В.Л. Цирлов

Основы информационной безопасности автоматизированных систем

краткий курс

ISBN 978-5-222-13164-0

Феникс
2008

В книге рассматриваются основные теоретические построения, лежащие в основе современных систем обеспечения информационной безопасности. Приводятся основы теории информационной безопасности, элементы формальной теории защиты информации, а также основные оценочные и управленческие стандарты в области информационной безопасности.

Для студентов, изучающих теоретические основы информационной безопасности в рамках университетского курса, а также для широкого круга специалистов в области защиты информации.

СОДЕРЖАНИЕ

ПРИНЯТЫЕ СОКРАЩЕНИЯ И УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

АС – Автоматизированная система
ГОСТ – Государственный стандарт
ЗБ – Задание по безопасности
ИБ – Информационная безопасность
ИСО – Международная организация по стандартизации
ИТ – Информационные технологии
ЛВС – Локальная вычислительная сеть
МБО – Монитор безопасности обращений
МЭ – Межсетевой экран
МЭК – Международная электротехническая комиссия
НСД – Несанкционированный доступ
ОДФ – Область действия функций безопасности объекта оценки
ОК – Общие критерии
ОМО – Общая методология оценки
ОО – Объект оценки
ОУД – Оценочный уровень доверия
ПБО – Политика безопасности организации
ПЗ – Профиль защиты
ПО – Программное обеспечение
ПРД – Правила разграничения доступа
ПФБ – Политика функций безопасности
ПЭМИН – Побочные электромагнитные излучения и наводки
РД – Руководящий документ
СВТ – Средство вычислительной техники
СП – Сообщение о проблемах
СРД – Система разграничения доступа
СУБД – Система управления базами данных
СУИБ – Система управления информационной безопасностью
ТОО – Технический отчёт об оценке
УК – Управление конфигурацией
ФБО – Функции безопасности объекта оценки
ФСТЭК – Федеральная служба по техническому и экспортному контролю
BSI – British Standards Institution (Британский институт стандартов)
CDI – Constrained Data Items (Данные, целостность которых контролируется)
FO – Failover (Связь синхронизации)
IDS – Intrusion Detection System (Система обнаружения вторжений)
ISO – International Organization for Standardization (Международная организация по стандартизации)
IEC – International Electrotechnical Commission (Международная электротехническая комиссия)
IVP – Integrity Verification Procedure (Процедура проверки целостности)

MAC – Message Authentication Code (Код проверки подлинности)
OSI – Open Systems Interconnection (Взаимодействие открытых систем)
PDCA – Plan-Do-Check-Act (Планирование – Реализация – Оценка – Корректировка)
RAID – Redundant Array of Independent Discs (Избыточный массив независимых дисков)
SI – Simple Integrity (Простое правило целостности)
SS – Simple Security (Простое правило безопасности)
TP – Transformation Procedure (Процедура преобразования)
UDI – Unconstrained Data Items (Данные, целостность которых не контролируется)
◄ – Начало примера или доказательства
► – Конец примера или доказательства
[ ] – Ссылка на библиографические источники

Введение

Людям свойственно защищать свои секреты. Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё более и более актуальными – и одновременно более сложными.

Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности. Действительно, универсальных методов защиты не существует, во многом успех при построении механизмов безопасности для реальной системы будет зависеть от её индивидуальных особенностей, учёт которых плохо подаётся формализации. Поэтому часто информационную безопасность рассматривают как некую совокупность неформальных рекомендаций по построению систем защиты информации того или иного типа.

Однако всё обстоит несколько сложнее. За практическими приёмами построения систем защиты лежат общие закономерности, которые не зависят от технических особенностей их реализации. Такие универсальные принципы и делают информационную безопасность самостоятельной научной дисциплиной – и именно им посвящена данная книга.

Книга состоит из трёх частей. В первой части рассматриваются общие положения теории информационной безопасности и универсальные подходы к построению систем защиты от основных классов угроз – конфиденциальности, целостности и доступности информации. Во второй – основные положения формальной теории защиты информации: основные модели управления доступом и ряд сопутствующих вопросов. Третья часть посвящена стандартам информационной безопасности как одному из основных механизмов накопления и упорядочения знаний в данной области.

В приложениях приведены глоссарий терминов, используемых при работе с «Общими критериями», и пример задания по безопасности.

Книга написана в стиле lecture notes и полностью соответствует курсу лекций, который автор читает студентам кафедры «Информационная безопасность» МГТУ имени Н.Э. Баумана.

Часть 1. Основные положения теории информационной безопасности

1.1. Информационная безопасность. Основные определения

Термин «информация» разные науки определяют различными способами. Так, например, в философии информация рассматривается как свойство материальных объектов и процессов сохранять и порождать определённое состояние, которое в различных вещественно-энергетических формах может быть передано от одного объекта к другому. В кибернетике информацией принято называть меру устранения неопределённости. Мы же под ***информацией*** в дальнейшем будем понимать всё то, что может быть представлено в символах конечного (например, бинарного) алфавита.

> Такое определение может показаться несколько непривычным. В то же время оно естественным образом вытекает из базовых архитектурных принципов современной вычислительной техники. Действительно, мы ограничиваемся вопросами информационной безопасности автоматизированных систем – а всё то, что обрабатывается с помощью современной вычислительной техники, представляется в двоичном виде.

Предметом нашего рассмотрения являются автоматизированные системы. Под ***автоматизированной системой обработки информации*** (***АС***) [1] мы будем понимать совокупность следующих объектов:

1. средств вычислительной техники;
2. программного обеспечения;
3. каналов связи;
4. информации на различных носителях;
5. персонала и пользователей системы.

Информационная безопасность АС рассматривается как состояние системы, при котором:

1. Система способна противостоять дестабилизирующему воздействию внутренних и внешних угроз.
2. Функционирование и сам факт наличия системы не создают угроз для внешней среды и для элементов самой системы.

На практике информационная безопасность обычно рассматривается как совокупность следующих трёх **базовых свойств защищаемой информации** [2]:

- ***конфиденциальность***, означающая, что доступ к информации могут получить только легальные пользователи;
- ***целостность***, обеспечивающая, что во-первых, защищаемая информация может быть изменена только законными и имеющими соответствующие полномочия пользователями, а во-вторых, информация внутренне непротиворечива и (если данное свойство применимо) отражает реальное положение вещей;
- ***доступность***, гарантирующая беспрепятственный доступ к защищаемой информации для законных пользователей.

Деятельность, направленную на обеспечение информационной безопасности, принято называть ***защитой информации***.

Методы обеспечения информационной безопасности (см. рис. 1.1) весьма разнообразны.

Рис. 1.1. Основные методы обеспечения информационной безопасности

Сервисы сетевой безопасности представляют собой механизмы защиты информации, обрабатываемой в распределённых вычислительных системах и сетях. ***Инженерно–технические методы*** ставят своей целью обеспечение защиты информации от утечки по техническим каналам – например, за счёт перехвата электромагнитного излучения или речевой информации. ***Правовые и организационные методы защиты информации*** создают нормативную базу для организации различного рода деятельности, связанной с обеспечением информационной безопасности.

Теоретические методы обеспечения информационной безопасности [3], в свою очередь, решают две основных задачи. Первая из них – это формализация разного рода процессов, связанных с обеспечением информационной безопасности. Так, например, формальные модели управления доступом позволяют строго описать все возможные информационные потоки в системе – а значит, гарантировать выполнение требуемых свойств безопасности. Отсюда непосредственно вытекает вторая задача – строгое обоснование корректности и адекватности функционирования систем обеспечения информационной безопасности при проведении анализа их защищённости. Такая задача возникает, например, при проведении сертификации автоматизированных систем по требованиям безопасности информации.

1.2. Угрозы информационной безопасности

При формулировании определения информационной безопасности АС мы упоминали понятие угрозы. Остановимся на нём несколько подробнее.

Заметим, что в общем случае под ***угрозой*** [1] принято понимать потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. В свою очередь, ***угроза информационной безопасности автоматизированной системы*** - это возможность реализации воздействия на информацию, обрабатываемую в АС, приводящего к нарушению конфиденциальности, целостности или доступности этой информации, а также возможность воздействия на компоненты АС, приводящего к их утрате, уничтожению или сбою функционирования.

Классификация угроз может быть проведена по множеству признаков. Приведём наиболее распространённые из них.

1. ***По природе возникновения*** принято выделять естественные и искусственные угрозы. ***Естественными*** принято называть угрозы, возникшие в результате воздействия на АС объективных физических процессов или стихийных природных явлений, не зависящих от человека. В свою очередь, ***искусственные угрозы*** вызваны действием человеческого фактора.

   Примерами естественных угроз могут служить пожары, наводнения, цунами, землетрясения и т.д. Неприятная особенность таких угроз – чрезвычайная трудность или даже невозможность их прогнозирования.

2. ***По степени преднамеренности*** выделяют случайные и преднамеренные угрозы. ***Случайные*** угрозы бывают обусловлены халатностью или непреднамеренными ошибками персонала. ***Преднамеренные*** угрозы обычно возникают в результате направленной деятельности злоумышленника.

   В качестве примеров случайных угроз можно привести непреднамеренный ввод ошибочных данных, неумышленную порчу оборудования. Пример преднамеренной угрозы – проникновение злоумышленника на охраняемую территорию с нарушением установленных правил физического доступа.

3. В зависимости от ***источника угрозы*** принято выделять:
   - Угрозы, источником которых является ***природная среда***. Примеры таких угроз – пожары, наводнения и другие стихийные бедствия.
   - Угрозы, источником которых является ***человек***. Примером такой угрозы может служить внедрение агентов в ряды персонала АС со стороны конкурирующей организации.
   - Угрозы, источником которых являются ***санкционированные программно-аппаратные средства***. Пример такой угрозы – некомпетентное использование системных утилит.
   - Угрозы, источником которых являются ***несанкционированные программно-аппаратные средства***. К таким угрозам можно отнести, например, внедрение в систему кейлоггеров.
4. По ***положению источника угрозы выделяют***:
   - Угрозы, источник которых расположен ***вне контролируемой зоны***. Примеры таких угроз – перехват побочных электромагнитных излучений (ПЭМИН) или перехват данных, передаваемых по каналам связи; дистанционная фото- и видеосъёмка; перехват акустической информации с использованием направленных микрофонов.

- Угрозы, источник которых расположен ***в пределах контролируемой зоны***. Примерами подобных угроз могут служить применение подслушивающих устройств или хищение носителей, содержащих конфиденциальную информацию.

5. ***По степени .воздействия на АС*** выделяют пассивные и активные угрозы. ***Пассивные угрозы*** при реализации не осуществляют никаких изменений в составе и структуре АС. Реализация активных угроз, напротив, нарушает структуру автоматизированной системы.

   Примером пассивной угрозы может служить несанкционированное копирование файлов с данными.

6. ***По способу доступа к ресурсам АС*** выделяют:
   - Угрозы, ***использующие стандартный доступ***. Пример такой угрозы – несанкционированное получение пароля путём подкупа, шантажа, угроз или физического насилия по отношению к законному обладателю.
   - Угрозы, ***использующие нестандартный путь доступа***. Пример такой угрозы – использование недекларированных возможностей средств защиты.

Критерии классификации угроз можно продолжать, однако на практике чаще всего используется следующая **основная классификация угроз**, основывающаяся на трёх введённых ранее базовых свойствах защищаемой информации:

1. ***Угрозы нарушения конфиденциальности информации***, в результате реализации которых информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.
2. ***Угрозы нарушения целостности информации***, к которым относится любое злонамеренное искажение информации, обрабатываемой с использованием АС.
3. ***Угрозы нарушения доступности информации,*** возникающие в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется.

   Отметим, что реальные угрозы информационной безопасности далеко не всегда можно строго отнести к какой-то одной из перечисленных категорий. Так, например, угроза хищения носителей информации может быть при определённых условиях отнесена ко всем трём категориям.

Заметим, что перечисление угроз, характерных для той или иной автоматизированной системы, является важным этапом анализа уязвимостей АС, проводимого, например, в рамках аудита информационной безопасности, и создаёт базу для последующего проведения анализа рисков. Выделяют два основных **метода перечисления угроз**:

1. ***Построение произвольных списков угроз***. Возможные угрозы выявляются экспертным путём и фиксируются случайным и неструктурированным образом. Для данного подхода характерны неполнота и противоречивость получаемых результатов.
2. ***Построение деревьев угроз*** [4]. Угрозы описываются в виде одного или нескольких деревьев. Детализация угроз осуществляется сверху вниз, и в конечном итоге каждый лист дерева даёт описание конкретной угрозы. Между поддеревьями в случае необходимости могут быть организованы логические связи.

   Рассмотрим в качестве примера дерево угрозы блокирования доступа к сетевому приложению (рис. 1.2.).

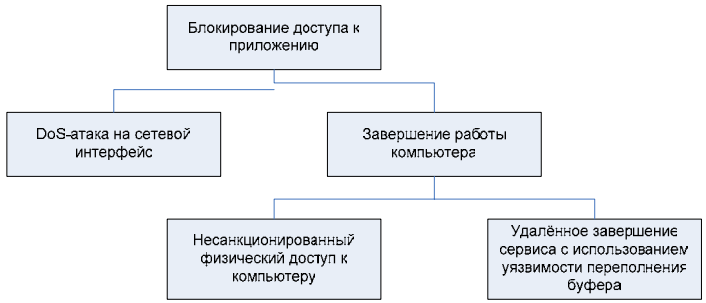

Рис. 1.2. Пример дерева угроз

Как видим, блокирование доступа к приложению может произойти либо в результате реализации DoS-атаки на сетевой интерфейс, либо в результате завершения работы компьютера. В свою очередь, завершение работы компьютера может произойти либо вследствие несанкционированного физического доступа злоумышленника к компьютеру, либо в результате использования злоумышленником уязвимости, реализующей атаку на переполнение буфера.

1.3. Построение систем защиты от угроз нарушения конфиденциальности информации

1.3.1. Модель системы защиты

При построении систем защиты от угроз нарушения конфиденциальности информации в автоматизированных системах используется комплексный подход. Схема традиционно выстраиваемой эшелонированной защиты приведена на рис. 1.3.1.

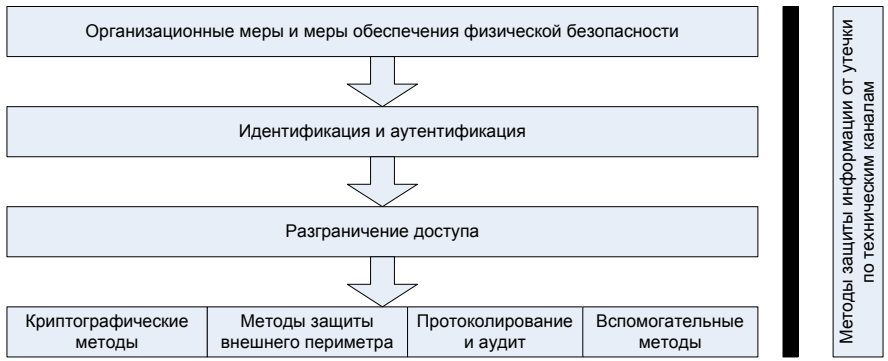

Рис. 1.3.1. Структура системы защиты от угроз нарушения конфиденциальности информации

Как видно из приведённой схемы, первичная защита осуществляется за счёт реализуемых организационных мер и механизмов контроля физического доступа к АС. В дальнейшем, на этапе контроля логического доступа, защита осуществляется с использованием различных сервисов сетевой безопасности. Во всех случаях параллельно должен быть развёрнут комплекс инженерно-технических средств защиты информации, перекрывающих возможность утечки по техническим каналам.

