компонентами данного семейства ассоциирован только минимальный аудит, это сделано исключительно потому, что потенциально механизмы обнаружения и оповещения могут быть реализованы полностью аппаратно, на уровне взаимодействий более низком, чем управление подсистемой аудита (например, это может быть система обнаружения на аппаратном уровне, реагирующая на разрыв цепи и подающая световой сигнал, если цепь разорвана в момент нажатия кнопки уполномоченным пользователем). Тем не менее, автор ПЗ/ЗБ может определить, что для некоторых угроз, исходящих от среды, требуется аудит физических нападений. В этом случае автору ПЗ/ЗБ следует включить в список событий аудита соответствующие требования. Необходимо иметь в виду, что наличие этих требований может повлиять на конструкцию аппаратуры и ее взаимодействие с программным обеспечением.

J.7.2 FPT_PHP.1 Пассивное обнаружение физического нападения

J.7.2.1 Замечания по применению для пользователя

Компонент FPT_PHP.1 «Пассивное обнаружение физической атаки» следует применять, если угрозам несанкционированного физического воздействия на части ОО не противопоставлены процедурные методы. В этом компоненте рассматривается угроза того, что физическое воздействие на ФБО может и не быть выявлено. Обычно задача верификации того, что нападение имело место, возлагается на уполномоченного пользователя. Как было изложено выше, этот компонент всего лишь представляет способность ФБО обнаруживать физическое воздействие, поэтому требуется зависимость от FMT_MOF.1 «Управление режимом выполнения функций безопасности», чтобы специфицировать, кто и каким образом может воспользоваться этой способностью. Если эта функция реализована с помощью механизма, не связанного с ИТ (например, путем физической проверки), то может быть указано, что зависимость от FMT_MOF.1 не удовлетворяется.

J.7.3 FPT_PHP.2 Оповещение о физическом нападении

J.7.3.1 Замечания по применению для пользователя

Компонент FPT_PHP.2 «Оповещение о физическом нападении» следует применять, если угрозам несанкционированного физического воздействия на части ОО не противопоставлены процедурные методы, и при этом требуется оповещение определенных лиц о физическом нападении. В этом компоненте рассматривается угроза, что физическое воздействие на элементы ФБО может быть хотя и выявлено, но не замечено (то есть о нем никто не оповещен).

J.7.3.2 Операции

J.7.3.2.1 Назначение

В FPT_PHP.2.3 автору ПЗ/ЗБ следует представить список устройств/элементов, реализующих ФБО, для которых требуется активное обнаружение физического воздействия.

В FPT_PHP.2.3 автору ПЗ/ЗБ следует указать пользователя или роль, уведомляемую об обнаружении физического воздействия. Тип пользователя или роли могут меняться на итерациях компонента управления безопасностью FMT_MOF.1 «Управление режимом выполнения функций безопасности», включенного в ПЗ/ЗБ.

J.7.4 FPT_PHP.3 Противодействие физическому нападению

J.7.4 1 Замечания по применению для пользователя

Для некоторых типов воздействия требуется, чтобы ФБО не только обнаруживали воздействие, но и фактически противодействовали ему или задерживали напавшего.

Компонент FPT_PHP.3 следует использовать, если устройства и элементы, реализующие ФБО, предназначены для эксплуатации в среде, где физическое воздействие (например, с целью наблюдения, анализа или модификации) на составляющие устройств, реализующих ФБО, или на элементы, реализующие ФБО, само по себе признано угрозой.

J.7.4.2 Операции

J.7.4.2.1 Назначение

В FPT_PHP.3.1 автору ПЗ/ЗБ следует специфицировать для списка устройств/элементов, реализующих ФБО, сценарии физического проникновения; ФБО следует противодействовать физическому проникновению, выполняемому по этим сценариям. Этот список может относиться к определенному подмножеству физических устройств и элементов, реализующих ФБО, выделенному на основе учета технологических ограничений и физической незащищенности прибора. Выделение такого подмножества следует четко определить и логически обосновать. Кроме того, ФБО следует реагировать на попытки физического проникновения автоматически. При автоматической реакции на физическое проникновение следует сохранять политику безопасности устройства, например, если проводится политика конфиденциальности, то прибор должен быть гарантированно отключен для того, чтобы защищаемая информация не могла быть считана.

В FPT_PHP.3.1 автору ПЗ/ЗБ следует специфицировать список устройств/элементов, реализующих ФБО, для которых ФБО следует противодействовать физическому проникновению согласно идентифицированным сценариям.

J.8 Надежное восстановление (FPT_RCV)

J.8.1 Замечания для пользователя

Требования семейства FPT_RCV «Надежное восстановление» обеспечивают, чтобы ФБО могли определить, не нарушена ли защита ФБО при запуске, и восстанавливаться без нарушения защиты после прерывания операций. Это семейство важно, потому что начальное состояние ФБО при запуске или восстановлении определяет защищенность ОО в последующем.

Компоненты данного семейства позволяют устанавливать безопасное состояние ФБО или предотвращать их переход в опасное состояние после сбоев, прерывания функционирования или перезапуска. В число возможных сбоев обычно включают:

a) сбои, которые всегда приводят к аварийным отказам системы (например устойчивая несогласованность критичных системных таблиц; неуправляемые переходы в коде ФБО, вызванные сбоями аппаратных или программно-аппаратных средств; сбои питания, процессора, связи);

b) сбои носителей, приводящие к тому, что часть носителя или весь носитель, представляющий объекты ФБО, становится недоступным или неисправным (например ошибки четности, неисправность головок дисков, устойчивый сбой чтения/записи, неточная юстировка головок дисков, износ магнитного покрытия, запыленность поверхности диска);

c) прерывание функционирования вследствие ошибочных действий администратора или отсутствия его своевременных действий (например неожиданное прекращение работы из-за неподготовленности к отключению питания, игнорирование перерасхода критичных ресурсов, неадекватная инсталлированная конфигурация).

Важно отметить, что восстановление может быть предусмотрено для сценария как частичного, так и полного отказа. Полный отказ может возникнуть в неразделенной операционной системе, в распределенной среде его вероятность меньше. В такой среде некоторые подсистемы могут отказать, в то время как другие части останутся работающими. Более того, критичные элементы могут иметь избыточность (дублирование дисков, альтернативные маршруты) и точки проверки. Под восстановлением имеется в виду восстановление безопасного состояния.

При выборе FPT_RCV «Надежное восстановление» необходимо принимать во внимание следующие взаимосвязи между FPT_RCV «Надежное восстановление» и FPT_TST «Самотестирование ФБО»:

a) на необходимость надежного восстановления могут указывать результаты самотестирования ФБО, если результаты самотестирования указывают, что ФБО находятся в небезопасном состоянии и требуется возврат в безопасное состояние или переход в режим аварийной поддержки;

b) сбой, как было рассмотрено выше, может быть идентифицирован администратором. Либо администратор может выполнить действия для возврата ОО в безопасное состояние и затем прибегнуть к самотестированию ФБО, для того чтобы подтвердить, что безопасное состояние было достигнуто. Либо самотестирование ФБО может быть применено для завершения процесса восстановления;

c) сочетание взаимосвязей по перечислениям a) и b): если на необходимость надежного восстановления указывают результаты самотестирования ФБО, администратор выполняет действия по возврату ОО в безопасное состояние, а затем прибегает к самотестированию ФБО, чтобы подтвердить, что безопасное состояние было достигнуто;

d) самотестирование направлено на обнаружение сбоев/прерываний обслуживания, за которым следует либо автоматическое восстановление, либо переход в режим аварийной поддержки.

Семейство FPT_RCV идентифицирует режим аварийной поддержки. В этом режиме нормальное функционирование может оказаться невозможным или сильно ограниченным из-за возможности перехода в опасное состояние. В таких случаях обычно доступ разрешается только уполномоченным пользователям, а конкретно тем, кто может получить доступ в режиме аварийной поддержки, и определяется в классе FMT «Управление безопасностью». Если в классе FMT нет никаких указаний о том, кто имеет право доступа в этом режиме, теоретически допускается, что восстановить систему может любой пользователь. Однако на практике это нежелательно, поскольку пользователь, восстанавливающий систему, может установить конфигурацию ОО, нарушающую ПБО.

Механизмы, предназначенные для обнаружения исключительных состояний при эксплуатации, определяются в FPT_TST «Самотестирование ФБО», FPT_FLS «Безопасность при сбое» и других разделах, относящихся к проблеме «Сохранность программного обеспечения». Вероятно, использование одного из этих семейств потребуется при выборе FPT_RCV «Надежное восстановление». Это обеспечит возможность ОО определить необходимость в восстановлении.

В данном семействе применяется выражение «безопасное состояние». Оно относится к состоянию, при котором данные ФБО непротиворечивы и продолжают корректное осуществление ПБО. Это состояние может быть состоянием после загрузки системы или состоянием в некоторой контрольной точке. «Безопасное состояние» определяется в модели ПФБ. Если разработчик предоставил четкое определение безопасного состояния и разъяснение, когда его следует считать таковым, зависимость любого из компонентов из FPT_RCV «Надежное восстановление» от ADV_SPM.1 «Неформальная модель политики безопасности ОО» можно не учитывать.

После восстановления может потребоваться (через самостестирование ФБО) подтверждение того, что безопасное состояние достигнуто. Однако если восстановление выполняется так, чтобы только безопасное состояние могло быть достигнуто, иначе восстановление не происходит, тогда зависимость от компонента самотестирования ФБО (FPT_TST.1 «Тестирование ФБО») может быть признана ненужной.

J.8.2 FPT_RCV.1 Ручное восстановление

J.8.2.1 Замечания по применению для пользователя

В иерархии семейства FPT_RCV «Надежное восстановление» восстановление, которое требует только ручного вмешательства, наименее желательно, так как при этом исключается восстановление системы без участия человека.

Компонент FPT_RCV.1 предназначен для применения в ОО, которые не требуют автоматического восстановления безопасного состояния. Требования этого компонента направлены против угрозы нарушения защиты в результате приведения ОО с участием человека в опасное состояние при восстановлении после сбоя или другого прерывания.

J.8.2.2 Замечания по применению для оценщика

Допускается, чтобы функции уполномоченного администратора по надежному восстановлению были доступны ему только в режиме аварийной поддержки. Следует предусмотреть средства ограничения доступа в режиме аварийной поддержки, предоставляя его только уполномоченным пользователям.

J.8.2.3 Операции

J.8.2.3.1 Назначение

В FPT_RCV.1.1 автору ПЗ/ЗБ следует специфицировать список сбоев или прерываний обслуживания (сбой электропитания, исчерпание объема памяти для хранения данных аудита, любой сбой или прерывание), после которых ОО перейдет в режим аварийной поддержки.

J.8.3 FPT_RCV.2 Автоматическое восстановление

J.8.3.1 Замечания по применению для пользователя

Автоматическое восстановление считается более предпочтительным, чем ручное, так как позволяет машине продолжать функционирование без участия человека.

Компонент FPT_RCV.2 «Автоматическое восстановление» расширяет FPT_RCV.1 «Ручное восстановление», требуя возможность автоматического восстановления хотя бы после одного типа сбоя/прерывания обслуживания. Требования этого компонента направлены против угрозы нарушения защиты в результате приведения ОО без участия человека в опасное состояние при восстановлении после сбоя или другого прерывания.

J.8.3.2 Замечания по применению для оценщика

Допускается, чтобы функции уполномоченного администратора по надежному восстановлению были доступны ему только в режиме аварийной поддержки. Следует предусмотреть средства ограничения доступа в режиме аварийной поддержки, предоставляя его только уполномоченным пользователям.

В соответствии с FPT_RCV.2.1 разработчик ФБО отвечает за определение совокупности сбоев и прерываний обслуживания, после которых возможно восстановление.

Предполагается, что робастность механизмов автоматического восстановления будет верифицирована.

J.8.3.3 Операции

J.8.3.3.1 Назначение

В FPT_RCV.2.1 автору ПЗ/ЗБ следует специфицировать список сбоев или прерываний обслуживания (сбой электропитания, исчерпание объема памяти для хранения данных аудита), после которых ОО перейдет в режим аварийной поддержки.

В FPT_RCV.2.2 автору ПЗ/ЗБ следует специфицировать список сбоев или других прерываний обслуживания, для которых автоматическое восстановление должно быть возможно.

J.8.4 FPT_RCV.3 Автоматическое восстановление без недопустимой потери

J.8.4.1 Замечания по применению для пользователя

Автоматическое восстановление считается более предпочтительным, чем ручное, но оно связано с риском потери большого числа объектов. Предотвращение недопустимых потерь объектов обеспечивается дополнительными средствами восстановления.

Компонент FPT_RCV.3 «Автоматическое восстановление без недопустимой потери» расширяет FPT_RCV.2 «Автоматическое восстановление», требуя, чтобы не было чрезмерных потерь данных или объектов ФБО в ОДФ. В соответствии с FPT_RCV.2 «Автоматическое восстановление» механизм автоматического восстановления мог бы в крайнем случае произвести восстановление путем уничтожения всех объектов и возвращения ФБО в известное безопасное состояние. Такой тип автоматического восстановления в FPT_RCV.3 «Автоматическое восстановление без недопустимой потери» запрещается.

Требования этого компонента направлены против угрозы нарушения защиты в результате непредусмотренного перехода ОО в опасное состояние при восстановлении после сбоя или перерывов в функционировании с большой потерей данных или объектов ФБО в ОДФ.

J.8.4.2 Замечания для оценщика

Допускается, чтобы функции уполномоченного администратора по надежному восстановлению были доступны ему только в режиме аварийной поддержки. Следует предусмотреть средства ограничения доступа в режиме аварийной поддержки, предоставляя его только уполномоченным пользователям.

Предполагается, что робастность механизмов автоматического восстановления будет верифицирована оценщиком.

J.8.4.3 Операции

J.8.4.3.1 Назначение

В FPT_RCV.3.1 автору ПЗ/ЗБ следует специфицировать список сбоев или прерываний обслуживания (сбой электропитания, исчерпание объема памяти для хранения данных аудита), после которых ОО перейдет в режим аварийной поддержки.

В FPT_RCV.3.2 автору ПЗ/ЗБ следует специфицировать список сбоев или других прерываний обслуживания, для которых необходима возможность автоматического восстановления.

В FPT_RCV.3.3 автору ПЗ/ЗБ следует предоставить количественную меру приемлемых потерь данных или объектов ФБО.

J.8.5 FPT_RCV.4 Восстановление функции

J.8.5.1 Замечания по применению для пользователя

Компонент FPT_RCV.4 содержит требование, чтобы в случае сбоя ФБО некоторые функции из числа ФБО нормально заканчивали работу либо возвращались к безопасному состоянию.

J.8.5.2 Операции

J.8.5.2.1 Назначение

В FPT_RCV.4.1 автору ПЗ/ЗБ следует специфицировать список функций безопасности и сценариев сбоев, для которых нормально заканчивается работа ФБ, указанных в списке, или восстанавливается их устойчивое и безопасное состояние.

J.9 Обнаружение повторного использования (FPT_RPL)

J.9.1 Замечания для пользователя

Семейство FPT_RPL связано с обнаружением повторного использования различных типов сущностей (например, сообщений, запросов на обслуживание, ответов на запросы обслуживания) и последующими действиями по его устранению.

J.9.2 FPT_RPL.1 Обнаружение повторного использования

J.9.2.1 Замечания по применению для пользователя

Рассматриваемыми здесь сущностями могут быть, например сообщения, запросы на обслуживание, ответы на запросы обслуживания или сеансы пользователей.

J.9.2.2 Операции

J.9.2.2.1 Назначение

В FPT_RPL.1.1 автору ПЗ/ЗБ следует представить список идентифицированных сущностей, для которых следует предусмотреть возможность обнаружения повторного использования. Их примерами могут быть: сообщения, запросы на обслуживание, ответы на запросы обслуживания, сеансы пользователей.

В FPT_RPL.1.2 автору ПЗ/ЗБ следует специфицировать список действий, предпринимаемых ФБО при обнаружении повторного использования. Совокупность предпринимаемых действий может включать в себя игнорирование повторно используемой сущности, запрос подтверждения сущности из идентифицированного источника и отключение субъекта, пытавшегося инициировать повторное использование.

J.10 Посредничество при обращениях (FPT_RVM)

J.10.1 Замечания для пользователя

Требования семейства FPT_RVM связаны с аспектом «постоянная готовность» традиционного монитора обращений. Цель этого семейства состоит в обеспечении для заданной ПФБ того, чтобы в ОДФ все действия,

требующие осуществления политики и инициируемые субъектами, недоверенными относительно одной или всех ПФБ, над объектами, управляемыми этой ПФБ, проверялись ФБО на соответствие ПФБ. Если помимо этого часть ФБО, осуществляющая ПФБ, выполняет требования соответствующих компонентов из семейств FPT_SEP «Разделение домена» и ADV_INT «Внутренняя структура ФБО», то эта часть ФБО обеспечивает «монитор обращений» для этой ПФБ.