Остановимся более подробно на каждой из участвующих в реализации защиты подсистем.

1.3.2. Организационные меры и меры обеспечения физической безопасности

Данные механизмы в общем случае ***предусматривают*** [5]***:***

- развёртывание системы контроля и разграничения физического доступа к элементам автоматизированной системы.
- создание службы охраны и физической безопасности.
- организацию механизмов контроля за перемещением сотрудников и посетителей (с использованием систем видеонаблюдения, проксимити-карт и т.д.);
- разработку и внедрение регламентов, должностных инструкций и тому подобных регулирующих документов;
- регламентацию порядка работы с носителями, содержащими конфиденциальную информацию.

Не затрагивая логики функционирования АС, данные меры при корректной и адекватной их реализации являются крайне эффективным механизмом защиты и жизненно необходимы для обеспечения безопасности любой реальной системы.

1.3.3. Идентификация и аутентификация

Напомним, что под ***идентификацией*** [5] принято понимать присвоение субъектам доступа уникальных идентификаторов и сравнение таких идентификаторов с перечнем возможных. В свою очередь, ***аутентификация*** понимается как проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Тем самым, задача идентификации – ответить на вопрос «кто это?», а аутентификации - «а он ди это на самом деле?».

Базовая схема идентификации и аутентификации приведена на рис. 1.3.2.

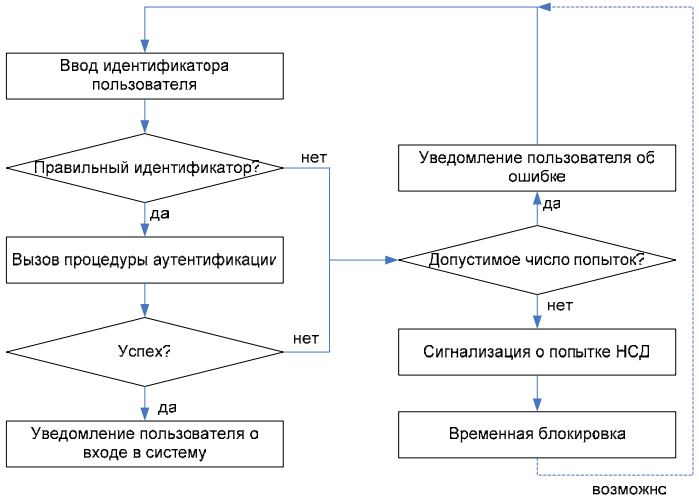

Рис. 1.3.2. Базовая схема идентификации и аутентификации

Приведённая схема учитывает возможные ошибки оператора при проведении процедуры аутентификации: если аутентификация не выполнена, но допустимое число попыток не превышено, пользователю предлагается пройти процедуру идентификации и аутентификации еще раз.

Всё множество использующих в настоящее время **методов аутентификации** можно разделить на 4 большие группы [6]:

1. ***Методы, основанные на знании некоторой секретной информации***. Классическим примером таких методов является ***парольная защита***, когда в качестве средства аутентификации пользователю предлагается ввести пароль – некоторую последовательность символов. Данные методы аутентификации являются наиболее распространёнными.
2. ***Методы, основанные на использовании уникального предмета.*** В качестве такого предмета могут быть использованы смарт-карта, токен, электронный ключ и т.д.
3. ***Методы, основанные на использовании биометрических характеристик человека***. На практике чаще всего используются одна или несколько из следующих биометрических характеристик:
   - отпечатки пальцев;
   - рисунок сетчатки или радужной оболочки глаза;
   - тепловой рисунок кисти руки;
   - фотография или тепловой рисунок лица;
   - почерк (роспись);
   - голос.

   Наибольшее распространение получили сканеры отпечатков пальцев и рисунков сетчатки и радужной оболочки глаза.
4. ***Методы, основанные на информации, ассоциированной с пользователем***. Примером такой информации могут служить координаты пользователя, определяемые при помощи GPS. Данный подход вряд ли может быть использован в качестве единственного механизма аутентификации, однако вполне допустим в качестве одного из нескольких совместно используемых механизмов.

Широко распространена практика совместного использования нескольких из перечисленных выше механизмов – в таких случаях говорят о ***многофакторной аутентификации***.

Особенности парольных систем аутентификации

При всём многообразии существующих механизмов аутентификации, наиболее распространённым из них остаётся парольная защита. Для этого есть несколько причин, из которых мы отметим следующие [6]:

- ***Относительная простота реализации***. Действительно, реализация механизма парольной защиты обычно не требует привлечения дополнительных аппаратных средств.
- ***Традиционность***. Механизмы парольной защиты являются привычными для большинства пользователей автоматизированных систем и не вызывают

психологического отторжения – в отличие, например, от сканеров рисунка сетчатки глаза.

В то же время для парольных систем защиты характерен парадокс, затрудняющий их эффективную реализацию: стойкие пароли мало пригодны для использования человеком. Действительно, стойкость пароля возникает по мере его усложнения; но чем сложнее пароль, тем труднее его запомнить, и у пользователя появляется искушение записать неудобный пароль, что создаёт дополнительные каналы для его дискредитации.

Остановимся более подробно на основных **угрозах безопасности парольных систем**. В общем случае пароль может быть получен злоумышленником одним из трёх основных способов:

1. ***За счёт использования слабостей человеческого фактора*** [7, 8]. Методы получения паролей здесь могут быть самыми разными: подглядывание, подслушивание, шантаж, угрозы, наконец, использование чужих учётных записей с разрешения их законных владельцев.
2. ***Путём подбора***. При этом используются следующие методы:
   - ***Полный перебор***. Данный метод позволяет подобрать любой пароль вне зависимости от его сложности, однако для стойкого пароля время, необходимое для данной атаки, должно значительно превышать допустимые временные ресурсы злоумышленника.
   - ***Подбор по словарю***. Значительная часть используемых на практике паролей представляет собой осмысленные слова или выражения. Существуют словари наиболее распространённых паролей, которые во многих случаях позволяют обойтись без полного перебора.
   - ***Подбор с использованием сведений о пользователе***. Данный интеллектуальный метод подбора паролей основывается на том факте, что если политика безопасности системы предусматривает самостоятельное назначение паролей пользователями, то в подавляющем большинстве случаев в качестве пароля будет выбрана некая персональная информация, связанная с пользователем АС. И хотя в качестве такой информации может быть выбрано что угодно, от дня рождения тёщи и до прозвища любимой собачки, наличие информации о пользователе позволяет проверить наиболее распространённые варианты (дни рождения, имена детей и т.д.).
3. ***За счёт использования недостатков реализации парольных систем***. К таким недостаткам реализации относятся эксплуатируемые уязвимости сетевых сервисов, реализующих те или иные компоненты парольной системы защиты, или же недекларированные возможности соответствующего программного или аппаратного обеспечения.

Рекомендации по практической реализации парольных систем

При построении системы парольной защиты необходимо учитывать специфику АС и руководствоваться результатами проведённого анализа рисков. В то же время можно привести следующие **практические рекомендации**:

- ***Установление минимальной длины пароля***. Очевидно, что регламентация минимально допустимой длины пароля затрудняет для злоумышленника реализацию подбора пароля путём полного перебора.
- ***Увеличение мощности алфавита паролей***. За счёт увеличения мощности (которое достигается, например, путём обязательного использования спецсимволов) также можно усложнить полный перебор.
- ***Проверка и отбраковка паролей по словарю***. Данный механизм позволяет затруднить подбор паролей по словарю за счёт отбраковки заведомо легко подбираемых паролей.
- ***Установка максимального срока действия пароля.*** Срок действия пароля ограничивает промежуток времени, который злоумышленник может затратить на подбор пароля. Тем самым, сокращение срока действия пароля уменьшает вероятность его успешного подбора.
- ***Установка минимального срока действия пароля.*** Данный механизм предотвращает попытки пользователя незамедлительно сменить новый пароль на предыдущий.
- ***Отбраковка по журналу истории паролей.*** Механизм предотвращает повторное использование паролей – возможно, ранее скомпрометированных.
- ***Ограничение числа попыток ввода пароля.*** Соответствующий механизм затрудняет интерактивный подбор паролей.
- ***Принудительная смена пароля при первом входе пользователя в систему.*** В случае, если первичную генерацию паролей для всех пользователь осуществляет администратор, пользователю может быть предложено сменить первоначальный пароль при первом же входе в систему – в этом случае новый пароль не будет известен администратору.
- ***Задержка при вводе неправильного пароля.*** Механизм препятствует интерактивному подбору паролей.
- ***Запрет на выбор пароля пользователем и автоматическая генерация пароля.*** Данный механизм позволяет гарантировать стойкость сгенерированных паролей – однако не стоит забывать, что в этом случае у пользователей неминуемо возникнут проблемы с запоминанием паролей.

Оценка стойкости парольных систем

Оценим элементарные взаимосвязи между основными параметрами парольных систем [1]. Введём следующие обозначения:

- A – мощность алфавита паролей;
- L – длина пароля;
- $S=A^L$ – мощность пространства паролей;
- V – скорость подбора паролей;
- T – срок действия пароля;
- P – вероятность подбора пароля в течение его срока действия.

Очевидно, что справедливо следующее соотношение:

$$P = \frac{V \cdot T}{S}.$$

Обычно скорость подбора паролей V и срок действия пароля T можно считать известными. В этом случае, задав допустимое значение вероятности P подбора пароля в

течение его срока действия, можно определить требуемую мощность пространства паролей S.

Заметим, что уменьшение скорости подбора паролей V уменьшает вероятность подбора пароля. Из этого, в частности, следует, что если подбор паролей осуществляется путём вычисления хэш-функции и сравнение результата с заданным значением, то большую стойкость парольной системы обеспечит применение медленной хэш-функции.

Методы хранения паролей

В общем случае возможны три **механизма хранения паролей в АС** [9]:

1. ***В открытом виде***. Безусловно, данный вариант не является оптимальным, поскольку автоматически создаёт множество каналов утечки парольной информации. Реальная необходимость хранения паролей в открытом виде встречается крайне редко, и обычно подобное решение является следствием некомпетентности разработчика.
2. ***В виде хэш-значения.*** Данный механизм удобен для проверки паролей, поскольку хэш-значения однозначно связаны с паролем, но при этом сами не представляют интереса для злоумышленника.
3. ***В зашифрованном виде.*** Пароли могут быть зашифрованы с использованием некоторого криптографического алгоритма, при этом ключ шифрования может храниться:
   - на одном из постоянных элементов системы;
   - на некотором носителе (электронный ключ, смарт-карта и т.п.), предъявляемом при инициализации системы;
   - ключ может генерироваться из некоторых других параметров безопасности АС – например, из пароля администратора при инициализации системы.

Передача паролей по сети

Наиболее распространены следующие варианты реализации:

1. ***Передача паролей в открытом виде***. Подход крайне уязвим, поскольку пароли могут быть перехвачены в каналах связи. Несмотря на это, множество используемых на практике сетевых протоколов (например, FTP) предполагают передачу паролей в открытом виде.
2. ***Передача паролей в виде хэш-значений*** иногда встречается на практике, однако обычно не имеет смысла – хэши паролей могут быть перехвачены и повторно переданы злоумышленником по каналу связи.
3. ***Передача паролей в зашифрованном виде*** в большинстве является наиболее разумным и оправданным вариантом.

1.3.4. Разграничение доступа

Под ***разграничением доступа*** [5] принято понимать установление полномочий субъектов для полследующего контроля санкционированного использования ресурсов, доступных в системе. Принято выделять два основных **метода разграничения доступа**: дискреционное и мандатное.

Дискреционным называется разграничение доступа между поименованными субъектами и поименованными объектами. На практике дискреционное разграничение

доступа может быть реализовано, например, с использованием ***матрицы доступа*** (рис. 1.3.4).

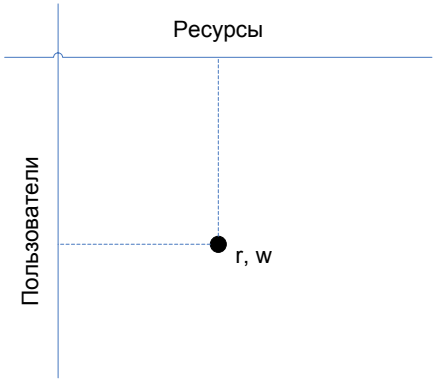

Рис. 1.3.4. Матрица доступа

Как видно из рисунка, матрица доступа определяет права доступа для каждого пользователя по отношению к каждому ресурсу.

Очевидно, что вместо матрицы доступа можно использовать списки полномочий: например, каждому пользователю может быть сопоставлен список доступных ему ресурсов с соответствующими правами, или же каждому ресурсу может быть сопоставлен список пользователей с указанием их прав на доступ к данному ресурсу.

Мандатное разграничение доступа обычно реализуется как разграничение доступа по уровням секретности. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. При этом все ресурсы АС должны быть классифицированы по уровням секретности.

Принципиальное различие между дискреционным и мандатным разграничением доступа состоит в следующем: если в случае дискреционного разграничения доступа права на доступ к ресурсу для пользователей определяет его владелец, то в случае мандатного разграничения доступа уровни секретности задаются извне, и владелец ресурса не может оказать на них влияния. Сам термин «мандатное» является неудачным переводом слова mandatory – «обязательный». Тем самым, мандатное разграничение доступа следует понимать как принудительное.

1.3.5. Криптографические методы обеспечения конфиденциальности информации

В целях обеспечения конфиденциальности информации используются следующие криптографические примитивы [10]:

1. Симметричные криптосистемы.

В симметричных криптосистемах для зашифрования и расшифрования информации используется один и тот же общий секретный ключ, которым взаимодействующие стороны предварительно обмениваются по некоторому защищённому каналу (рис. 1.3.5.1).