Монитор обращений является частью ФБО, ответственной за осуществление ПБО, и обладает следующими тремя свойствами:

1) недоверенные субъекты не могут вмешиваться в работу монитора, то есть он устойчив к проникновению. Это свойство обеспечивается требованиями компонентов семейства FPT_SEP «Разделение домена»;

2) недоверенные субъекты не могут обойти проверки монитора, то есть он постоянно готов к работе. Это свойство обеспечивается требованиями компонентов семейства FPT_RVM «Посредничество при обращениях»;

3) монитор достаточно прост, его устройство поддается анализу, его действия понятны (то есть его построение концептуально несложно). Это свойство обеспечивается требованиями компонентов семейства ADV_INT «Внутреняя структура ФБО».

Единственный компонент семейства FPT_RVM содержит следующее требование: «ФБО должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ». В любой системе (распределенной или нет) имеется конечное число функций, ответственных за осуществление ПБО. В этом требовании не утверждается, что для управления безопасностью применяется одна функция. Наоборот, утверждается, что роль механизма проверки правомочности обращений выполняют несколько функций, и именно их совокупность, осуществляющая ПБО, объединена под именем монитора обращений. При этом необходимо принимать во внимание задачу сохранения простоты «монитора обращений».

ФБО при реализации ПФБ предоставляют эффективную защиту от несанкционированных операций тогда и только тогда, когда правомочность всех потенциально осуществляемых действий (например, доступа к объектам), запрошенных субъектами, недоверенными относительно всех или именно этой ПФБ, проверяется ФБО до выполнения действий. Если действия по проверке будут выполнены неправильно или проигнорированы (обойдены), то осуществление ПФБ в целом может быть поставлено под угрозу (ее можно обойти). Тогда «недоверенные» субъекты смогут обходить ПФБ различными способами (такими, как обход проверки доступа для некоторых субъектов и объектов, обход проверки для объектов, защита которых управляется прикладными программами, сохранение права доступа после истечения установленного срока действия, обход аудита событий, подлежащих аудиту, обход аутентификации). Важно отметить, что термин «недоверенный субъект» относится к субъектам, недоверенным относительно какой-либо или всех осуществляемых ПФБ; субъект может быть доверенным относительно одной ПФБ и недоверенным относительно другой.

J.10.2 FPT_RVM.1 Невозможность обхода ПБО

J.10.2.1 Замечания по применению для пользователя

Для получения эквивалента монитора обращений необходимо применить данный компонент совместно с FPT_SEP.2 «Отделение домена ПФБ» либо с FPT_SEP.3 «Полный монитор обращений», а также с ADV_INT.3 «Минимизация сложности». Кроме того, если требуется полное посредничество при обращениях, требования компонентов из класса FDP «Защита данных пользователя» необходимо распространить на все объекты в составе ОО.

J.11 Разделение домена (FPT_SEP)

J.11.1 Замечания для пользователя

Компоненты семейства FPT_SEP обеспечивают, чтобы, по меньшей мере, один домен безопасности был доступен только для собственного выполнения ФБО и чтобы они (ФБО) были защищены от внешнего вмешательства и искажения (например модификации кода или структур данных ФБО) со стороны недоверенных субъектов. Выполнение требований этого семейства устанавливает такую самозащиту ФБО, что недоверенный субъект не сможет модифицировать или повредить ФБО.

Данное семейство содержит следующие требования:

a) ресурсы домена безопасности ФБО («защищенного домена») и ресурсы субъектов и активных сущностей, внешних по отношению к этому домену, разделяются так, что сущности, внешние по отношению к защищенному домену, не смогут получить или модифицировать данные или код ФБО в пределах защищенного домена;

b) обмен между доменами управляется так, что невозможен произвольный вход в защищенный домен или произвольный выход из него;

c) параметры пользователя или прикладной программы, переданные в защищенный домен по адресу, проверяются относительно адресного пространства защищенного домена, а переданные по значению — относительно значений, ожидаемых этим доменом;

d) защищенные домены субъектов разделены, за исключением случаев, когда совместное использование одного домена управляется ФБО.

Данное семейство применяют, если требуется уверенность в том, что ФБО не подвержены внешнему воздействию.

Для получения эквивалента монитора обращений необходимо применить компонент FPT_SEP.2 «Отделение домена ПФБ» или FPT_SEP.3 «Полный монитор обращений» совместно с FPT_RVM.1 «Невозможность обхо-

да ПБО» и ADV_INT.3 «Минимизация сложности». Кроме того, если требуется полное посредничество при обращениях, требования компонентов из класса FDP «Защита данных пользователя» необходимо распространить на все объекты.

J.11.2 FPT_SEP.1 Отделение домена ФБО

J.11.2.1 Замечания для пользователя

Без отдельного защищенного домена для ФБО не может быть доверия тому, что ФБО не подвергались каким-либо воздействиям со стороны недоверенных субъектов. Такие воздействия могут привести к модификации кода и/или структур данных ФБО.

J.11.3 FPT_SEP.2 Отделение домена ПФБ

J.11.3.1 Замечания по применению для пользователя

Наиболее важной функцией ФБО является поддержка осуществляемых ими ПФБ. Чтобы упростить разработку ПФБ и приблизить их свойства к свойствам монитора обращений, в частности, к стойкости к воздействиям, функции, проводящие ПФБ, необходимо сосредоточить в домене, отличном от остальной части ФБО.

J.11.3.2 Замечания по применению для оценщика

Возможно, что монитор обращений в многоуровневом проекте предоставляет больше функций, чем требуется в ПФБ. Это проистекает из практической реализации многоуровневого проекта программного обеспечения. При этом функции, не относящиеся к ПФБ, следует свести к минимуму.

Допустимо, чтобы мониторы обращений для всех осуществляемых ПФБ находились как в одном домене монитора обращений, так и в нескольких доменах (каждый используется для осуществления одной или нескольких ПФБ). Если имеется несколько доменов монитора обращений для нескольких ПФБ, они могут быть равноправными или образовывать иерархию.

Для FPT_SEP.2.1 выражение «неизолированная часть ФБО» относится к той части ФБО, которая не охвачена в FPT_SEP.2.3.

J.11.3.3 Операции

J.11.3.3.1 Назначение

В FPT_SEP.2.3 автору ПЗ/ЗБ следует специфицировать те ПФБ управления доступом и/или информационными потоками, которым следует занимать отдельный домен.

J.11.4 FPT_SEP.3 Полный монитор обращений

J.11.4.1 Замечания по применению для пользователя

Наиболее важной функцией из числа ФБО является поддержка осуществляемых ими ПФБ. Компонент FPT_SEP.3 завершает требования предыдущих компонентов семейства, устанавливая, что все функции безопасности, проводящие ПФБ управления доступом и/или информационными потоками, будут выполняться в домене, отличном от домена выполнения остальных ФБО. Это упрощает разработку ФБО и приближает их свойства к свойствам монитора обращений, в частности, к стойкости к воздействиям.

J.11.4.2 Замечания по применению для оценщика

Возможно, что монитор обращений в многоуровневом проекте предоставляет больше функций, чем требуется в ПФБ. Это проистекает из практической реализации многоуровневого проекта программного обеспечения. При этом функции, не относящиеся к ПФБ, следует свести к минимуму.

Допустимо, чтобы мониторы обращений для всех осуществляемых ПФБ находились как в одном домене монитора обращений, так и в нескольких доменах (каждый используется для осуществления одной или нескольких ПФБ). Если имеется несколько доменов монитора обращений для нескольких ПФБ, они могут или быть равноправными, или образовывать иерархию.

J.12 Протокол синхронизации состояний (FPT_SSP)

J.12.1 Замечания для пользователя

Распределенные системы могут иметь бóльшую сложность, чем нераспределенные, из-за многообразия состояний частей системы, а также из-за задержек связи. В большинстве случаев синхронизация состояния между распределенными функциями включает в себя, вместо обычных действий, применение протокола обмена. Если в среде распределенных систем существуют угрозы безопасности, потребуются более сложные защищенные протоколы.

Семейство FPT_SSP «Протокол синхронизации состояний» устанавливает требование использования надежных протоколов некоторыми критичными по безопасности функциями из числа ФБО. Оно обеспечивает, чтобы две распределенные части ОО (например главные ЭВМ) синхронизировали свои состояния после действий, связанных с безопасностью.

Некоторые состояния невозможно синхронизировать, или затраты на транзакцию будут слишком велики для практического применения; отмена ключа шифрования является примером, когда после выполнения действия состояние может стать неопределенным. Другой пример: действие предпринято, а подтверждение не может быть отправлено либо сообщение проигнорировано получателем и поэтому отмены не произойдет. Неопределенность присуща распределенным системам. Проблема неопределенности связана с необходимостью синхронизации состояний и может решаться соответствующими методами. Планировать неопределенные состояния бесполезно; в подобных случаях автору ПЗ/ЗБ следует прибегнуть к другим требованиям (например подача сигнала тревоги, проведение аудита).

J.12.2 FPT_SSP.1 Одностороннее надежное подтверждение

J.12.2.1 Замечания по применению для пользователя

В компоненте FPT_SSP.1 необходимо, чтобы по запросу ФБО предоставляли подтверждение для другой части ФБО. Это подтверждение требуется для указания, что в одной части распределенного ОО успешно получено немодифицированное сообщение из другой части ОО.

J.12.3 FPT_SSP.2 Взаимное надежное подтверждение

J.12.3.1 Замечания по применению для пользователя

Компонент FPT_SSP.2 содержит требование, что в дополнение к предоставлению подтверждения получения передаваемых данных принимающей части ФБО необходимо обратиться к передающей за уведомлением о получении подтверждения.

Например, локальная часть ФБО передает данные удаленной части ФБО. Последняя подтверждает успешный прием сообщения и запрашивает у передавшей сообщение части ФБО уведомление, что она получила подтверждение. Этот механизм дает дополнительную уверенность, что обе части ФБО, участвующие в передаче данных, извещены об успешном завершении передачи.

J.13 Метки времени (FPT_STM)

J.13.1 Замечания для пользователя

Семейство FPT_STM содержит требования по предоставлению надежных меток времени в пределах ОО.

На автора ПЗ/ЗБ возлагается ответственность за разъяснение смысла выражения «надежные метки времени» и указание, где принимается решение о надежности.

J.13.2 FPT_STM.1 Надежные метки времени

J.13.2.1 Замечания по применению для пользователя

Применение компонента FPT_STM.1 возможно для предоставления надежных меток времени при проведении аудита, а также для ограничения срока действия атрибутов безопасности.

J.14 Согласованность данных ФБО между ФБО (FPT_TDC)

J.14.1 Замечания для пользователя

В среде распределенной или сложной системы от ОО может потребоваться произвести обмен данными ФБО (такими, как атрибуты ПФБ, ассоциированные с данными, информация аудита или идентификации) с другим доверенным продуктом ИТ. Семейство FPT_TDC определяет требования для совместного использования и непротиворечивой интерпретации этих атрибутов между ФБО и другим доверенным продуктом ИТ.

Компоненты данного семейства предназначены для определения требований к автоматической поддержке согласованности данных ФБО при их передаче между ФБО рассматриваемого ОО и ФБО другого доверенного продукта. Возможна и такая ситуация, когда для согласования атрибутов безопасности применяются только процедурные меры, однако они здесь не рассматриваются.

Семейство FPT_TDC «Согласованность данных ФБО между ФБО» отличается от FDP_ETC «Экспорт данных за пределы действия ФБО» и FDP_ITC «Импорт данных из-за пределов действия ФБО», так как последние направлены лишь на соотнесение атрибутов безопасности между ФБО и носителями импортируемой или экспортируемой ими информации.

В случае, если важна целостность данных ФБО, следует выбрать требования из семейства FPT_ITI «Целостность экспортируемых данных ФБО». Его компоненты определяют требования, чтобы ФБО были способны обнаружить и/или исправить модификации данных ФБО во время передачи.

J.14.2 FPT_TDC.1 Базовая согласованность данных ФБО между ФБО

J.14.2.1 Замечания по применению для пользователя

ФБО отвечают за поддержку согласованности данных ФБО, используемых ими или ассоциированных с ними, которые являются общими у двух или более доверенных систем. Например, данные ФБО для ФБО двух различных систем могут толковаться внутри них по-разному. Для правильного применения данных ФБО принимающим доверенным продуктом ИТ (например, для обеспечения такой же защиты данных пользователя, как и в ОО) необходимо, чтобы ОО и другой доверенный продукт ИТ применяли заранее установленный протокол обмена данными ФБО.

J.14.2.2 Операции

J.14.2.2.1 Назначение

В FPT_TDC.1.1 автору ПЗ/ЗБ следует определить список типов данных ФБО, которые должны согласованно интерпретироваться при совместном использовании ФБО и другим довереным продуктом ИТ.

В FPT_TDC.1.2 автору ПЗ/ЗБ следует привести список правил интерпретации, применяемых ФБО.

J.15 Согласованность данных ФБО при дублировании в пределах ОО (FPT_TRC)

J.15.1 Замечания для пользователя

Требования семейства FPT_TRC необходимы, чтобы обеспечить согласованность данных ФБО, если они дублируются в пределах ОО. Такие данные могут стать несогласованными при нарушении работоспособности внутреннего канала между частями ОО. Если ОО внутренне структурирован как сеть, то это может произойти из-за отключения отдельных частей сети при разрыве сетевых соединений.

Метод обеспечения согласованности в данном семействе не указывается. Согласованность может достигаться с помощью некоторой формы обработки транзакций (где соответствующие транзакции «возвращаются назад» к месту отправления через повторное соединение) или путем обновления дублируемых данных через

протокол синхронизации. Если для ПЗ/ЗБ необходим конкретный протокол, то он может быть специфицирован с использованием операции уточнения.

Может оказаться, что синхронизировать некоторые состояния невозможно или затраты на такую синхронизацию слишком высоки. Примером подобной ситуации служит отмена каналов связи и ключей шифрования. Могут также возникать неопределенные состояния. Если желателен конкретный режим функционирования, его следует специфицировать с использованием операции уточнения.

J.15.2 FPT_TRC.1 Согласованность дублируемых данных ФБО

J.15.2.1 Операции

J.15.2.1.1 Назначение

В FPT_TRC.1.2 автору ПЗ/ЗБ следует специфицировать список ФБ, которые зависят от согласованности дублирования данных ФБО.

J.16 Самотестирование ФБО (FPT_TST)

J.16.1 Замечания для пользователя

Семейство FPT_TST определяет требования для самотестирования ФБО путем выполнения некоторых типичных операций с известным результатом. Примерами могут служить обращения к интерфейсам осуществляемых функций, а также некоторые арифметические операции, выполняемые критичными частями ОО. Эти тесты могут выполняться при запуске, периодически, по запросу уполномоченного пользователя или при удовлетворении других условий. Действия ОО, предпринимаемые по результатам самотестирования, определены в других семействах.

Требования данного семейства также необходимы для обнаружения искажения выполняемого кода ФБО (то есть программной реализации ФБО) и данных ФБО в результате различных сбоев, которые не всегда приводят к приостановке функционирования ОО (рассмотренной в других семействах). Такие проверки необходимо выполнять, так как подобные сбои не всегда можно предотвратить. Они могут происходить из-за непредусмотренных типов сбоев или имеющихся неточностей в проекте аппаратных, программно-аппаратных и программных средств либо вследствие злонамеренного искажения ФБО, допущенного из-за неадекватной логической и/или физической защиты.

Дополнительно данное семейство может, при соответствующих условиях, помочь предотвратить неприемлемые или наносящие ущерб изменения ФБО, которые могут быть произведены в эксплуатируемом ОО при выполнении действий по сопровождению.

Термин «правильное выполнение ФБО» относится главным образом к функционированию программного обеспечения ФБО и целостности его данных. Абстрактная машина, на которой реализуется программное обеспечение ФБО, проверяется через зависимость от FPT_AMT «Тестирование базовой абстрактной машины».

J.16.2 FPT_TST.1 Тестирование ФБО

J.16.2.1 Замечания по применению для пользователя

Компонент FPT_TST.1 поддерживает как тестирование критичных функций из числа ФБО через требование возможности запускать тестирование функций, так и проверку целостности данных и выполняемого кода ФБО.

J.16.2.2 Замечания по применению для оценщика

Допускается, чтобы функции, предоставляемые уполномоченному пользователю для периодического тестирования, были доступны только в автономном режиме и режиме аварийной поддержки. В этих режимах следует предусмотреть средства ограничения доступа, предоставляя его только уполномоченным пользователям.

J.16.2.3 Операции

J.16.2.3.1 Выбор

В FPT_TST.1 автору ПЗ/ЗБ следует специфицировать, когда функциями безопасности ОО будет выполняться тестирование ФБО: при запуске, периодически в процессе нормального функционирования, по запросу уполномоченного пользователя, при других условиях. В последнем случае автору ПЗ/ЗБ следует также указать конкретные условия, используя операцию назначения.

В FPT_TST.1.1 автору ПЗ/ЗБ следует специфицировать, будет ли самотестирование выполняться для демонстрации правильного выполнения всего ФБО или только специфицированных частей ФБО.