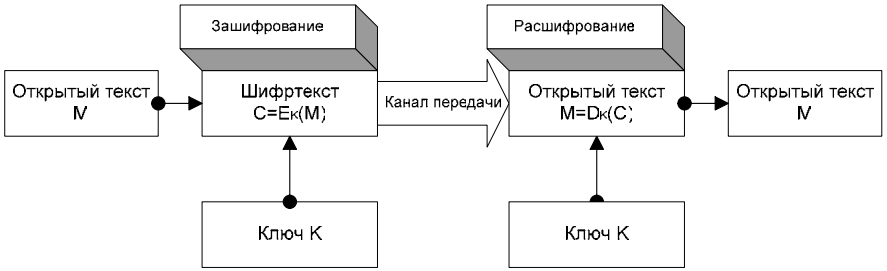

Рис. 1.3.5.1. Структура симметричной криптосистемы

В качестве примеров симметричных криптосистем можно привести отечественный алгоритм *ГОСТ 28147-89*, а также международные стандарты *DES* и пришедший ему на смену *AES*.

2. Асимметричные криптосистемы.

Асимметричные криптосистемы характерны тем, что в них используются различные ключи для зашифрования и расшифрования информации. Ключ для зашифрования (***открытый ключ***) можно сделать общедоступным, с тем чтобы любой желающий мог зашифровать сообщение для некоторого получателя. Получатель же, являясь единственным обладателем ключа для расшифрования (***секретный ключ),*** будет единственным, кто сможет расшифровать зашифрованные для него сообщения. Данный механизм проиллюстрирован на рисунке 1.3.5.2.

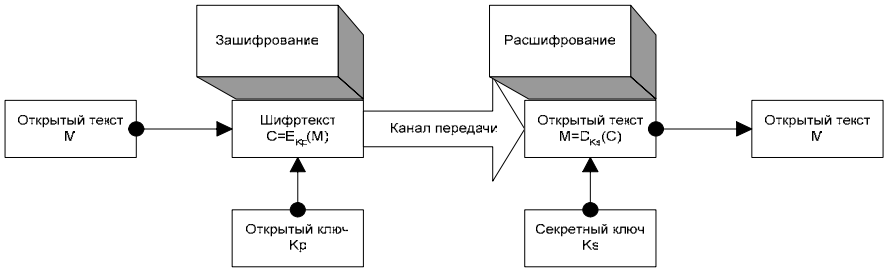

Рис. 1.3.5.2. Структура асимметричной криптосистемы

Примеры асимметричных криптосистем – *RSA* и *схема Эль-Гамаля*.

Симметричные и асимметричные криптосистемы, а также различные их комбинации используются в АС прежде всего для шифрования данных на различных носителях и для шифрования трафика.

1.3.6. Методы защиты внешнего периметра

Подсистема защиты внешнего периметра автоматизированной системы обычно включает в себя два основных механизма: средства межсетевого экранирования и средства обнаружения вторжений. Решая родственные задачи, эти механизмы часто

реализуются в рамках одного продукта и функционируют в качестве единого целого. В то же время каждый из механизмов является самодостаточным и заслуживает отдельного рассмотрения.

Межсетевое экранирование

Межсетевой экран (МЭ) [11] выполняет функции разграничения информационных потоков на границе защищаемой автоматизированной системы. Это позволяет:

- повысить безопасность объектов внутренней среды за счёт игнорирования неавторизованных запросов из внешней среды;
- контролировать информационные потоки во внешнюю среду;
- обеспечить регистрацию процессов информационного обмена.

Контроль информационных потоков производится посредством ***фильтрации информации***, т.е. анализа её по совокупности критериев и принятия решения о распространении в АС или из АС.

В зависимости от принципов функционирования, выделяют несколько ***классов межсетевых экранов***. Основным классификационным признаком является уровень модели ISO/OSI, на котором функционирует МЭ.

1. Фильтры пакетов.

Простейший класс межсетевых экранов, работающих на сетевом и транспортном уровнях модели ISO/OSI. Фильтрация пакетов обычно осуществляется по следующим критериям:

- IP-адрес источника;
- IP-адрес получателя;
- порт источника;
- порт получателя;
- специфические параметры заголовков сетевых пакетов.

Фильтрация реализуется путём сравнения перечисленных параметров заголовков сетевых пакетов с базой правил фильтрации.

2. Шлюзы сеансового уровня

Данные межсетевые экраны работают на сеансовом уровне модели ISO/OSI. В отличие от фильтров пакетов, они могут контролировать допустимость сеанса связи, анализируя параметры протоколов сеансового уровня.

3. Шлюзы прикладного уровня

Межсетевые экраны данного класса позволяют фильтровать отдельные виды команд или наборы данных в протоколах прикладного уровня. Для этого используются ***прокси-сервисы*** – программы специального назначения, управляющие трафиком через межсетевой экран для определённых высокоуровневых протоколов (http, ftp, telnet и т.д.).

Порядок использования прокси-сервисов показан на рис. 1.3.6.1.

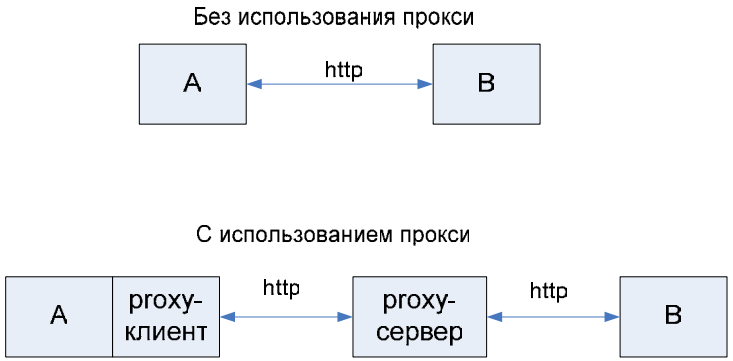

Рис. 1.3.6.1. Использование прокси-сервисов

Если без использование прокси-сервисов сетевое соединение устанавливается между взаимодействующими сторонами *A* и *B* напрямую, то в случае использования прокси-сервиса появляется посредник – ***прокси-сервер***, который самостоятельно взаимодействует со вторым участником информационного обмена. Такая схема позволяет контролировать допустимость использования отдельных команд протоколов высокого уровня, а также фильтровать данные, получаемые прокси-сервером извне; при этом прокси-сервер на основании установленных политик может принимать решение о возможности или невозможности передачи этих данных клиенту *A*.

4. Межсетевые экраны экспертного уровня.

Наиболее сложные межсетевые экраны, сочетающие в себе элементы всех трёх приведённых выше категорий. Вместо прокси-сервисов в таких экранах используются алгоритмы распознавания и обработки данных на уровне приложений.

Большинство используемых в настоящее время межсетевых экранов относятся к категории экспертных. Наиболее известные и распространённые МЭ – *CISCO PIX* и *CheckPoint FireWall-1*.

Системы обнаружения вторжений

Обнаружение вторжений представляет собой процесс выявления несанкционированного доступа (или попыток несанкционированного доступа) к ресурсам автоматизированной системы. ***Система обнаружения вторжений*** (Intrusion Detection System, IDS) [12] в общем случае представляет собой программно-аппаратный комплекс, решающий данную задачу.

Общая структура IDS приведена на рис. 1.3.6.2:

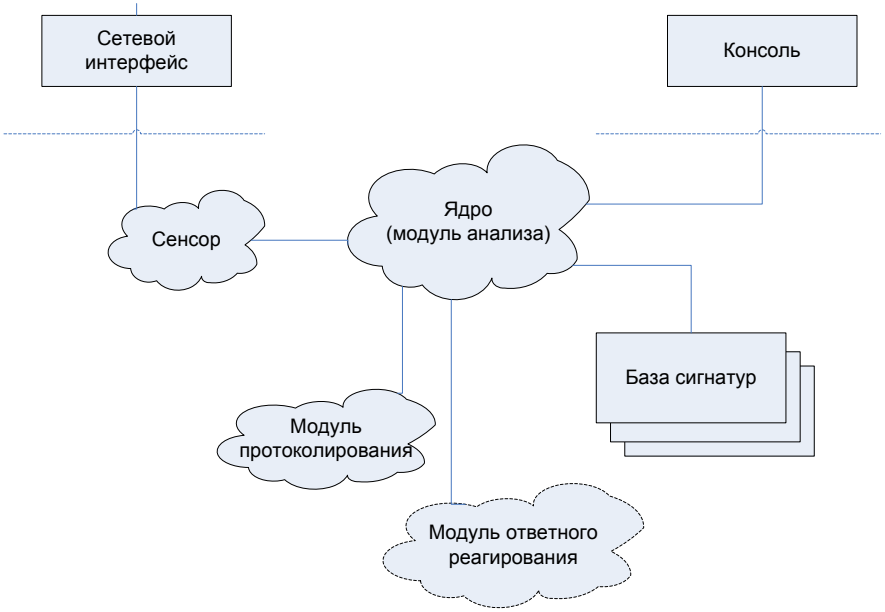

Рис. 1.3.6.2. Структурная схема IDS

Алгоритм функционирования системы IDS приведён на рис. 1.3.6.3:

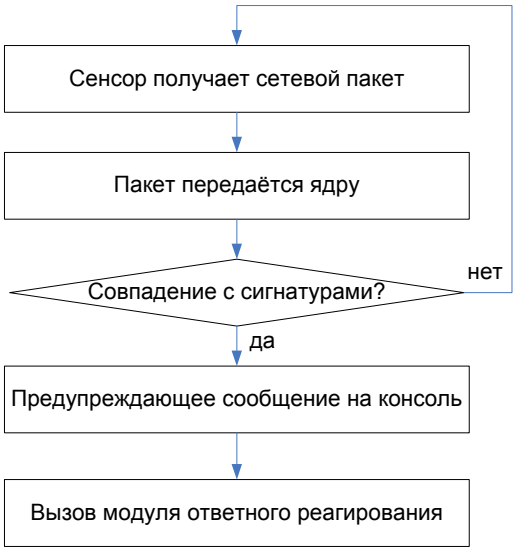

Рис. 1.3.6. Алгоритм функционирования IDS

Как видно из рисунков, функционирование систем IDS во многом аналогично межсетевым экранам: сенсоры получают сетевой трафик, а ядро путём сравнения полученного трафика с записями имеющейся базы сигнатур атак пытается выявить следы попыток несанкционированного доступа. Модуль ответного реагирования представляет собой опциональный компонент, который может быть использован для оперативного блокирования угрозы: например, может быть сформировано правило для межсетевого экрана, блокирующее источник нападения.

Существуют две основных **категории систем IDS**:

1. ***IDS уровня сети***.

   В таких системах сенсор функционирует на выделенном для этих целей хосте в защищаемом сегменте сети. Обычно сетевой адаптер данного хоста функционирует в режиме прослушивания (promiscuous mode), что позволяет анализировать весь проходящий в сегменте сетевой трафик.

2. IDS уровня хоста.

   В случае, если сенсор функционирует на уровне хоста, для анализа может быть использована следующая информация:

   - записи стандартных средств протоколирования операционной системы;
   - информация об используемых ресурсах;
   - профили ожидаемого поведения пользователей.

Каждый из типов IDS имеет свои достоинства и недостатки. IDS уровня сети не снижают общую производительность системы, однако IDS уровня хоста более эффективно выявляют атаки и позволяют анализировать активность, связанную с отдельным хостом. На практике целесообразно использовать системы, совмещающие оба описанных подхода.

Существуют разработки, направленные на использование в системах IDS методов искусственного интеллекта. Стоит отметить, что в настоящее время коммерческие продукты не содержат таких механизмов.

1.3.7. Протоколирование и аудит

Подсистема протоколирования и аудита [5] является обязательным компонентом любой АС. ***Протоколирование***, или ***регистрация,*** представляет собой механизм подотчётности системы обеспечения информационной безопасности, фиксирующий все события, относящиеся к вопросам безопасности. В свою очередь, ***аудит*** – это анализ протоколируемой информации с целью оперативного выявления и предотвращения нарушений режима информационной безопасности.

Системы обнаружения вторжений уровня хоста можно рассматривать как системы активного аудита.

Назначение механизма регистрации и аудита:

- обеспечение подотчётности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий (что бывает необходимо, например, при расследовании инцидентов, связанных с информационной безопасностью);
- обнаружение попыток нарушения информационной безопасности;
- предоставление информации для выявления и анализа технических проблем, не связанных с безопасностью.

Протоколируемые данные помещаются в ***регистрационный журнал***, который представляет собой хронологически упорядоченную совокупность записей результатов деятельности субъектов АС, достаточную для восстановления, просмотра и анализа последовательности действий с целью контроля конечного результата.

Типовая запись регистрационного журнала выглядит следующим образом (рис. 1.3.7.1).

Рис. 1.3.7.1. Типовая запись регистрационного журнала

Поскольку системные журналы являются основным источником информации для последующего аудита и выявления нарушений безопасности, вопросу защиты системных журналов от несанкционированной модификации должно уделяться самое пристальное внимание. Система протоколирования должна быть спроектирована таким образом, чтобы ни один пользователь (включая администраторов!) не мог произвольным образом модифицировать записи системных журналов.

Не менее важен вопрос о порядке хранения системных журналов. Поскольку файлы журналов хранятся на том или ином носителе, неизбежно возникает проблема переполнения максимально допустимого объёма системного журнала. При этом реакция системы может быть различной, например:

- система может быть заблокирована вплоть до решения проблемы с доступным дисковым пространством;
- могут быть автоматически удалены самые старые записи системных журналов;
- система может продолжить функционирование, временно приостановив протоколирование информации.

Безусловно, последний вариант в большинстве случаев является неприемлемым, и порядок хранения системных журналов должен быть чётко регламентирован в политике безопасности организации.

1.4. Построение систем защиты от угроз нарушения целостности

1.4.1. Принципы обеспечения целостности

Большинство механизмов, реализующих защиту информации от угроз нарушения конфиденциальности, в той или иной степени способствуют обеспечению целостности информации. В данном разделе мы остановимся более подробно на механизмах, специфичных для подсистемы обеспечения целостности.

Сформулируем для начала **основные принципы обеспечения целостности**, сформулированные Кларком и Вилсоном [13]:

1. ***Корректность транзакций.***

   Принцип требует обеспечения невозможности произвольной модификации данных пользователем. Данные должны модифицироваться исключительно таким образом, чтобы обеспечивалось сохранение их целостности.

2. ***Аутентификация пользователей.***

   Изменение данных может осуществляться только аутентифицированными для выполнения соответствующих действий пользователями.

3. ***Минимизация привилегий.***

Процессы должны быть наделены теми и только теми привилегиями в АС, которые минимально достаточны для их выполнения.

4. ***Разделение обязанностей.***
   Для выполнения критических или необратимых операций требуется участие нескольких независимых пользователей.
   На практике разделение обязанностей может быть реализовано либо исключительно организационными методами, либо с использованием криптографических схем разделения секрета.
5. ***Аудит произошедших событий.***
   Данный принцип требует создания механизма подотчётности пользователей, позволяющего отследить моменты нарушения целостности информации.
6. ***Объективный контроль.***
   Необходимо реализовать оперативное выделение данных, контроль целостности которых является оправданным.
   Действительно, в большинстве случаев строго контролировать целостность всех данных, присутствующих в системе, нецелесообразно хотя бы из соображений производительности: контроль целостности является крайне ресурсоёмкой операцией.
7. ***Управление передачей привилегий.***
   Порядок передачи привилегий должен полностью соответствовать организационной структуре предприятия.