J.16.2.3.2 Назначение

В FPT_TST.1.1 автору ПЗ/ЗБ следует, если сделан соответствующий выбор, специфицировать условия, при которых следует выполнять самотестирование.

В FPT_TST.1.1 автору ПЗ/ЗБ следует, если сделан соответствующий выбор, специфицировать список частей ФБО, которые будут предметом самотестирования ФБО.

J.16.2.3.3 Выбор

В FPT_TST.1.2 автору ПЗ/ЗБ следует специфицировать, должна ли быть предусмотрена возможность верификации целостности для всех данных ФБО или только для выбранных данных.

J.16.2.3.4 Назначение

В FPT_TST.1.2 автору ПЗ/ЗБ следует, если сделан соответствующий выбор, специфицировать список данных ФБО, целостность которых будет верифицироваться.

Приложение К
(обязательное)

Использование ресурсов (FRU)

Класс FRU содержит три семейства, которые поддерживают доступность требуемых ресурсов, таких как вычислительные возможности и/или объем памяти. Семейство FRU_FLT «Отказоустойчивость» предоставляет защиту от недоступности ресурсов, вызванной сбоем ОО. Семейство FRU_PRS «Приоритет обслуживания» обеспечивает, чтобы ресурсы выделялись наиболее важным или критичным по времени задачам и не могли быть монополизированы задачами с более низким приоритетом. Семейство FRU_RSA «Распределение ресурсов» устанавливает ограничения использования доступных ресурсов, предотвращая монополизацию ресурсов пользователями.

Декомпозиция класса FRU «Использование ресурсов» на составляющие его компоненты показана на рисунке К.1.

Рисунок К.1 — Декомпозиция класса FRU «Использование ресурсов»

К.1 Отказоустойчивость (FRU_FLT)

К.1.1 Замечания для пользователя

Семейство FRU_FLT содержит требования к доступности функциональных возможностей даже в случае сбоев. Примеры таких сбоев: отключение питания, отказ аппаратуры, сбой программного обеспечения. В случае таких ошибок, если это специфицировано, ОО будет поддерживать определенные возможности. Автор ПЗ/ЗБ может, например, специфицировать, что ОО, используемый на атомной станции, продолжит работу по выполнению процедуры остановки реактора при сбое в энергоснабжении или средствах связи.

Поскольку ОО может продолжать правильное функционирование только при продолжении осуществления ПБО, то имеется требование, что после сбоя система должна оставаться в безопасном состоянии. Эта способность обеспечивается привлечением компонента FPT_FLS.1 «Сбой с сохранением безопасного состояния».

Механизмы обеспечения отказоустойчивости могут быть активными или пассивными. Активный механизм имеет специальные функции, которые активизируются при возникновении ошибки. Например, пожарная сигнализация является активным механизмом: ФБО обнаружат пожар и смогут предпринять действия по включению операции резервирования. Пассивная схема применяется, если в архитектуре ОО заложена способность обработки ошибки. Например, применение мажоритарной схемы голосования с несколькими процессорами является пассивным решением; отказ одного процессора не прервет функционирование ОО (хотя отказ требуется обнаружить для исправления).

Для данного семейства не имеет значения, был ли сбой инициирован случайно (например переполнение или ошибочное отключение устройства) или преднамеренно (например, из-за монополизации ресурса).

К.1.2 FRU_FLT.1 Пониженная отказоустойчивость

К.1.2.1 Замечания по применению для пользователя

Компонент FRU_FLT.1 предназначен для спецификации того, какие возможности ОО продолжит предоставлять после сбоя системы. Так как сложно описать все возможные отказы, можно специфицировать их категории. Примерами типичных сбоев являются: затопление помещения с аппаратурой, короткое замыкание, сбой центрального процессора или главной ЭВМ, сбой программного обеспечения, переполнение буфера.

К.1.2.2 Операции

К.1.2.2.1 Назначение

В FRU_FLT.1.1 автору ПЗ/ЗБ следует специфицировать список возможностей ОО, которые ОО будет поддерживать во время и после специфицированного сбоя.

В FRU_FLT.1.1 автору ПЗ/ЗБ следует специфицировать список типов сбоев, от которых ОО должен быть обязательно защищен. Если случится сбой из этого списка, ОО будет способен продолжить функционирование.

К.1.3 FRU_FLT.2 Ограниченная отказоустойчивость

К.1.3.1 Замечания по применению для пользователя

Компонент FRU_FLT.2 позволяет специфицировать, каким типам сбоев ОО необходимо противодействовать. Так как сложно описать все возможные отказы, можно специфицировать их категории. Примерами типичных сбоев являются: затопление помещения с аппаратурой, кратковременное отключение энергоснабжения, сбой центрального процессора или главной ЭВМ, сбой программного обеспечения, переполнение буфера.

К.1.3.2 Операции

К.1.3.2.1 Назначение

В FRU_FLT.2.1 автору ПЗ/ЗБ следует специфицировать список типов сбоев, от которых ОО должен быть обязательно защищен. Если случится сбой из этого списка, ОО будет способен продолжить функционирование.

К.2 Приоритет обслуживания (FRU_PRS)

К.2.1 Замечания для пользователя

Требования семейства FRU_PRS позволяют ФБО управлять использованием ресурсов пользователями и субъектами в пределах своей области действия так, что высокоприоритетные операции в пределах ОДФ всегда будут выполняться без препятствий или задержек со стороны операций с более низким приоритетом. Другими словами, задачи, критичные по времени выполнения, не будут задерживаться задачами, менее критичными по времени выполнения.

Это семейство может применяться к различным типам ресурсов, например, вычислительным возможностям, пропускной способности каналов связи.

Механизм приоритетов обслуживания может быть пассивным или активным. В системе с пассивным приоритетом обслуживания выбирается задача с наивысшим приоритетом, если предлагается сделать выбор между двумя ожидающими приложениями. При использовании пассивных механизмов приоритетов обслуживания выполняемая задача с более низким приоритетом не может быть прервана задачей с более высоким приоритетом. При использовании активных механизмов приоритетов обслуживания задачи с более низким приоритетом могут прерываться новыми задачами с более высоким приоритетом.

Требования аудита устанавливают, что все причины отклонения операций следует подвергать аудиту. На усмотрение разработчика оставлена ситуация, когда операция не отклоняется, а задерживается.

К.2.2 FRU_PRS.1 Ограниченный приоритет обслуживания

К.2.2.1 Замечания по применению для пользователя

Компонент FRU_PRS.1 определяет приоритеты для субъектов и ресурсы, к которым будет применяться механизм приоритетов обслуживания. Если субъект пытается предпринять действие для получения ресурса, контролируемого требованиями приоритета обслуживания, доступ и/или время доступа будут поставлены в зависимость от приоритета субъекта, приоритета субъекта, действующего в настоящий момент, и приоритета субъектов в очереди.

К.2.2.2 Операции

К.2.2.2.1 Назначение

В FRU_PRS.1.2 автору ПЗ/ЗБ следует специфицировать список управляемых ресурсов, для которых ФБО осуществляют приоритетное обслуживание (примеры ресурсов: процессы, дисковое пространство, память, полоса пропускания).

К.2.3 FRU_PRS.2 Полный приоритет обслуживания

К.2.3.1 Замечания по применению для пользователя

Компонент FRU_PRS.2 определяет приоритеты для субъектов. Все ресурсы в ОДФ, которые могут использоваться совместно, будут управляться механизмом приоритетного обслуживания. Если субъект пытается предпринять действия на ресурсе в ОДФ, который может использоваться совместно, доступ и/или время доступа будет поставлено в зависимость от приоритета субъекта, приоритета субъекта, действующего в настоящий момент, и приоритета субъектов в очереди.

К.3 Распределение ресурсов (FRU_RSA)

К.3.1 Замечания для пользователя

Требования семейства FRU_RSA позволяют ФБО в пределах ОДФ управлять использованием ресурсов пользователями и субъектами так, чтобы не допустить несанкционированные отказы в обслуживании из-за монополизации ресурсов другими пользователями или субъектами.

Правила распределения ресурсов позволяют назначать квоты или создавать другие средства определения ограничений на количество ресурса или время его использования, которые могут быть распределены конкретным пользователям или субъектам. Этими правилами, например, могут быть:

- введение квот объектов, ограничивающих число объектов и/или их размер, которые могут быть назначены конкретному пользователю;
- управление распределением/освобождением выделенных ранее единиц ресурсов в случае, если они находятся под управлением ФБО.

В общем случае эти функции будут реализованы с применением атрибутов, назначенных пользователям и ресурсам.

Целью этих компонентов является обеспечение определенной степени «справедливости» по отношению к пользователям (например, всю доступную память не следует распределять одному пользователю) и субъектам.

Так как продолжительность распределения ресурсов часто превышает время существования субъекта (например, файлы часто существуют дольше, чем приложения, создавшие их), то неоднократное воплощение субъектов одним и тем же пользователем не должно оказывать слишком сильное отрицательное воздействие на других пользователей. Компоненты семейства позволяют связать ограничения на распределение ресурсов с пользователями. В некоторых же ситуациях ресурсы распределяются для субъектов (например оперативная память или циклы центрального процессора). В этом случае компоненты семейства позволяют распределять ресурсы на уровне субъектов.

Данное семейство налагает требования на распределение ресурсов, но не на их использование. Поэтому установлено, что требования аудита также распространяются на распределение ресурсов, но не на их использование.

К.3.2 FRU_RSA.1 Максимальные квоты

К.3.2.1 Замечания по применению для пользователя

Компонент FRU_RSA.1 содержит требования к механизмам квотирования, которые применимы только к специфицированной совокупности разделяемых ресурсов в ОО. Эти требования позволяют ассоциировать квоты с пользователем или, возможно, связывать их с группами пользователей или субъектов, если это предусмотрено в ОО.

К.3.2.2 Операции

К.3.2.2.1 Назначение

В FRU_RSA.1.1 автору ПЗ/ЗБ следует специфицировать список управляемых ресурсов, для которых требуются ограничения максимального выделения ресурса (например процессы, дисковое пространство, память, полоса пропускания). Если это требование необходимо распространить на все ресурсы в ОДФ, разрешается специфицировать «все ресурсы в ОДФ».

К.3.2.2.2 Выбор

В FRU_RSA.1.1 автору ПЗ/ЗБ следует выбрать, относятся ли максимальные квоты к отдельным пользователям, определенным группам пользователей, субъектам или любому их сочетанию.

В FRU_RSA.1.1 автору ПЗ/ЗБ следует выбрать, применимы ли максимальные квоты в любое заданное время (одновременно) или в течение определенного периода времени.

К.3.3 FRU_RSA.2 Минимальные и максимальные квоты

К.3.3.1 Замечания по применению для пользователя

Компонент FRU_RSA.2 содержит требования к механизмам квотирования, которые применимы только к специфицированной совокупности разделяемых ресурсов в ОО. Эти требования позволяют ассоциировать квоты с пользователем или, возможно, связывать их с группами пользователей или субъектов, если это предусмотрено в ОО.

К.3.3.2 Операции

К.3.3.2.1 Назначение

В FRU_RSA.2.1 автору ПЗ/ЗБ следует специфицировать управляемые ресурсы, для которых требуются ограничения максимального выделения ресурса (например процессы, дисковое пространство, память, полоса пропускания). Если это требование необходимо распространить на все ресурсы в ОДФ, разрешается специфицировать «все ресурсы в ОДФ».

К.3.3.2.2 Выбор

В FRU_RSA.2.1 автору ПЗ/ЗБ следует выбрать, относятся ли максимальные квоты к отдельным пользователям, определенным группам пользователей, субъектам или любому их сочетанию.

В FRU_RSA.2.1 автору ПЗ/ЗБ следует выбрать, применимы ли максимальные квоты в любое заданное время (одновременно) или в течение определенного периода времени.

К.3.3.2.3 Назначение

В FRU_RSA.2.2 автору ПЗ/ЗБ следует специфицировать управляемые ресурсы, для которых необходимо установить предел минимального выделения ресурса (например процессы, дисковое пространство, память, полоса пропускания). Если это требование необходимо распространить на все ресурсы в ОДФ, разрешается специфицировать «все ресурсы в ОДФ».

К.3.3.2.4 Выбор

В FRU_RSA.2.2 автору ПЗ/ЗБ следует выбрать, относятся ли минимальные квоты к отдельным пользователям, определенным группам пользователей, субъектам или любому их сочетанию.

В FRU_RSA.2.2 автору ПЗ/ЗБ следует выбрать, применимы ли минимальные квоты в любое заданное время (одновременно) или в течение определенного периода времени.

Федеральное агентство по техническому регулированию и метрологии

Приложение L
(обязательное)

Доступ к ОО (FTA)

Открытие сеанса пользователя обычно состоит из создания одного или нескольких субъектов, выполняющих операции в ОО от имени пользователя. В конце процедуры открытия сеанса, если удовлетворены требования доступа к ОО, созданные субъекты имеют атрибуты, определенные функциями идентификации и аутентификации. Класс FTA определяет требования к управлению открытием сеанса пользователя.

Сеанс пользователя определен как период времени, начинающийся с момента идентификации/аутентификации (или, точнее, с начала взаимодействия между пользователем и системой) вплоть до момента, когда освобождены все субъекты, ресурсы и атрибуты, относящиеся к данному сеансу.

Декомпозиция класса FTA «Доступ к ОО» на составляющие его компоненты показана на рисунке L.1.

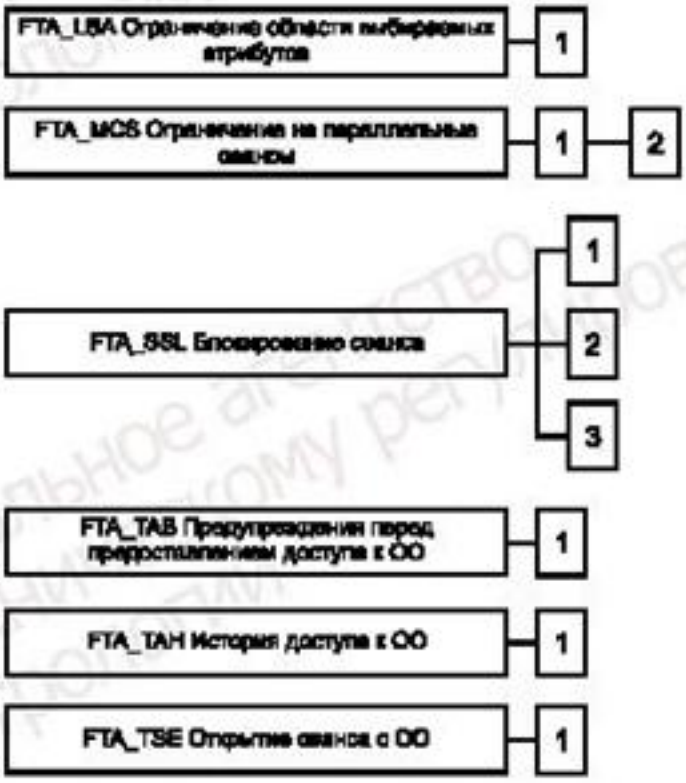

Рисунок L.1 — Декомпозиция класса FTA «Доступ к ОО»

L.1 Ограничение области выбираемых атрибутов (FTA_LSA)

L.1.1 Замечания для пользователя

Семейство FTA_LSA определяет требования по ограничению как атрибутов безопасности сеанса, которые может выбирать пользователь, так и субъектов, с которыми пользователь может быть связан, на основе метода или места доступа, порта, с которого осуществляется доступ, и/или времени (например, времени суток, дня недели).

Это семейство предоставляет авторам ПЗ/ЗБ возможность специфицировать требования для ФБО по установлению ограничений на область выбираемых атрибутов безопасности уполномоченных пользователей в зависимости от условий среды. Например, пользователю может быть разрешено открыть «секретный сеанс» в рабочее время, но вне рабочего времени он может открыть только «неклассифицированный сеанс». Для идентификации соответствующих ограничений на область выбираемых атрибутов предусмотрена операция выбора. Эти ограничения могут следовать из значений других атрибутов. Если необходимо специфицировать ограничения для нескольких атрибутов, то этот компонент придется повторить несколько раз по числу атрибутов. Примерами атрибутов, которые можно использовать для ограничения атрибутов безопасности сеанса, являются:

а) метод доступа. Может использоваться для спецификации среды, в которой будет работать пользователь (например протокол передачи файлов, терминал, виртуальный телекоммуникационный метод доступа);

b) место доступа. Может использоваться для ограничения области выбираемых атрибутов пользователя на основе места расположения пользователя или порта доступа. Эта возможность особенно важна при использовании телефонных линий или сетевых средств;

c) время доступа, которое можно использовать для ограничения области выбираемых атрибутов пользователя. Например, ограничения могут быть основаны на времени суток, дне недели, календарных датах. Это ограничение предоставляет определенную защиту от действий пользователя в то время, когда могут не применяться необходимые процедурные меры или мониторинг.

L.1.2 FTA_LSA.1 Ограничение области выбираемых атрибутов

L.1.2.1 Операции

L.1.2.1.1 Назначение

В FTA_LSA.1.1 автору ПЗ/ЗБ следует специфицировать совокупность атрибутов безопасности сеанса, которые нужно ограничить. Примеры таких атрибутов: уровень допуска пользователя, уровень целостности, роли.