Перечисленные принципы позволяют сформировать общую структуру системы защиты от угроз нарушения целостности (рис. 1.4.1).

Рис. 1.4.1. Структура системы защиты от угроз нарушения целостности

Как видно из рис. 1.4.1, принципиально новыми по сравнению с сервисами, применявшимися для построения системы защиты от угроз нарушения конфиденциальности, являются криптографические механизмы обеспечения целостности. Отметим, что механизмы обеспечения корректности транзакций также могут включать в семя криптографические примитивы.

1.4.2. Криптографические методы обеспечения целостности информации

При построении систем защиты от угроз нарушения целостности информации используются следующие криптографические примитивы [10]:

- цифровые подписи;
- криптографические хэш-функции;
- коды проверки подлинности.

Цифровые подписи

Цифровая подпись [14, 15] представляет собой механизм подтверждения подлинности и целостности цифровых документов. Во многом она является аналогом рукописной подписи – в частности, к ней предъявляются практически аналогичные **требования**:

1. Цифровая подпись должна позволять доказать, что именно законный автор, и никто другой, сознательно подписал документ.
2. Цифровая подпись должна представлять собой неотъемлемую часть документа. Должно быть невозможно отделить подпись от документа и использовать её для подписывания других документов.
3. Цифровая подпись должна обеспечивать невозможность изменения подписанного документа (в том числе и для самого автора!).
4. Факт подписывания документа должен быть юридически доказуемым. Должен быть невозможным отказ от авторства подписанного документа.

В простейшем случае для реализации цифровой подписи может быть использован механизм, аналогичный асимметричной криптосистеме. Разница будет состоять в том, что для зашифрования (являющегося в данном случае подписыванием) будет использован секретный ключ, а для расшиврования, играющего роль проверки подписи, - общеизвестный открытый ключ (рис. 1.4.2.1).

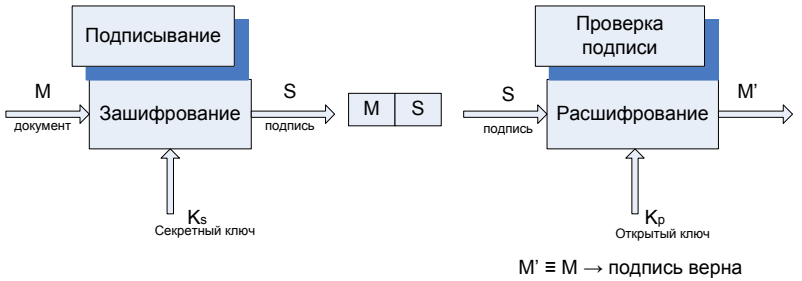

Рис. 1.4.2.1. Реализация механизма цифровой подписи

Порядок использования цифровой подписи в данном случае будет следующим:

1. Документ зашифровывается секретным ключом подписывающего, и зашифрованная копия распространяется вместе с оригиналом документа в качестве цифровой подписи.
2. Получатель, используя общедоступный открытый ключ подписывающего, расшифровывает подпись, сличает её с оригиналом и убеждается, что подпись верна.

Нетрудно убедиться, что данная реализация цифровой подписи полностью удовлетворяет всем приведённым выше требованиям, но в то же время имеет принципиальный недостаток: объём передаваемого сообщения возрастает как минимум в два раза. Избавиться от этого недостатка позволяет использование хэш-функций.

Криптографические хэш-функции

Функция вида *y=f(x)* называется ***криптографической хэш-функцией*** [15], если она удовлетворяет следующим свойствам:

1. На вход хэш-функции может поступать последовательность данных произвольной длины, результат же (называемый ***хэш***, или ***дайджест***) имеет фиксированную длину.
2. Значение *y* по имеющемуся значению *x* вычисляется за полиномиальное время, а значение *x* по имеющемуся значению *y* почти во всех случаях вычислить невозможно.
3. Вычислительно невозможно найти два входных значения хэш-функции, дающие идентичные хэши.
4. При вычислении хэша используется вся информация входной последовательности.
5. Описание функции является открытым и общедоступным.

Покажем, как хэш-функции могут быть использованы в схемах цифровой подписи. Если подписывать не само сообщение, а его хэш, то можно значительно сократить объём передаваемых данных. Схема подобной реализации приведена на рис. 1.4.2.2.

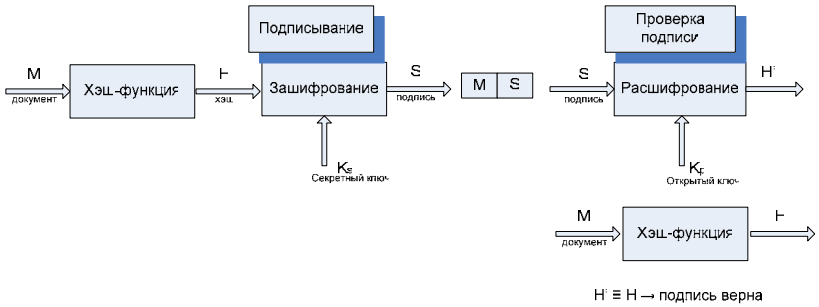

Рис. 1.4.2.2. Цифровая подпись, использующая хэш-функцию

Подписав вместо исходного сообщения его хэш, мы передаём результат вместе с исходным сообщением. Получатель расшифровывает подпись и сравнивает полученный

результат с хэшем сообщения. В случае совпадения делается вывод о том, что подпись верна.

Коды проверки подлинности

Часто криптографические хэш-функции используются в качестве средств контрольного суммирования: например, для некоторого файла, помещённого в публичный доступ на ftp-сервере, может быть приведён его хэш, подсчитанный с использованием некоторого алгоритма (чаще всего в таких случаях используется алгоритм md5). В этом случае пользователь, скачавший данный файл, может убедиться в его подлинности,

Однако в этом случае злоумышленник может подменить файл и привести хэш, соответствующий новому файлу – выявить подобные манипуляции, используя обычные хэш-функции, невозможно. Защита от подобного рода атак обеспечивается путём применения кодов проверки подлинности.

Коды проверки подлинности, или ***MAC-коды*** [15], представляют собой криптографические хэш-функции, для вычисления которых необходимо знать секретный ключ. Использование ключа позволяет гарантировать невозможность подмены защищаемых объектов, аналогичной приведённой выше: злоумышленник, не знающий секретного ключа, не сможет пересчитать хэш для нового файла.

В качестве кодов проверки подлинности часто используются модификации симметричных криптографических систем.

1.5. Построение систем защиты от угроз нарушения доступности

В общем случае обеспечение защиты от угроз нарушения доступности информации реализуется путём создания той или иной избыточности [2]. Структурная схема системы защиты от угроз нарушения доступности приведена на рис. 1.5.1.

Рис. 1.5.1. Структура системы защиты от угроз нарушения доступности

Дублирование каналов связи может осуществляться как в пределах автоматизированной системы, так и в отношении каналов, связывающих АС с внешней средой (например, путём использования каналов доступа к Internet от нескольких независимых провайдеров).

Дублирование шлюзов и межсетевых экранов позволяет избежать ситуации, когда связность АС нарушается из-за неисправности узла, представляющего собой «узкое место» - единую точку входа для всего трафика. Дублирование может осуществляться, например, следующим образом (рис. 1.5.2).

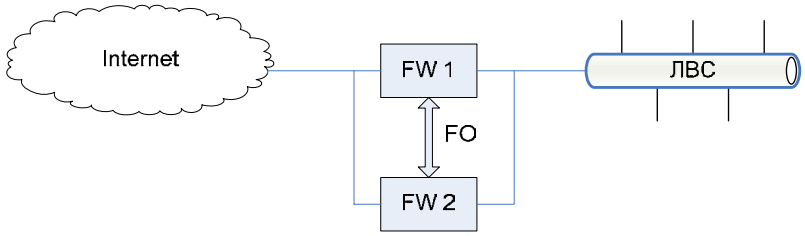

Рис. 1.5.2. Дублирование шлюзов и межсетевых экранов

В схеме на рис. 1.5.2. в нормальных условиях функционирования работает межсетевой экран *FW 1*. Связь *FO* (failover) обеспечивает непрерывную синхронизацию *FW 2* с *FW 1*, и в случае сбоя *FW 1* всё управление берёт на себя *FW 2*.

Резервное копирование информации является одним из важнейших механизмов, обеспечивающих её доступность и целостность. Используются следующие **методы резервного копирования**:

1. ***Полное /full/***. В этом случае все без исключения файлы, потенциально подвергаемые резервному копированию, переносятся на резервный носитель.
2. ***Инкрементальное /incremental/.*** Резервному копированию подвергаются только файлы, изменённые с момента последнего инкрементального копирования.
3. ***Дифференциальное /differential/.*** Копируются файлы, изменённые с момента полного резервного копирования. Количество копируемых данных в этом случае с каждым разом возрастает.

На практике резервное копирование обычно осуществляется следующим образом: периодически проводится полное резервное копирование, в промежутках - инкрементальное или дифференциальное. Выбор между дифференциальным и инкрементальным резервным копированием осуществляется с учётом требуемых характеристик подсистемы резервного копирования: инкрементальное копирование выполняется быстрее, однако в случае дифференциального копирования легче восстановить оригинал по резервной копии.

Использование ***RAID-массивов*** решает задачу оптимального (с точки зрения надёжности и производительности) распределения данных по нескольким дисковым накопителям. Выделяют следующие типы RAID-массивов:

- ***Уровень 0***.
  В данном случае несколько дисков представляются как один виртуальный диск. Защита от сбоев на данном уровне никак не обеспечивается.
- ***Уровень 1.***
  Реализуется ***зеркалирование*** – идентичные данные хранятся на нескольких (обычно на двух) дисках. Данный вариант обеспечивает надёжную защиту от сбоев носителя, однако является чрезвычайно неэффективным.
- ***Уровень 2***
  Биты данных поочерёдно размещаются на различных дисках; имеются выделенные диски, содержащие контрольные суммы. Для контроля ошибок используется код Хэмминга. Всего используется 39 дисков: 32 с данными и 7 с контрольными суммами. На практике данный уровень используется крайне редко.
- ***Уровни 3,4***
  Байты или блоки данных записываются на различные диски, биты чётности – на выделенный диск.
- ***Уровень 5***
  Данные и контрольные суммы распределяются по всем дискам. Достоинство данного подхода состоит в том, что возможно одновременное выполнение нескольких операций чтения или записи, что значительно повышает общую производительность системы.
- ***Уровень 7***
  Функционирование аналогично массивам уровня 5, дополнительно на аппаратном уровне реализовано представление массива в виде единого виртуального диска.

Иногда на практике используются и другие уровни RAID, представляющие собой нестандартизованные комбинации выше перечисленных.

Зеркалирование серверов в целом аналогично зеркалированию дисковых накопителей: идентичные данные в целях защиты от сбоев оборудования записываются на два независимых сервера. Речь в данном случае идёт исключительно о хранении данных.

Дублирование серверов, в свою очередь, позволяет обеспечить полноценную замену сервера в случае его сбоя за счёт передачи управления резервному серверу (рис. 1.5.3).

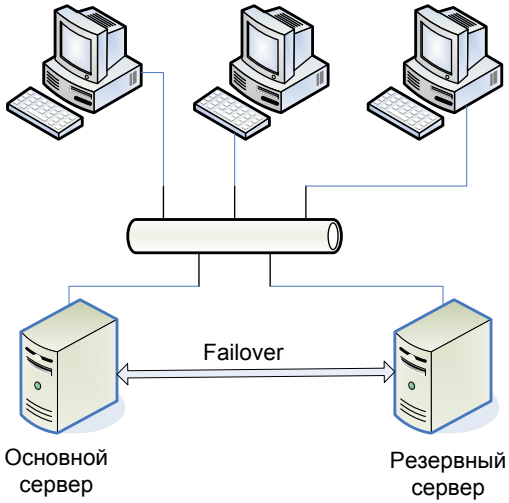

Рис. 1.5.3. Дублирование серверов

В случае отказа основного сервера, резервный сервер, постоянно синхронизирующийся с основным с использованием failover-связи, оперативно перехватит управление.

Использование кластеров позволяет наиболее эффективно обеспечить балансировку нагрузки между нескольким серверами. ***Кластером*** называется группа независимых серверов, управляемых как единая система. В отличие от механизма дублирования, в данном случае все серверы являются активными и принимают полноценное участие в обслуживании запросов клиентов.

Механизмы ***избыточной маршрутизации*** позволяют за счёт использования избыточных маршрутизаторов и дополнительных соединений гарантировать возможность передачи информации за пределы АС в случае недоступности части маршрутов.

Вопросы ***надёжности оборудования*** в общем случае решаются с привлечением методов теории надёжности. Стоит отметить, что оценка надёжности аппаратных средств вычислительной техники плохо поддаётся формализации, и выбор требуемых механизмов обеспечения надёжности (а это прежде всего резервирование и дублирование аппаратуры) осуществляется исходя из наихудших сценариев возможного развития событий.

1.6. Выводы

Рассмотренные нами в данном разделе механизмы построения защиты от угроз нарушения конфиденциальности, целостности и доступности информации достаточно универсальны, чтобы быть применимыми для большинства автоматизированных систем, однако являются описательными и носят неформальный характер. В дальнейшем изложении мы покажем, как можно строго формализовать некоторые из механизмов обеспечения информационной безопасности.

Часть 2. Основы формальной теории защиты информации

2.1. Основные определения

Введём некоторые обозначения [3]. Пусть A – конечный алфавит, A^* - множество слов конечной длины в алфавите A, $L \subset A^*$ - ***язык***, т.е. множество слов, выделенных по определённым правилам из A^*.

Аксиома 1. *Любая информация в автоматизированной системе представляется словом в некотором языке L.*

Назовём ***объектом*** относительно языка L произвольное конечное множество слов языка L. Очевидно, что в качестве объектов можно рассматривать многие сущности, входящие в состав АС. Например, текстовый файл представляет собой объект, поскольку в произвольный момент времени в него может быть записана некая последовательность символов, которая в общем случае будет представлять собой одно из конечного множества слов L над некоторым алфавитом A. Аналогично может быть составлен язык, описывающий клавиатуру и её состояния в произвольный момент времени. Языком описания клавиатуры можно считать множество возможных её состояний.

Преобразованием информации мы будем называть отображение, заданное на множестве слов языка L. Другими словами, преобразование отображает слово, описывающее исходные данные, в другое слово. Заметим, что само описание преобразования при этом также является словом. Примером преобразования может служить программа, написанная на некотором языке программирования.

Заметим, что программа может либо выполняться, либо просто храниться в файле на некотором носителе. Аналогично, **преобразование может**:

- ***храниться*** – в этом случае описание преобразования хранится в некотором объекте и ничем не отличается от других данных;
- ***действовать*** – преобразование может взаимодействовать с некоторыми ресурсами АС.