В FTA_LSA.1.1 автору ПЗ/ЗБ следует специфицировать совокупность атрибутов, которые можно использовать для определения области атрибутов безопасности сеанса. Примеры таких атрибутов: идентификатор пользователя, расположение источника, время доступа и метод доступа.

L.2 Ограничение на параллельные сеансы (FTA_MCS)

L.2.1 Замечания для пользователя

Семейство FTA_MCS определяет, сколько сеансов пользователь может иметь одновременно (параллельные сеансы). Допустимое число параллельных сеансов может указываться для группы пользователей либо для каждого отдельного пользователя.

L.2.2 FTA_MCS.1 Базовое ограничение на параллельные сеансы

L.2.2.1 Замечания по применению для пользователя

Компонент FTA_MCS.1 предоставляет системе возможность ограничения числа сеансов в целях эффективного использования ресурсов ОО.

L.2.2.2 Операции

L.2.2.2.1 Назначение

В FTA_MCS.1.2 автору ПЗ/ЗБ следует специфицировать, какое ограничение числа параллельных сеансов будет использоваться по умолчанию.

L.2.3 FTA_MCS.2 Ограничение на параллельные сеансы по атрибутам пользователя

L.2.3.1 Замечания по применению для пользователя

Компонент FTA_MCS.2 предоставляет дополнительные возможности по сравнению с FTA_MCS.1 «Базовое ограничение на параллельные сеансы», позволяя установить дополнительные ограничения на число параллельных сеансов, которые пользователи в состоянии открыть. Эти ограничения основаны на атрибутах безопасности пользователя, таких как идентификатор пользователя или принадлежность к роли.

L.2.3.2 Операции

L.2.3.2.1 Назначение

В FTA_MCS.2.1 автору ПЗ/ЗБ следует специфицировать правила, определяющие максимально предоставляемое число параллельных сеансов. Примером такого правила является: «максимальное число параллельных сеансов равно одному, если пользователь имеет уровень допуска «секретно», и пяти — в остальных случаях».

В FTA_MCS.2.2 автору ПЗ/ЗБ следует специфицировать, какое ограничение числа параллельных сеансов будет использоваться по умолчанию.

L.3 Блокирование сеанса (FTA_SSL)

L.3.1 Замечания для пользователя

Семейство FTA_SSL определяет требования к ФБО по предоставлению возможности блокировать и разблокировать интерактивные сеансы (например, блокировать клавиатуру).

Когда пользователь непосредственно взаимодействует с субъектами в ОО (интерактивный сеанс), терминал пользователя уязвим, если он оставлен без надзора. Это семейство содержит требования к ФБО по отключению (блокированию) терминала или завершению сеанса после установленного времени бездеятельности, а к пользователю — по возможности инициировать отключение (блокирование) терминала. Для возвращения терминала в активное состояние необходимо, чтобы произошло событие, специфицированное автором ПЗ/ЗБ, например, повторная аутентификация пользователя.

Пользователь считается бездействующим, если он никак не воздействовал на ОО в течение некоторого периода времени.

Автору ПЗ/ЗБ следует учесть, требуется ли привлекать компонент FTP_TPR.1 «Доверенный маршрут». В этом случае следует через операцию компонента FTP_TPR.1 подключить функцию «блокирование сеанса».

L.3.2 FTA_SSL.1 Блокирование сеанса, инициированное ФБО

L.3.2.1 Замечания по применению для пользователя

Компонент FTA_SSL.1 «Блокирование сеанса, инициированное ФБО» предоставляет ФБО возможность блокировать сеанс пользователя по истечении заданного периода времени. Блокирование терминала прекратило бы все дальнейшие действия в данном сеансе с использованием заблокированного терминала.

Если на устройстве отображения перезаписывается информация, содержание замещающей информации необязательно статично (например, разрешается использовать «хранитель экрана»).

Данный компонент позволяет автору ПЗ/ЗБ специфицировать события, деблокирующие сеанс. Эти события могут быть связаны с терминалом (например набор установленной последовательности символов для разблокирования сеанса), с пользователем (например его повторная аутентификация) или со временем.

L.3.2.2 Операции

L.3.2.2.1 Назначение

В FTA_SSL.1.1 автору ПЗ/ЗБ следует специфицировать интервал бездействия пользователя, по истечении которого произойдет блокирование сеанса. При желании автор ПЗ/ЗБ может использовать данную операцию, чтобы возложить определение интервала времени на уполномоченного администратора или пользователя. Функции управления в классе FMT могут специфицировать возможность модификации этого интервала, задавая его значение по умолчанию.

В FTA_SSL.1.2 автору ПЗ/ЗБ следует специфицировать событие или события, которые происходили бы до разблокирования сеанса. Примеры таких событий: «повторная аутентификация пользователя» или «ввод пользователем с клавиатуры деблокирующей последовательности символов».

L.3.3 FTA_SSL.2 Блокирование, инициированное пользователем

L.3.3.1 Замечания по применению для пользователя

Компонент FTA_SSL.2 «Блокирование, инициированное пользователем» предоставляет уполномоченному пользователю возможность блокировать и деблокировать свой собственный терминал. Это предоставило бы уполномоченным пользователям возможность эффективно блокировать свои сеансы без необходимости их завершения.

Если на устройстве отображения перезаписывается информация, содержание замещающей информации необязательно статично (например, разрешается использовать «хранитель экрана»).

L.3.3.2 Операции

L.3.3.2.1 Назначение

В FTA_SSL.2.2 автору ПЗ/ЗБ следует специфицировать событие или события, которые происходили бы до разблокирования сеанса. Примеры таких событий: «повторная аутентификация пользователя» или «ввод пользователем с клавиатуры деблокирующей последовательности символов».

L.3.4 FTA_SSL.3 Завершение, инициированное ФБО

L.3.4.1 Замечания по применению для пользователя

Компонент FTA_SSL.3 «Завершение, инициированное ФБО» содержит требование, чтобы ФБО завершали интерактивный сеанс пользователя после установленного периода его бездействия.

Автору ПЗ/ЗБ следует учесть, что сеанс может продолжаться и после того, как пользователь окончил активные действия, например, в виде фонового выполнения. Данное требование направлено на завершение этого фонового субъекта после периода бездействия пользователя, независимо от статуса субъекта.

L.3.4.2 Операции

L.3.4.2.1 Назначение

В FTA_SSL.3.1 автору ПЗ/ЗБ следует специфицировать интервал бездействия пользователя, по истечении которого произойдет блокирование сеанса. При желании автор ПЗ/ЗБ может использовать операцию назначения, чтобы возложить определение интервала времени на уполномоченного администратора или пользователя. Функции управления в классе FMT могут специфицировать возможность модификации этого интервала, задавая его значение по умолчанию.

L.4 Предупреждения перед предоставлением доступа к ОО (FTA_TAB)

L.4.1 Замечания для пользователя

Требования доступа к ОО предусматривают для ОО возможность еще до идентификации и аутентификации отобразить для потенциальных пользователей предупреждающее сообщение относительно характера использования ОО.

L.4.2 FTA_TAB.1 Предупреждения по умолчанию перед предоставлением доступа к ОО

L.4.2.1 Замечания по применению для пользователя

Компонент FTA_TAB.1содержит требование наличия предупреждающего сообщения о несанкционированном использовании ОО. Автор ПЗ/ЗБ может уточнить это требование с целью задания предупреждения по умолчанию.

L.5 История доступа к ОО (FTA_TAH)

L.5.1 Замечания для пользователя

Семейство FTA_TAH определяет требования к ФБО по отображению для пользователя, при успешном открытии сеанса, истории неуспешных попыток получить доступ от имени этого пользователя. Эта история может содержать дату, время, средства доступа и порт последнего успешного доступа к ОО, а также число неуспешных попыток доступа к ОО после последнего успешного доступа идентифицированного пользователя.

L.5.2 FTA_TAH.1 История доступа к ОО

L.5.2.1 Замечания по применению для пользователя

Компонент FTA_TAH.1 может предоставить уполномоченным пользователям информацию о возможном злоупотреблении их учетными данными.

Этот компонент содержит требование предоставления такой информации пользователю. Следует предоставить пользователю возможность просмотреть информацию, но не заставлять его делать это. При желании

пользователь может, например, создать командный файл для игнорирования этой информации и перехода к последующим действиям.

L.5.2.2 Операции

L.5.2.2.1 Выбор

В FTA_TAH.1.1 автору ПЗ/ЗБ следует выбрать атрибуты безопасности последнего успешного открытия сеанса, которые будут показаны через пользовательский интерфейс. К этим атрибутам относятся: дата, время, метод доступа (например протокол пересылки файлов) и/или место доступа (например терминал 50).

В FTA_TAH.1.2 автору ПЗ/ЗБ следует выбрать атрибуты безопасности последней неуспешной попытки открытия сеанса, которые будут показаны через пользовательский интерфейс. К этим атрибутам относятся: дата, время, метод доступа (например протокол пересылки файлов) и/или место доступа (например терминал 50).

L.6 Открытие сеанса с ОО (FTA_TSE)

L.6.1 Замечания для пользователя

Семейство FTA_TSE определяет требования по запрещению пользователям открытия сеанса с ОО на основе таких атрибутов, как место или порт доступа, атрибуты безопасности пользователя (например, идентификатора, уровня допуска, уровня целостности, принадлежности к роли), интервалы времени (например время суток, день недели, календарные даты) или сочетания параметров.

Это семейство предоставляет автору ПЗ/ЗБ возможность специфицировать требования к ФБО с целью установить ограничения на способность уполномоченного пользователя открывать сеанс с ОО. Идентификация соответствующих ограничений может быть выполнена с применением операции выбора. Примерами атрибутов, которые можно использовать для установки ограничений на открытие сеанса, являются:

a) место доступа может использоваться для ограничения способности пользователя открывать активный сеанс с ОО на основе места расположения пользователя или порта доступа. Эта возможность особенно рекомендуется при использовании телефонных линий или сетевых средств;

b) атрибуты безопасности пользователя могут использоваться для ограничения возможностей пользователя устанавливать активные сеансы с ОО. Например, запретить открытие сеанса можно на основе любого из следующих атрибутов пользователя:

- идентификатора;
- уровня допуска;
- уровня прав на модификацию данных (уровня целостности);
- принадлежности к роли.

Эта возможность особенно применима в случае, если авторизация или вход может происходить не в том месте, где выполняется проверка доступа к ОО;

c) время доступа может использоваться для ограничения возможности пользователя открыть активный сеанс с ОО на основе интервалов времени. Например, ограничения могут быть основаны на времени суток, дне недели, календарных датах. Это ограничение предоставляет определенную защиту от действий пользователя в то время, когда могут не применяться необходимые процедурные меры или мониторинг.

L.6.2 FTA_TSE.1 Открытие сеанса с ОО

L.6.2.1 Операции

L.6.2.1.1 Назначение

В FTA_TSE.1.1 автору ПЗ/ЗБ следует специфицировать атрибуты, которые могут быть использованы для ограничения открытия сеанса. Примеры возможных атрибутов: идентификатор пользователя, место доступа (например, не с удаленного терминала), время доступа (например, неурочное), метод доступа (например X-windows).

Федеральное агентство по техническому регулированию и метрологии

Приложение М
(обязательное)

Доверенный маршрут/канал (FTP)

Пользователям часто необходимо выполнять свои функции, непосредственно взаимодействуя с ФБО. Доверенный маршрут обеспечивает уверенность в том, что пользователь взаимодействует непосредственно с ФБО независимо от места своего расположения. Ответ пользователя через доверенный маршрут гарантирует, что недоверенные приложения не смогут перехватить или модифицировать сообщение пользователя. Со своей стороны, доверенные каналы являются одним из способов безопасной связи между ФБО и удаленными продуктами ИТ.

Взаимосвязи между различными типами передачи сообщений, которые могут иметь место в ОО или в сети из ОО и внешних сущностей ИТ (то есть передача в пределах ОО, передача между ФБО, импорт/экспорт из/в ОДФ), и различные формы доверенных маршрутов и каналов показаны на рисунке 2 (см. раздел 5).

Отсутствие доверенного маршрута может привести к нарушениям учета или управления доступом в средах с недоверенными приложениями. Эти приложения могут перехватить приватную информацию пользователя, такую как пароли, и выдавать себя за других пользователей, используя эту информацию. Как следствие, ответственность за любые действия в системе не может быть надежно связана с учитываемыми сущностями. Кроме того, эти приложения могут выводить ошибочную информацию на дисплеи не подозревающих об этом пользователей, что может привести к ошибочным действиям пользователей и, как следствие, к нарушению безопасности.

Декомпозиция класса FTP «Доверенный маршрут/канал» на составляющие его компоненты показана на рисунке М.1.

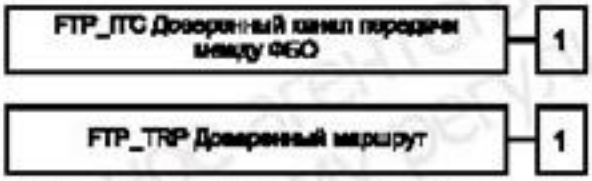

Рисунок М.1 — Декомпозиция класса FTP «Доверенный маршрут/канал»

М.1 Доверенный канал передачи между ФБО (FTP_ITC)

М.1.1 Замечания для пользователя

Семейство FTP_ITC определяет правила создания соединения через доверенный канал между ФБО и другими доверенными продуктами ИТ для выполнения операций, критичных для безопасности, между продуктами. Примером такой критичной для безопасности операции является обновление базы данных аутентификации ФБО посредством передачи данных от доверенного продукта, функцией которого является накопление данных аудита.

М.1.2 FTP_ITC.1 Доверенный канал передачи между ФБО

М.1.2.1 Замечания по применению для пользователя

Компонент FTP_ITC.1 следует использовать, если требуется доверенный канал передачи между ФБО и удаленным доверенным продуктом ИТ.

М.1.2.2 Операции

М.1.2.2.1 Выбор

В FTP_ITC.1.2 автору ПЗ/ЗБ следует специфицировать, должны ли локальные ФБО, удаленный доверенный продукт ИТ или все они иметь возможность инициировать доверенный канал.

М.1.2.2.2 Назначение

В FTP_ITC.1.3 автору ПЗ/ЗБ следует специфицировать функции, для которых требуется доверенный канал. К таким функциям могут относиться передача атрибутов безопасности пользователя, субъекта и/или объекта и обеспечение согласованности данных ФБО.

М.2 Доверенный маршрут (FTP_TRP)

М.2.1 Замечания для пользователя

Семейство FTP_TRP определяет требования установки и поддержания доверенной связи между пользователями и ФБО. Доверенный маршрут может потребоваться для любого связанного с безопасностью взаимодействия. Обмен по доверенному маршруту может быть инициирован пользователем при взаимодействии с ФБО, или же сами ФБО могут установить связь с пользователем по доверенному маршруту.

М.2.2 FTP_TRP.1 Доверенный маршрут

М.2.2.1 Замечания по применению пользователю

Компонент FTP_TRP.1 следует использовать, если требуется доверенная связь между пользователем и ФБО как для целей начальной аутентификации, так и для дополнительно специфицированных действий пользователя.

М.2.2.2 Операции

М.2.2.2.1 Выбор

В FPT_TRP.1.1 автору ПЗ/ЗБ следует специфицировать, необходимо ли предоставлять доверенный маршрут удаленным и/или локальным пользователям.

В FTP_TRP.1.2 автору ПЗ/ЗБ следует специфицировать, кому предоставлять возможность инициировать доверенный маршрут: ФБО, локальным пользователям и/или удаленным пользователям.

В FTP_TRP.1.3 автору ПЗ/ЗБ следует специфицировать, использовать ли доверенный маршрут для начальной аутентификации пользователя и/или для других специфицированных услуг.

М.2.2.2.2 Назначение

В FTP_TRP.1.3, если это выбрано, автору ПЗ/ЗБ следует идентифицировать (при необходимости) другие услуги, для которых требуется доверенный маршрут.

Приложение N
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица N.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 15408-1:2005	ГОСТ Р ИСО/МЭК 15408-1—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ИСО/МЭК 15408-2:2005	ГОСТ Р ИСО/МЭК 15408-2—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
ИСО/МЭК 15408-3:2005	ГОСТ Р ИСО/МЭК 15408-3—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

Федеральное агентство по техническому регулированию и метрологии

УДК 681.324:006.354 ОКС 35.040 П85

Ключевые слова: информационная технология, задание по безопасности, профиль защиты, объект оценки, критерии оценки безопасности, функция безопасности, функциональные требования безопасности

Федеральное агентство по техническому регулированию и метрологии

Редактор *В. Н. Копысов*
Технический редактор *В. Н. Прусакова*
Корректор *Е. Д. Дульнева*
Компьютерная верстка *А. П. Финогеновой*

Сдано в набор 12.03.2009. Подписано в печать 29.06.2009. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 20,00. Уч.-изд. л. 23,10. Тираж 278 экз. Зак. 501.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.