Ресурсы системы, выделенные для действия преобразования, принято называть ***доменом***. Чтобы инициировать действие преобразования, ему надо придать определённый статус – передать управление. Преобразование, которому передано управление, называется ***процессом***. В свою очередь, объект, описывающий преобразование, которому выделен домен и передано управление, называется ***субъектом***.

Субъект для реализации преобразования использует информацию, содержащуюся в объекте, т.е. осуществляет ***доступ*** к объекту. Существуют два основных вида доступа:

1. ***Чтение.***
   Если субъект S получает доступ к объекту O на чтение, то это означает, что производится перенос информации от объекта O к субъекту S – иначе говоря, возникает ***информационный поток*** от O к S (рис. 2.1.1).

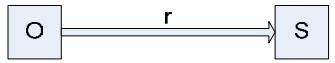

Рис. 2.1.1. Информационный поток от O к S

2. ***Запись.***
   Если субъект *S* получает доступ к объекту *O* на запись, то производится перенос информации от субъекта *S* к объекту *O*, т.е. возникает информационный поток от *S* к *O* (рис. 2.1.2).

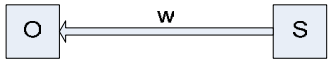

Рис. 2.1.2. Информационный поток от S к O

Данные два вида доступа являются базовыми. Существуют и более сложные варианты – например, активизация процесса, когда субъект *S* получает доступ к объекту *O* на активизацию процесса, записанного в *O* в виде данных. В этом случае для преобразования, описанного в *O*, формируется домен, и этому преобразованию передаётся управление.

Заметим, что любой субъект сам является объектом относительно некоторого языка. Поэтому если *S* – множество всех субъектов в системе, а *O* – множество всех объектов, то $S \subseteq O$.

Сформулированные утверждения позволяют сформировать базовую аксиому, лежащую в основе всей формальной теории защиты информации.

Аксиома 2. *Все вопросы безопасности информации описываются доступами субъектов к объектам*.

В дальнейшем изложении мы всюду будем иметь в виду это утверждение. Безусловно, данный подход сужает применимость формальной теории, поскольку принципиально ограничивается исключительно вопросами архитектуры систем безопасности, оставляя за рамками специфику их реализации.

2.2. Монитор безопасности обращений

Концепция монитора безопасности обращений является достаточно естественной формализацией некого механизма, реализующего разграничение доступа в системе. ***Монитор безопасности обращений*** (МБО) [3] представляет собой фильтр, который разрешает или запрещает доступ, основываясь на установленных в системе правилах разграничения доступа (рис. 2.2).

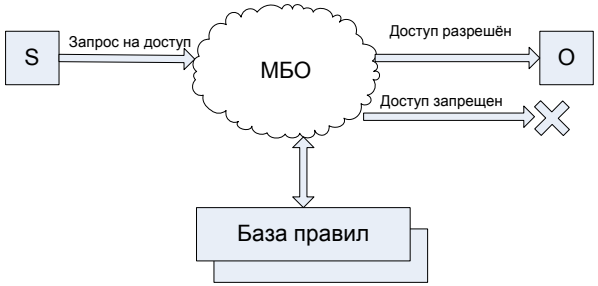

Рис. 2.2. Монитор безопасности обращений

Получив запрос на доступ от субъекта *S* к объекту *O*, монитор безопасности обращений нализирует базу правил, соответствующую установленной в системе политике безопасности, и либо разрешает, либо запрещает доступ.

Монитор безопасности обращений удовлетворяет следующим **свойствам**:

1. Ни один запрос на доступ субъекта к объекту не должен выполняться в обход МБО.
2. Работа МБО должна быть защищена от постороннего вмешательства.
3. Представление МБО должно быть достаточно простым для возможности верификации корректности его работы.

Несмотря на то, что концепция монитора безопасности обращений является абстракцией, перечисленные свойства справедливы и для программных или аппаратных модулей, реализующих функции монитора обращений в реальных системах.

2.3. Формальные модели управления доступом

2.3.1. Модель Харрисона-Руззо-Ульмана

Разработанная в 1971 г. ***модель Харрисона-Руззо-Ульмана*** [16] формализует упоминавшееся ранее понятие ***матрицы доступа*** – таблицы, описывающей права доступа субъектов к объектам (рис. 2.3.1.1).

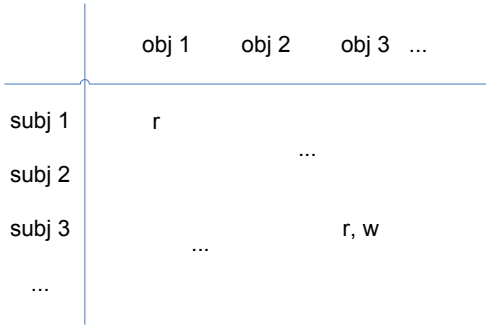

Рис. 2.3.1.1. Матрица доступа

Строки матрицы доступа соответствуют субъектам, существующим в системе, а столбцы – объектам. На пересечении строки и столбца указаны права доступа соответствующего субъекта к данному объекту: например, на рис. 2.3.1.1 субъект *subj 3* обладает правами чтения и записи по отношению к объекту *obj 3*.

Введём следующие ***обозначения***:

- *S* – множество возможных субъектов,
- *O* – множество возможных объектов (напомним, что $S \subset O$);
- $R=\{r_1, \ldots, r_n\}$ – конечное множество прав доступа
- $O \times S \times R$ - ***пространство состояний системы***;
- *M* – матрица прав доступа, описывающая текущие права доступа субъектов к объектам;
- *Q=(S, O, M)* – текущее состояние системы;

- $M[s,o]$ – ячейка матрицы, содержащая набор прав доступа субъекта $s \in S$ к объекту $o \in O$.

Поведение системы во времени моделируется переходами между различными её состояниями. Переходы осуществляются путём внесения изменений в матрицу M с использованием ***команд*** следующего вида:

command $\alpha(x_{1,\dots,}x_k)$
  if r_1 in $M[x_{s1}, x_{o1}]$ **and**
    r_2 in $M[x_{s2}, x_{o2}]$ **and**
    …
    r_m in $M[x_{sm}, x_{om}]$
  then
    op_1,
    op_2,
    …
    op_n,
end

Здесь α - имя команды; x_i – параметры команды, представляющие собой идентификаторы субъектов и объектов, op_i – элементарные операции.

Элементарные операции $op_1 \dots op_n$ будут выполнены в том случае, если выполняются все без исключения условия из блока **if … then**.

При описании элементарных операций мы будем полагать, что в результате выполнения операции система переходит из состояния $Q=(S, O, M)$ в состояние $Q'=(S', O', M')$.

Модель предусматривает наличие шести **элементарных операций**:

1. **enter *r* into *M[s,o]*** ($s \in S, o \in O$) – добавление субъекту s права r по отношению к объекту o. В результате выполнения команды происходят следующие изменения в состоянии системы:
   - $S'=S$,
   - $O'=O$,
   - $M'[x_s, x_o]=M[x_s, x_0]$, *если* $(x_s, x_o) \neq (s,o)$,
   - $M'[s, o]=M[s, o] \cup \{r\}$.

   Заметим, что содержимое ячейки таблицы рассматривается как множество. Это, в частности, означает, что если добавляемый элемент уже присутствовал в ячейке, то её содержимое не изменяется.
2. **delete *r* from *M[s,o]*** ($s \in S, o \in O$) – удаление у субъекта s права r по отношению к объекту o. Изменения в состоянии системы:
   - $S'=S$,
   - $O'=O$,
   - $M'[x_s, x_o]=M[x_s, x_0]$, *если* $(x_s, x_o) \neq (s,o)$,
   - $M'[s,o]=M[s.o] \setminus \{r\}$.

   Если удаляемое право отсутствовало в ячейке, то состояние системы в результате выполнения данной команды никак не изменяется.
3. **create subject *s*** ($s \notin S$) – создание нового субъекта s. Изменения в состоянии системы:

   - $O'=O \cup \{s\}$,
   - $S'=S \cup \{s\}$,
   - $M'[x_s, x_o]=M[x_s, x_o]$ *для* $\forall (x_s, x_o) \in S \times O$,
   - $M'[s, x_o]=\varnothing$ *для* $\forall x_o \in O'$
   - $M'[s, x_s]=\varnothing$ *для* $\forall x_s \in S'$

   Как видим, при создании субъекта в матрицу M добавляются строка и столбец.
4. **destroy subject *s*** ($s \in S$) – удаление существующего субъекта s.

   Изменения в состоянии системы:
   - $S'=S \setminus \{s\}$,
   - $O'=O \setminus \{s\}$,
   - $M'[x_s, x_o]=M[x_s, x_o]$ *для* $\forall (x_s, x_o) \in S' \times O'$.
5. **create object *o*** ($o \notin O$) – создание нового объекта o.

   Изменения в состоянии системы:
   - $O'=O \cup \{o\}$,
   - $S'=S$,
   - $M'[x_s, x_o]=M[x_s, x_o]$ *для* $\forall (x_s, x_o) \in S \times O$,
   - $M'[x_s, o]=\varnothing$ *для* $\forall x_s \in S'$

   При добавлении объекта в матрице доступа создаётся новый столбец.
6. **destroy object *o*** ($o \in O \setminus S$) – удаление существующего объекта o.

   Изменения в состоянии системы:
   - $O'=O \setminus \{o\}$,
   - $S'=S$,
   - $M'[x_s, x_o]=M[x_s, x_o]$ *для* $\forall (x_s, x_o) \in S' \times O'$.

Приведём несколько **примеров команд**:

1. ***Создание файла***.

   Пользователь p создаёт файл f и получает на него права владения, чтения и записи.

```
command create_file (p, f)
    create object f,
    enter own into M[p, f],
    enter r into M[p, f],
    enter w into M[p, f],
end
```

2. ***Создание процесса***.

   Процесс p создаёт процесс q и получает на него право чтения, записи и владения, передавая процессу q права записи и чтения по отношению к самому себе.

```
command exec_process(p, q)
    create subject q,
    enter own into M[p, q],
    enter r into M[p, q],
    enter w into M[p, q],
```

enter r **into** M[q, p],
enter w **into** M[q, p],
end

3. ***Передача права чтения по отношению к файлу***

Право чтения на файл *f* передаётся владельцем p субъекту *q*.

command grant_read(p, q, f)
if own **in** M[p, f]
then
enter r **into** M[q, f],
end

Формальное описание системы в модели Харрисона-Руззо-Ульмана выглядит следующим образом. ***Система*** $\Sigma = (Q, R, C)$ состоит из следующих **элементов**:

1. Конечный набор прав доступа $R=\{r_1, \ldots, r_n\}$.
2. Конечный набор исходных субъектов $S_0=\{s_1, \ldots, s_l\}$.
3. Конечный набор исходных объектов $O_0=\{o_1, \ldots, o_m\}$.
4. Исходная матрица доступа M_0.
5. Конечный набор команд $C = \{\alpha_i(x_1,\ldots,x_k)\}$.

Поведение системы во времени рассматривается как последовательность состояний $\{Q_i\}$, каждое последующее состояние является результатом применения некоторой команды к предыдущему: $Q_{n+1}=C_n(Q_n)$.

Для заданной системы начальное состояние $Q_0=\{S_0, O_0, M_0\}$ называется ***безопасным относительно права r***, если не существует применимой к Q_0 последовательности команд, в результате выполнения которой право *r* будет занесено в ячейку матрицы *M*, в которой оно отсутствовало в состоянии Q_0.

Другими словами это означает, что субъект никогда не получит право доступа *r* к объекту, если он не имел его изначально.

Если же право *r* оказалось в ячейке матрицы *M*, в которой оно изначально отсутствовало, то говорят, что произошла ***утечка права r***.

Рассмотрим **пример** [17]. ◄Пусть система допускает использование двух прав доступа: $R=\{r, w\}$, где *r* – чтение, а *w* – запись, и пусть система описывается следующими командами:

1. Создание субъекта

command create (s, o)
create subject o,
enter r **into** M[s, o],
enter w **into** M[s, o],
end

Команда разрешает создание нового субъекта с одновременным получением по отношению к нему прав доступа на чтение и на запись.

2. Получение прав доступа

command take$_x$(s, o, p)
if r **in** M[s, o] **and**
x **in** M[o, p]

then
enter x **into** M[s, p],
end

Команда разрешает получение произвольного права доступа *x* от любого субъекта *o*, по отношению к которому исходный субъект *s* имеет право чтения.

3. Передача прав доступа

command grant$_x$(s, o, p)
if w **in** M[s, o] **and**
x **in** M[s, p]
then
enter x **into** M[o, p],
end

Команда разрешает передачу произвольного права доступа *x* от любого субъекта *p* любому субъекту, по отношению к которому исходный субъект *s* обладает правом записи.

Пусть в начальном состоянии в системе имеются три субъекта: *o*, *s* и *t*; s обладает правом записи по отношению к *t*, а *t* обладает некоторым правом *a* (которое может представлять собой либо *r*, либо *w*) по отношению к *o*. Покажем, как субъект *s* может получить право доступа *a* по отношению к субъекту *o*.

1. Система находится в начальном состоянии.
2. Субъект *s* создаёт новый субъект *x*, по отношению к которому автоматически получает права чтения и записи.
3. Субъект *s* передаёт субъекту *t* права чтения и записи по отношению к *x*.
4. Субъект *t* передаёт субъекту *x* право доступа *a* по отношению к *o*.
5. Субъект *s* получает от субъекта *x* право доступа a по отношению к *o*.

Приведённая последовательность операций проиллюстрирована на рис. 2.3.1.2.

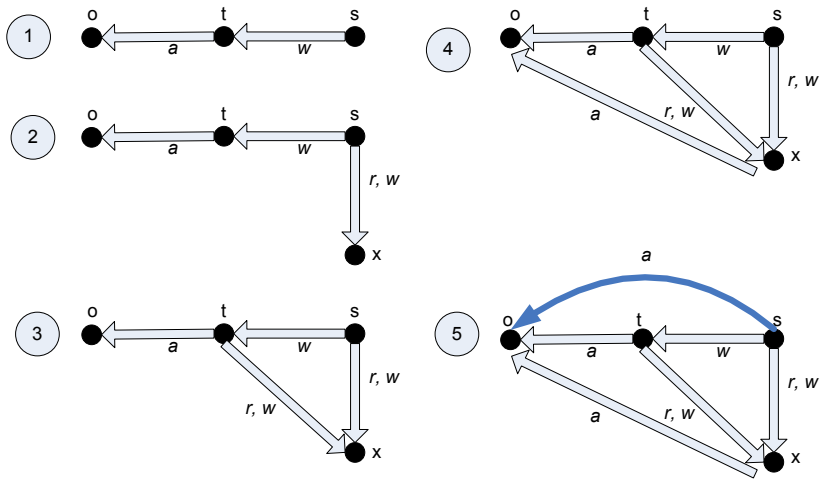

Рис. 2.3.1.2. Утечка права a

Как видим, в результате выполнения шагов 1-5 субъект s обходным путём получает право доступа a по отношению к субъекту o – т.е. происходит утечка права a – а это значит, что исходное состояние не является безопасным. ►

С практической точки зрения значительный интерес представлял бы универсальный метод определения того, является ли заданная система с некоторым начальным состоянием безопасной относительно того или иного права доступа. Покажем, как эта задача может быть решена для одного из частных случаев.

Система $\Sigma = (Q, R, C)$ называется ***монооперационной***, если каждая команда $\alpha_i \in C$ выполняет один примитивный оператор.

Теорема. *Существует алгоритм, который проверяет, является ли исходное состояние монооперационной системы безопасным для данного права a.*

◄ Покажем, что число последовательностей команд системы, которое необходимо проверить, является ограниченным. В этом случае проверка безопасности исходного состояния системы сведётся к полному перебору всех последовательностей и проверке конечного состояния каждой из них на отсутствие утечки права a.

Заметим, что команды **delete** и **destroy** можно не рассматривать, поскольку нас интересует наличие права a, а не его отсутствие. Аналогично, нет необходимости рассматривать более одного оператора **create**: система является монооперационной, и одна команда не может одновременно создать объект или субъект и модифицировать его права доступа, поскольку путём замены параметров можно ограничиться работой с последовательностями команд, которые оперируют над существующими субъектами и объектами. Единственная команда **create** будет необходима на случай, если в начальном состоянии в системе не было ни одного субъекта.

Итак, пусть $c_1, c_2, \ldots, c_n$ – последовательность команд, в результате выполнения которой происходит утечка права a. Упростим эту последовательность команд следующим образом:

1. Удалим все команды **delete** и **destroy**.
2. Добавим в начало последовательности $c_1, c_2, \ldots, c_n$ команду s_{init} вида **create subject**.
3. Проходя последовательность команд справа налево, последовательно удалим все команды вида **create subject** и заменим все ссылки на создаваемые с помощью этих команд субъекты ссылкой на s_{init}.
4. Аналогично удалим все команды вида **create object**, заменяя ссылки на создаваемые с помощью этих команд объекты ссылками на s_{init}.
5. Удалим все команды вида **enter**, вносящие право a в ячейку, которая уже содержит это право.

Согласно приведённым выше замечаниям, получившаяся в результате данных преобразований последовательность команд также приводит к утечке права a. Проанализируем состав возможных команд в получившейся последовательности.

Команды вида **create object, destroy subject, destroy object** и **delete** в последовательности отсутствуют. Команда **create subject** присутствует в единственном числе. Максимальное число команд вида **enter** равно $|R|(|S_0|+1)(|O_0|+1)$. Тем самым,

общее число возможных команд равно $|R|(|S_0|+1)(|O_0|+1)+1$ – а значит, количество последовательностей команд ограничено.►

К сожалению, расширить полученный результат на произвольные системы невозможно.

Теорема. *Для систем общего вида задача определения того, является ли исходное состояние системы безопасным для данного права a, является вычислительно неразрешимой.*

◄Для доказательства этого утверждения достаточно свести задачу проверки безопасности системы к заведомо неразрешимой задаче остановки машины Тьюринга.►

Классическая модель Харриона-Руззо-Ульмана до сих пор широко используется при проведении формальной верификации корректности построения систем разграничения доступа в высоко защищённых автоматизированных системах. Развитие моделей дискреционного управления доступом [18, 19] заключается преимущественно в построении всевозможных модификаций модели Харрисона-Руззо-Ульмана, а также в поиске минимально возможных ограничений, которые можно наложить на описание системы, чтобы вопрос её безопасности был вычислительно разрешимым.

2.3.2. Модель Белла-ЛаПадулы

Данная модель была предложена в 1975 году [20] для формализации механизмов мандатного управления доступом. Мандатный принцип разграничения доступа, в свою очередь, ставил своей целью перенести на автоматизированные системы практику секретного документооборота, принятую в правительственных и военных структурах, когда все документы и допущенные к ним лица ассоциируются с иерархическими уровнями секретности.

В ***модели Белла-ЛаПадулы*** по грифам секретности распределяются субъекты и объекты, действующие в системе, и при этом выполняются следующие **правила**:

1. ***Простое правило безопасности (Simple Security, SS).***
   Субъект с уровнем секретности x_s может читать информацию из объекта с уровнем секретности x_o тогда и только тогда, когда x_s преобладает над x_o.
2. ****-свойство (*-property).***
   Субъект с уровнем секретности x_s может писать информацию в объект с уровнем секретности x_o в том и только в том случае, когда x_o преобладает над x_s.

Для первого правила существует мнемоническое обозначение ***No Read Up***, а для второго – ***No Write Down***.

Диаграмма информационных потоков, соответствующая реализации модели Белла-ЛаПадулы в системе с двумя уровнями секретности, приведена на рис. 2.3.2.1.

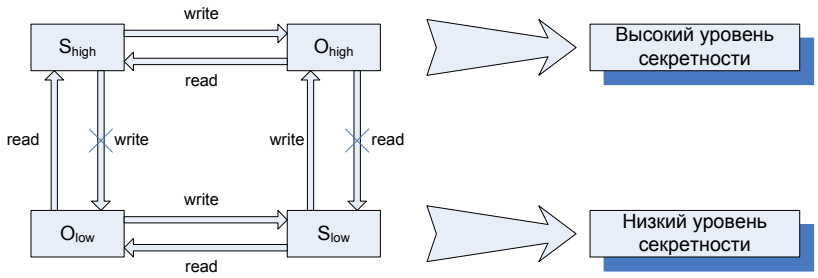

Рис. 2.3.2.1. Диаграмма информационных потоков (модель Белла-ЛаПадулы)

Перейдём к формальному описанию системы. Введём следующие **обозначения**:

- S – множество субъектов;
- O – множество объектов, $S \subset O$;
- $R=\{r, w\}$ – множество прав доступа, r – доступ на чтение, w – доступ на запись;
- $L=\{U, SU, S, TS\}$ – множество уровней секретности, *U- Unclassified, SU – Sensitive but unclassified, S – Secret, TS – Top secret;*
- $\Lambda = (L, \le, \bullet, \otimes)$ - решётка уровней секретности;
- V – множество состояний системы, представляемое в виде набора упорядоченных пар *(F, M)*, где:
  - $F : S \cup O \to L$ - функция уровней секретности, ставящая в соответствие каждому объекту и субъекту в системе определённый уровень секретности;
  - M – матрица текущих прав доступа.

Остановимся более подробно на решётке уровней секретности. Напомним, что ***решёткой*** Λ называется алгебраическая система вида $(L, \le, \bullet, \otimes)$, где:

- $\le$ - оператор, определяющий частичное нестрогое отношение порядка для уровней секретности;
- $\bullet$ - оператор наименьшей верхней границы;
- $\otimes$ - оператор набольшей нижней границы.

Отношение $\le$ обладает следующими **свойствами**:

1. ***Рефлексивность***: $\forall a \in L : a \le a$.
   С точки зрения уровней безопасности это означает, что разрешена передача информации между субъектами и объектами одного уровня безопасности.
2. ***Антисимметричность***: $\forall a_1, a_2 \in L : ((a_1 \le a_2) \,\&\, (a_2 \le a_1)) \to a_2 = a_1$.
   Антисимметричность в нашем случае означает, что если информация может передаваться как от субъектов и объектов уровня A к субъектам и объектам уровня B, так и от субъектов и объектов уровня B к субъектам и объектам уровня A, то эти уровни эквивалентны.
3. ***Транзитивность***: $\forall a_1, a_2, a_3 \in L : ((a_1 \le a_2) \,\&\, (a_2 \le a_3)) \to a_1 \le a_3$.
   Транзитивность означает, что если информации может передаваться от субъектов и объектов уровня A к субъектам и объектам уровня B, и от субъектов и объектов уровня B к субъектам и объектам уровня C, то она может

передаваться от субъектов и объектов уровня A к субъектам и объектам уровня C.

Операторы ***наименьшей верхней границы*** $\bullet$ и ***наибольшей нижней границы*** $\otimes$ определяются следующим образом:

- $a = a_1 \bullet a_2 \Leftrightarrow (a_1, a_2 \le a) \,\&\, (\forall a' \in L : (a' \le a) \to (a' \le a_1 \vee a' \le a_2))$;
- $a = a_1 \otimes a_2 \Leftrightarrow (a \le a_1, a_2) \,\&\, (\forall a' \in L : (a' \le a_1 \,\&\, a' \le a_2) \to (a' \le a))$.

Нетрудно показать, что *для каждой пары* $a_1, a_2 \in L$ *существует единственный элемент наименьшей верхней границы и единственный элемент наибольшей нижней границы*.

Заметим, что в качестве уровней безопасности совершенно не обязательно выбирать целые числа, в ряде случаев удобнее использовать более сложные структуры. За счёт этого, например, в пределах каждого уровня секретности можно реализовать категории секретности (см. рис. 2.3.2.2). В этом случае наличие допуска к той или иной категории информации может служить дополнительным механизмом безопасности, ограничивающим доступ к защищаемым субъектам или объектам.

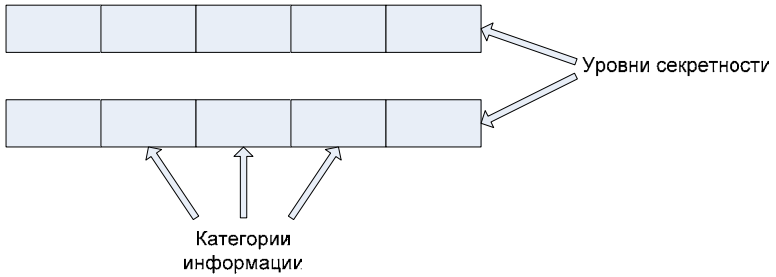

Рис. 2.3.2.2. Уровни секретности и категории информации

Система $\Sigma = (v_0, R, T)$ в модели Белла-ЛаПадулы состоит из следующих элементов:

- v_0 – начальное состояние системы;
- R – множество прав доступа;
- $T : V \times R \to V$ - функция перехода, которая в ходе выполнения запросов переводит систему из одного состояния в другое.

Изменение состояний системы во времени происходит следующим образом: система, находящаяся в состоянии $v \in V$, получает запрос на доступ $r \in R$ и переходит в состояние $v^* = T(v, r)$.

Состояние v_n называется ***достижимым*** в системе $\Sigma = (v_0, R, T)$, если существует последовательность $\{(r_0, v_0), \ldots, (r_{n-1}, v_{n-1}), (r_n, v_n)\} : T(r_i, v_i) = v_{i+1} \forall i = \overline{0, n-1}$. Начальное состояние v_0 является достижимым по определению.

Состояние системы *(F, M)* называется ***безопасным по чтению*** (или ***simple-безопасным***), если для каждого субъекта, осуществляющего в этом состоянии доступ по

чтению к объекту, уровень безопасности субъекта доминирует над уровнем безопасности объекта:

$$\forall s \in S, \forall o \in O,\ r \in M[s,o] \rightarrow F(o) \le F(s).$$

Состояние *(F, M)* называется ***безопасным по записи*** (или **** - безопасным***) в случае, если для каждого субъекта, осуществляющего в этом состоянии доступ по записи к объекту, уровень безопасности объекта доминирует над уровнем безопасности субъекта:

$$\forall s \in S, o \in O:\ w \in M[s,o] \rightarrow F(s) \le F(o).$$

Состояние *(F, M)* называется ***безопасным***, если оно безопасно по чтению и по записи.

Наконец, система $\Sigma = (v_0, R, T)$ называется ***безопасной***, если её начальное состояние v_0 безопасно, и все состояния, достижимые из v_0 путём применения конечной последовательности запросов из R, безопасны.

Теорема (***Основная теорема безопасности Белла-ЛаПадулы***). *Система* $\Sigma = (v_0, R, T)$ *безопасна тогда и только тогда, когда выполнены следующие условия:*

1. *Начальное состояние* v_0 *безопасно.*
2. *Для любого состояния v, достижимого из* v_0 *путём применения конечной последовательности запросов из R, таких, что* $T(v,r) = v^*$, *v=(F, M) и* $v^* = (F^*, M^*)$, *для* $\forall s \in S, \forall o \in O$ *выполнены условия:*
   1. *Если* $r \in M^*[s,o]$ *и* $r \notin M[s,o]$, *то* $F^*(o) \le F^*(s)$.
   2. *Если* $r \in M[s,o]$ *и* $F^*(s) < F^*(o)$, *то* $r \notin M^*[s,o]$.
   3. *Если* $w \in M^*[s,o]$ *и* $w \notin M[s,o]$, *то* $F^*(s) \le F^*(o)$.
   4. *Если* $w \in M[s,o]$ *и* $F^*(o) < F^*(s)$, *то* $w \notin M^*[s,o]$.

◄ Пусть система $\Sigma = (v_0, R, T)$ безопасна. В этом случае начальное состояние v_0 безопасно по определению. Предположим, что существует безопасное состояние v^*, достижимое из состояния v: $T(v,r) = v^*$, и для данного перехода нарушено одно из условий 1-4. Легко заметить, что в случае, если нарушены условия 1 или 2, то состояние v^* будет небезопасным по чтению, а если нарушены условия 3 или 4 – небезопасным по записи. В обоих случаях мы получаем противоречие с тем, что состояние v^* является безопасным.

Докажем достаточность утверждения. Система $\Sigma = (v_0, R, T)$ может быть небезопасной в двух случаях:

1. В случае если начальное состояние v_0 небезопасно. Однако данное утверждение противоречит условию теоремы.
2. Если существует небезопасное состояние v^*, достижимое из безопасного состояния v_0 путём применения конечного числа запросов из R. Это означает, что на каком-то промежуточном этапе произошёл переход $T(v,r) = v^*$, где v – безопасное состояние, а v^* - небезопасное. Однако условия 1-4 делают данный переход невозможным. ►

Отметим, что изложенная модель в силу своей простоты имеет целый ряд серьёзных недостатков. Например, никак не ограничивается вид функции перехода T – а это означает, что можно построить функцию, которая при попытке запроса на чтения к объекту более высокого уровня секретности до проверки всех правил будет понижать уровень секретности объекта. Другим принципиальным недостатком модели Белла-ЛаПадулы является потенциальная возможность организации скрытых каналов передачи информации. Тем самым, дальнейшее развитие моделей мандатного управления доступом было связано с поиском условий и ограничений, повышающих её безопасность.

В настоящее время модель Белла-ЛаПадулы и другие модели мандатного управления доступом [18, 19] широко используются при построении и верификации автоматизированных систем, преимущественно предназначенных для работы с информацией, составляющей государственную тайну.

2.4. Формальные модели целостности

2.4.1. Модель Кларка-Вилсона

Модель целостности Кларка-Вилсона была предложена в 1987 г. [13] как результат анализа практики бумажного документооборота, эффективной с точки зрения обеспечения целостности информации. Модель Кларка-Вилсона является описательной и не содержит каких бы то ни было строгих математических конструкций – скорее её целесообразно рассматривать как совокупность практических рекомендаций по построению системы обеспечения целостности в АС.

Введём следующие обозначения:

- S – множество субъектов;
- D – множество данных в автоматизированной системе (множество объектов);
- *CDI* (Constrained Data Items) – данные, целостность которых контролируется;
- *UDI* (Unconstrained Data Items) – данные, целостность которых не контролируется;

  При этом $D = CDI \cup UDI$, $CDI \cap UDI = \varnothing$.
- *TP* (Transformation Procedure) – ***процедура преобразования***, т.е. компонент, котрый может инициировать ***транзакцию*** – последовательность операций, переводящую систему из одного состояния в другое;
- *IVP* (Integrity Verification Procedure) – процедура проверки целостности *CDI*.

Правила модели Кларка-Вилсона:

1. В системе должны иметься *IVP*, способные подтвердить целостность любого *CDI*.

   Примером *IVP* может служить механизм подсчёта контрольных сумм.
2. Применение любой *TP* к любому *CDI* должно сохранять целостность этого *CDI*.
3. Только *TP* могут вносить изменения в *CDI*.
4. Субъекты могут инициировать только определённые *TP* над определёнными *CDI*.

   Данное требование означает, что система должна поддерживать отношения вида *(s, t, d)*, где $s \in S$, $t \in TP$, $d \in CDI$. Если отношение определено, то субъект s может применить преобразование t к объекту d.

5. Должна быть обеспечена политика разделения обязанностей субъектов – т.е. субъекты не должны изменять *CDI* без вовлечения в операцию других субъектов системы.
6. Специальные *TP* могут превращать *UDI* в *CDI*.
7. Каждое применение *TP* должно регистрироваться в специальном *CDI*. При этом:
   - данный *CDI* должен быть доступен только для добавления информации;
   - в данный *CDI* необходимо записывать информацию, достаточную для восстановления полной картины функционирования системы.
8. Система должна распознавать субъекты, пытающиеся инициировать *TP*.
9. Система должна разрешать производить изменения в списках авторизации только специальным субъектам (например, администраторам безопасности).

Данное требование означает, что тройки *(s, t, d)* могут модифицировать только определённые субъекты.

Безусловными достоинствами модели Кларка-Вилсона являются её простота и лёгкость совместного использования с другими моделями безопасности.

2.4.2. Модель Биба

Модель Биба была разработана в 1977 году как модификация модели Белла-ЛаПадулы, ориентированная на обеспечение целостности данных. Аналогично модели Белла-ЛаПадулы, модель Биба использует ***решётку классов целостности*** $\Lambda = (IC, \leq, \bullet, \otimes)$, где IC – классы целостности данных.

Базовые правила Модели Биба формулируются следующим образом:

1. ***Простое правило целостности (Simple Integrity, SI).***
   Субъект с уровнем целостности x_s может читать информацию из объекта с уровнем целостности x_o тогда и только тогда, когда x_o преобладает над x_s.
2. **** - свойство (* - integrity).***
   Субъект с уровнем целостности x_s может писать информацию в объект с уровнем целостности x_o тогда и только тогда, когда x_s преобладает над x_o.

Для первого правила существует мнемоническое обозначение ***No Read Down***, а для второго – ***No Write Up***.

Диаграмма информационных потоков, соответствующая реализации модели Биба в системе с двумя уровнями секретности, приведена на рис. 2.4.2.

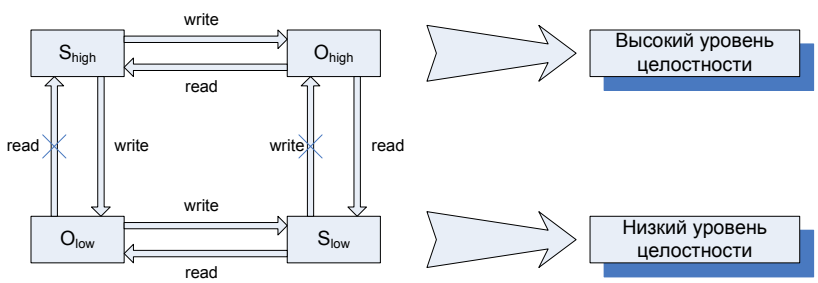

Рис. 2.4.2. Диаграмма информационных потоков (модель Биба)

Отдельного комментария заслуживает вопрос, что именно понимается в модели Биба под уровнями целостности. Действительно, в большинстве приложений целостность данных рассматривается как некое свойство, которое либо сохраняется, либо не сохраняется – и введение иерархических уровней целостности может представляться излишним. В действительности уровни целостности в модели Биба стоит рассматривать как уровни достоверности, а соответствующие информационные потоки – как передачу информации из более достоверной совокупности данных в менее достоверную и наоборот.

Формальное описание модели Биба полностью аналогично описанию модели Белла-ЛаПадулы.

К достоинствам модели Биба следует отнести её простоту, а также использование хорошо изученного математического аппарата. В то же время модель сохраняет все недостатки, присущие модели Белла-ЛаПадулы.

2.5. Совместное использование моделей безопасности

В реальных автоматизированных системах редко встречаются системы защиты, ориентированные исключительно на обеспечение конфиденциальности или исключительно на обеспечение целостности информации. Как правило, система защиты должна сочетать оба механизма – а значит, при построении и анализе этой системы будет необходимым совместное использование нескольких формальных моделей безопасности.

Рассмотрим в качестве примера возможные **варианты совместного использования моделей Белла-ЛаПадулы и Биба** [12].

1. Две модели могут быть реализованы в системе независимо друг от друга. В этом случае субъектам и объектам независимо присваиваются уровни секретности и уровни целостности.
2. Возможно логическое объединение моделей за счёт выделения общих компонентов. В случае моделей Биба и Белла-ЛаПадулы таким общим компонентом является порядок разграничения доступа в пределах одного уровня секретности (рис. 2.5.1).

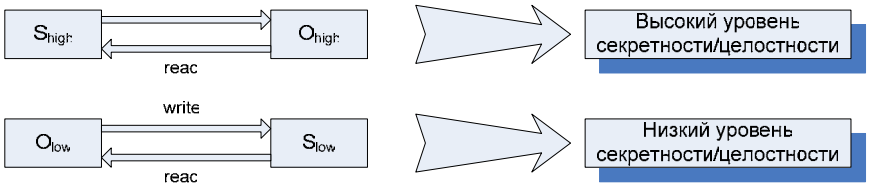

Рис. 2.5.1. Совместное использование моделей Белла-ЛаПадулы и Биба (выделение общих компонентов)

3. Возможно использование одной и ой же решётки уровней как для секретности, так и для целостности. При этом субъекты и объекты с высоким уровнем целостности будут располагаться на низких уровнях секретности, а субъекты и объекты с низким уровнем целостности – на высоких уровнях секретности (рис. 2.5.2).

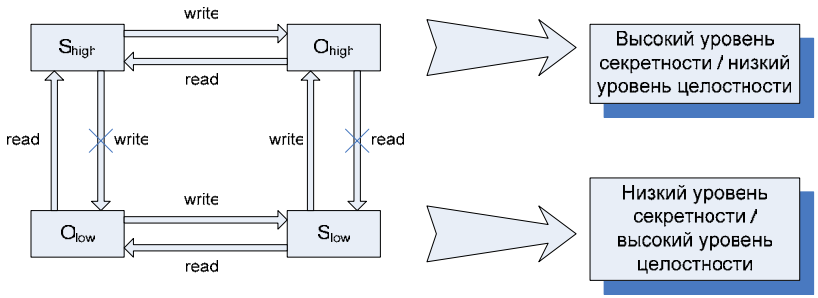

Рис. 2.5.2. Совместное использование моделей Белла-ЛаПадулы и Биба (единая решётка уровней целостности и секретности)

Последняя реализация позволяет, например, разместить системные файлы на нижнем уровне иерархии, что обеспечит их максимальную целостность, не акцентируя внимание на излишней в данном случае секретности.

2.6. Ролевое управление доступом

Ролевая модель управления доступом [19] содержит ряд особенностей, которые не позволяют отнести её ни к категории дискреционных, ни к категории мандатных моделей. Основная идея реализуемого в данной модели подхода состоит в том, что понятие «субъект» заменяется двумя новыми понятиями:

- ***пользователь*** – человек, работающий в системе;
- ***роль*** – активно действующая в системе абстрактная сущность, с которой связан ограниченный и логически непротиворечивый набор полномочий, необходимых для осуществления тех или иных действий в системе.

Классическим примером роли является root в Unix-подобных системах – суперпользователь, обладающий неограниченными полномочиями. Данная роль по мере необходимости может быть задействована различными администраторами.

Основным достоинством ролевой модели является близость к реальной жизни: роли, действующие в АС, могут быть выстроены в полном соответствии с корпоративной иерархией и при этом привязаны не к конкретным пользователям, а к должностям – что, в частности, упрощает администрирование в условиях большой текучки кадров.

Управление доступом при использовании ролевой модели осуществляется следующим образом:

1. Для каждой роли указывается набор полномочий, представляющий собой набор прав доступа к объектам АС.
2. Каждому пользователю назначается список доступных ему ролей.

Отметим, что пользователь может быть ассоциирован с несколькими ролями – данная возможность также значительно упрощает администрирование сложных корпоративных АС.

Перейдём к формальному описанию системы. Введём следующие **обозначения**:

- U – множество пользователей;
- R – множество ролей;

- P – совокупность полномочий на доступ к объектам (реализованная, например, в виде матрицы доступа);
- S – множество сеансов работы пользователей с системой

Управление доступом реализуется с использованием следующих **отображений**:

- $PA \subseteq P \times R$ - отображение множества полномочий на множество ролей, задающее для каждой роли установленный набор полномочий;
- $UA \subseteq U \times R$ - отображение множества пользователей на множество ролей, определяющее набор ролей, доступных данному пользователю;
- $user : S \to U$ - функция, определяющая для сеанса $s \in S$ текущего пользователя $u \in U$:

$$user(s) = u;$$

- $roles : S \to \{R\}$ - функция, определяющая для сеанса $s \in S$ набор ролей из множества R, доступных в данном сеансе:

$$roles(s) = \{r_i \mid (user(s), r_i) \in UA\};$$

- $permissions : S \to \{P\}$ - функция, задающая для сеанса $s \in S$ набор доступных в нём полномочий (иначе говоря, совокупность полномочий всех ролей, доступных в данном сеансе):

$$permissions(s) = \bigcup_{r \in roles(s)} \{p_i \mid (p_i, r) \in PA\}.$$

Взаимосвязь пользователей, ролей, полномочий и сеансов показана на рис. 2.6.

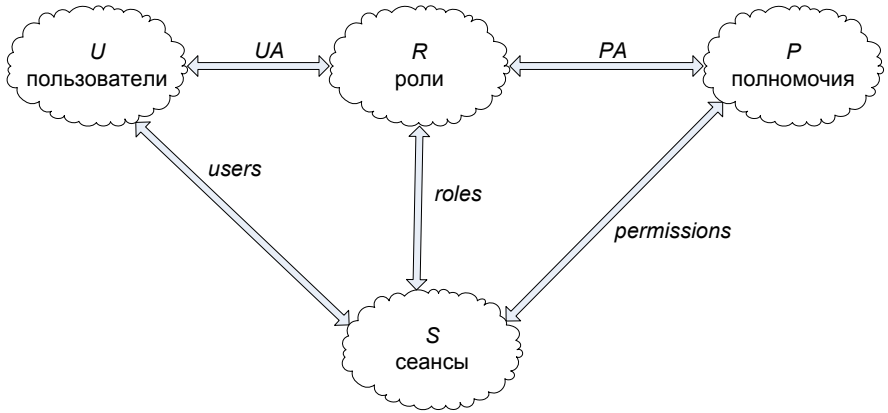

Рис. 2.6. Взаимосвязь ролей, полномочий, пользователей и сеансов

Критерий безопасности системы при использовании ролевой модели звучит следующим образом: система считается ***безопасно***й, если любой пользователь в системе, работающий в сеансе $s \in S$, может осуществлять действия, требующие полномочий $p \in P$, только в том случае, если $p \in permissions(s)$.

На практике управление доступом в АС при использовании ролевой модели осуществляется главным образом не с помощью назначения новых полномочий ролям, а

путём задания отношения *UA* – т.е. путём определения ролей, доступных данному пользователю.

Подходы к распределению ролей могут быть различными и определяются спецификой организации, однако в большинстве случаев реализуется один из двух вариантов:

1. Создание иерархических ролей, полностью копирующих корпоративную иерархию и сохраняющих отношения между ролями, существующие в реальном мире.
2. Использование взаимоисключающих ролей, позволяющих эффективно реализовать разделение обязанностей.

Во всех случаях использование ролевой модели позволяет значительно повысить эффективность администрирования сложных автоматизированных систем, поэтому данный подход чрезвычайно популярен.

2.7. Скрытые каналы передачи информации

Неформально под ***скрытым каналом передачи информации*** [22] понимают любой канал связи, изначально для передачи информации не предназначенный. Для нас будут представлять интерес скрытые каналы, реализуемые за счёт особенностей формальных моделей управления доступом.

Пусть имеется модель мандатного управления доступом *M* и её реализация *I(M)*. Тогда любая потенциальная связь между двумя субъектами $I(s_h)$ и $I(s_l)$ называется ***скрытым каналом передачи информации*** (рис. 2.7.1), если эта связь не разрешена в модели *M*.

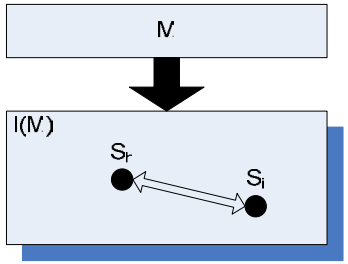

Рис. 2.7.1. Скрытый канал передачи информации

Выделяют следующие **типы скрытых каналов**:

1. ***Скрытые каналы по памяти***, в которых информация передаётся через доступ отправителя на запись и получателя на чтение к одним и тем же ресурсам или объектам;
2. ***Скрытые каналы по времени***, которые характеризуются доступом отправителя и получателя к одному и тому же процессу или изменяемому во времени атрибуту.

Приведём **примеры** скрытых каналов передачи информации. ◄Рассмотрим систему, в которой имеются два уровня секретности: *High* и *Low*. Передача информации с

уровня *Low* на уровень *High* разрешена, а в обратном направлении – запрещена (рис. 2.7.2).

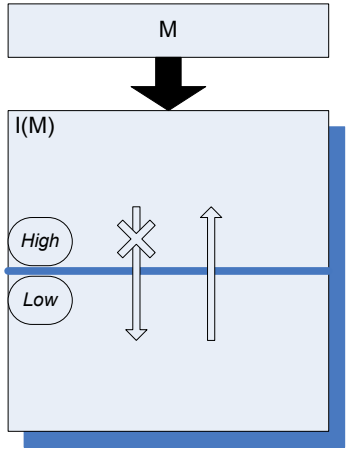

Рис. 2.7.2. Система с двумя уровнями секретности

Цель нарушителя состоит в том, чтобы организовать скрытый канал для передачи информации от программно-аппаратного агента, функционирующего в среде *High*, к другому программно-аппаратному агенту, функционирующему в среде *Low*.

Пример скрытого канала по памяти приведён на рис. 2.7.3.

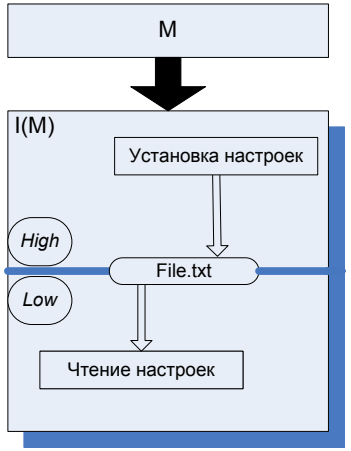

Рис. 2.3.7. Пример скрытого канала по памяти

Субъект, функционирующий в среде *High*, может выполнять настройки параметров безопасности элементов файловой системы, и настройки доступны для наблюдения в среде *Low*. В этом случае злоумышленник может закодировать передаваемую информацию в значениях параметров безопасности тех или иных элементов файловой системы (на рисунке это файл File.txt).

Пример скрытого канала по времени приведён на рис. 2.3.8.

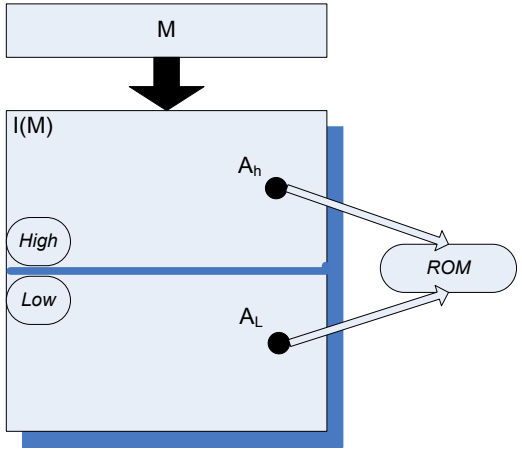

Рис. 2.3.8. Пример скрытого канала по времени

В данном случае между уровнями *High* и *Low* нет общих ресурсов, за исключением системной библиотеки *ROM*, доступ к которой возможен только на чтение. Для организации скрытого канала передачи информации субъект A_h может модулировать определённым образом интервалы занятости библиотеки, а субъект A_l – сканировать время занятости библиотеки, осуществляя запросы к ней с заданной периодичностью.►

Подходы к решению задачи выявления скрытых каналов передачи информации в настоящее время активно изучаются и совершенствуются. На сегодняшний день наиболее распространены следующие **методы**:

1. ***Метод разделяемых ресурсов Кемерера*** [23], который состоит в следующем:
   - для каждого разделяемого ресурса в системе строится матрица, строки которой соответствуют всевозможным атрибутам разделяемого ресурса, а столбцы – операциям, выполняемым в системе;
   - значения в ячейках матрицы соответствуют воздействиям, осуществляемым при выполнении тех или иных операций в отношении атрибутов разделяемых ресурсов.

   Получившаяся в результате матрица позволяет отследить информационные потоки, существующие в системе.
2. ***Сигнатурный анализ*** [24] исходных текстов программного обеспечения. Данный метод предполагает проведение анализа исходных текстов программ с целью выявления конструкций, характерных для скрытых каналов передачи информации.

Необходимость проведения анализа автоматизированных систем в ходе проведения сертификационных испытаний регламентируется соответствующими оценочными стандартами и обычно является необходимым для высоко доверенных систем.

2.8. Выводы

Мы рассмотрели наиболее распространённые модели управления доступом, позволяющие реализовать формальный анализ систем защиты, ориентированных на обеспечение конфиденциальности и целостности информации. За рамками рассмотрения остались вопросы формализации механизмов обеспечения доступности, относящиеся преимущественно к сфере теории надёжности.

Формализация механизмов защиты может преследовать различные цели, но главная из них – это оценка стойкости архитектуры реальных систем, проводимая, например, в рамках комплексного анализа их защищённости. Место такого анализа в жизненном цикле автоматизированных систем во многом определяют стандарты информационной безопасности – один из основных механизмов накопления знаний в данной области. Именно стандартам и посвящена последняя, самая объёмная часть книги.

Часть 3. Стандарты в информационной безопасности

3.1. Общие сведения

В общем случае ***стандартом*** принято называть документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт может задавать и другие требования – например, к символике или терминологии.

Формальной причиной **необходимости использования** стандартов является тот факт, что необходимость следования некоторым из них закреплена законодательно. Реальные причины гораздо глубже – обычно стандарт является результатом формализации опыта лучших специалистов в той или иной области, и потому представляет собой надёжный источник оптимальных и проверенных решений. Стандарты являются также одним из основных механизмов обеспечения совместимости продуктов и систем – в частности, АС, использующих решения от различных производителей.

Остановимся на стандартах в области информационной безопасности [25]. Их общепринятая классификация с примерами приведена на рис. 3.1.

Рис. 3.1. Классификация стандартов в области информационной безопасности

Перечислим основные стандарты в области информационной безопасности, имеющие в настоящее время официальный статус в Российской Федерации:

- ***Руководящие документы (РД) Гостехкомиссии России*** действуют и активно используются при проведении сертификации средств защиты информации в системах сертификации ФСТЭК России, Минобороны России, а также в ряде добровольных систем сертификации.
- Стандарт ***ГОСТ Р ИСО/МЭК 15408-2002***, более известный как ***«Общие критерии»***, действует и применяется при проведении сертификации средств защиты, не предназначенных для работы с информацией, составляющей государственную тайну. В перспективе предполагается отказ от РД Гостехкомиссии России и полноценный переход к «Общим критериям» как единому оценочному стандарту.
- ***Криптографические стандарты*** (ГОСТ 28147-89, ГОСТ 3410-2001, ГОСТ 3411-94) являются обязательными для применения в системах защиты информации, позиционируемых как средства криптографической защиты.
- ***Управленческие стандарты*** ISO 17799-2005 и ISO 27001-2005 в настоящее время не имеют в РФ официального статуса, однако планируются к принятию в качестве ГОСТ в ближайшее время

Все остальные спецификации носят сугубо добровольный характер, однако активно используются при построении реальных систем, в первую очередь в целях обеспечения их взаимной совместимости.

3.2. «Оранжевая книга»

Стандарт ***«Критерии оценки доверенных компьютерных систем»*** /***Trusted Computer System Evaluation Criteria***/, более известный как ***«Оранжевая книга»***, [26] был разработан Министерством Обороны США в 1983 г. и стал первым в истории общедоступным оценочным стандартом в области информационной безопасности.

Требования «Оранжевой книги» имеют следующую **структуру**:

1. Политика безопасности

1.1. Система должна поддерживать точно определённую политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом. По мере необходимости должна использоваться политика мандатного управления доступом.

1.2. С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Для реализации мандатного управления доступом система должна обеспечивать каждому объекту набор атрибутов, определяющих степень конфиденциальности объекта и режимы доступа к этому объекту.

2. Подотчётность

2.1. Все субъекты должны имеет уникальные идентификаторы. Контроль доступа должен осуществляться на основе идентификации субъекта и объекта доступа, аутентификации и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами

компьютерной системы, функционирование которых критично сточки зрения безопасности.

2.2. Для определения степени ответственности пользователя за действия в системе, все происходящие в ней события, имеющие значение сточки зрения безопасности, должны отслеживаться и регистрироваться в защищённом протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделят из него только те события, которые оказывают влияние на безопасность. Протокол событий должен быть надёжно защищён от несанкционированного доступа, модификации и уничтожения.

3. Гарантии

3.1. Средства защиты должны содержать независимые аппаратные или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Средства контроля должны быть полностью независимы от средств защиты.

3.2. Все средства защиты должны быть защищены от несанкционированного вмешательства и отключения, причём эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и автоматизированной системы в целом. Данное требование распространяется на весь жизненный цикл автоматизированной системы.

Напомним, что «Оранжевая книга» является оценочным стандартом – а значит, предназначена в первую очередь для проведения анализа защищённости автоматизированных систем. По результатам такого анализа АС должна быть отнесена к одному из определённых в документе классов защищённости.

«Оранжевая книга» определяет четыре **группы классов защищённости**:

A – содержит единственный класс *A1*.

B – содержит классы *B1, B2* и *B3*.

C – содержит классы *C1* и *C2*.

D – содержит единственный класс *D1*.

Требуемый уровень защищённости системы возрастает от группы *D* к группе *A*, а в пределах одной группы – с увеличением номера класса. Каждый класс характеризуется определённым фиксированным набором требований к подсистеме обеспечения информационной безопасности, реализованной в АС.

Приведём краткие характеристики каждого из классов защищённости.

I. Группа D – минимальная защита.

К данной категории относятся те системы, которые были представлены для сертификации по требованиям одного из более высоких классов защищённости, но не прошли испытания.

II. Группа C - дискреционная защита.

Данная группа характеризуется наличием дискреционного управления доступом и регистрации действий субъектов.

- ***Класс C1 – дискреционная защита***

Система включает в себя средства контроля и управления доступом, позволяющие задавать ограничения для отдельных пользователей. Класс C1 рассчитан на однопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиденциальности.

- ***Класс C2 – управление доступом***

Система обеспечивает более избирательное управление доступом путём применения средств индивидуального контроля за действиями пользователей, регистрации, учёта событий и выделения ресурсов.

3. Группа B – мандатная защита

Система обеспечивает мандатное управление доступом с использованием меток безопасности, поддержку модели и политики безопасности. Предполагается наличие спецификаций на функции ядра безопасности. Реализуется концепция монитора безопасности обращений, контролирующего все события в системе.

- ***Класс B1 – защита с применением меток безопасности***

Помимо выполнения всех требований к классу *C2*, система должна поддерживать маркировку данных и мандатное управление доступом. При экспорте из системы информация должна подвергаться маркировке.

- ***Класс B2 – структурированная защита***

Ядро безопасности должно поддерживать формально определённую и чётко документированную модель безопасности, предусматривающую дискреционное и мандатное управление доступом, которое распространяется на все субъекты. Должен осуществляться контроль скрытых каналов передачи информации. В структуре ядра безопасности должны быть выделены элементы, критичные с точки зрения безопасности. Интерфейс ядра безопасности должен быть чётко определён, а его архитектура и реализация должны быть выполнены с учётом возможности проведения тестовых испытаний. Управление безопасностью должно осуществляться администратором безопасности.

- ***Класс B3 – домены безопасности***

Ядро безопасности должно поддерживать монитор безопасности обращений, который контролирует все типы доступа субъектов к объектам и который невозможно обойти. Ядро безопасности содержит исключительно подсистемы, отвечающие за реализацию функций защиты, и является достаточно компактным для обеспечения возможности эффективного тестирования. Средства аудита должны включать механизмы оповещения администратора о событиях, имеющих значение для безопасности системы. Необходимо наличие средств восстановления работоспособности системы.

4. Группа A – верифицированная защита

Группа характеризуется применением формальных методов верификации корректности функционирования механизмов управления доступом. Требуется дополнительная документация, демонстрирующая, что архитектура и реализация ядра безопасности отвечает требованиям безопасности. Функциональные требования совпадают с классом *B3*, однако на всех этапах

разработки АС требуется применение формальных методов верификации систем защиты.

Разработка и публикация «Оранжевой книги» стали важнейшей вехой в становлении теории информационной безопасности. Такие базовые понятия, как «политика безопасности», «монитор безопасности обращений» или «администратор безопасности» впервые в открытой литературе появились именно в «Оранжевой книге».

В то же время с течением времени стали проявляться многочисленные недостатки «Оранжевой книги» и предложенного подхода к классификации АС в целом. Во многом её устаревание было связано с принципиальными изменениями аппаратной базы средств вычислительной техники, произошедшими с 1983 г. – и прежде всего, с распространением распределённых вычислительных систем и сетей, особенности которых в «Оранжевой книге» никак не учитываются. Не нашли отражения в «Оранжевой книге» и вопросы обеспечения доступности информации. Наконец, с усложнением АС всё больше стала проявляться принципиальная ограниченность «табличного» подхода к классификации систем по требованиям безопасности информации, когда автоматизированная система должна быть отнесена к одному из классов защищённости исходя из выполнения фиксированного набора требований к функциональным характеристикам – такой подход принципиально не позволяет учесть особенности системы и является недостаточно гибким.

Стараясь не отстать от развивающихся информационных технологий, разработчики «Оранжевой книги» вплоть до 1995 г. выпустили целый ряд вспомогательных документов, известных как «Радужная серия». Эти документы содержали рекомендации по применению положений «Оранжевой книги» для различных категорий автоматизированных систем, а также вводили ряд дополнительных требований. Наибольший интерес в «Радужной серии» представляют три документа: «Интерпретация для защищённых сетей», «Интерпретация для защищённых СУБД» и «Руководство по управлению паролями».

В настоящее время «Оранжевая книга» не используется для оценки автоматизированных систем и представляет интерес исключительно с исторической точки зрения.

3.3. Руководящие документы Гостехкомиссии России

3.3.1. Общие положения

Гостехкомиссия России (ныне это Федеральная служба по техническому и экспортному контролю – ФСТЭК России) в период с 1992 по 1999 г. разработала пакет руководящих документов, посвящённых вопросам защиты информации в автоматизированных системах. Наибольший интерес представляют следующие документы:

- Защита от несанкционированного доступа к информации. Термины и определения [27].
- Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [28].

- Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [29].
- Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации [30].
- Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищённости от несанкционированного доступа к информации [31].
- Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей [32].

3.3.2. Основные положения концепции защиты СВТ и АС от НСД к информации

Под ***несанкционированным доступом*** (НСД) понимается доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств предоставляемых СВТ или АС. Выделяют два **направления защиты от НСД**:

1. Связанные со средствами вычислительной техники (СВТ).
2. Связанные с автоматизированными системами (АС).

Средства вычислительной техники представляют собой элементы, из которых строятся автоматизированные системы. Для СВТ, в отличие от АС, контролируется реализация исключительно тех функций защиты, для реализации которых они предназначены.

Выделяют следующие **основные способы НСД**:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить НСД (например, путём внедрения программных закладок);
- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД (например, выполнить загрузку компьютера в обход штатной операционной системы).

Предлагаются следующие **принципы защиты от НСД**:

1. Защита СВТ и АС основывается на положениях и требованиях соответствующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.
2. Защита СВТ обеспечивается комплексом программно-технических средств.
3. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.
4. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

5. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС:
   - надёжность;
   - быстродействие;
   - возможность изменения конфигурации АС.
6. Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.
7. Защита АС должна предусматривать контроль эффективности средств защиты от НСД, который либо может быть периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

Концепция также предлагает модель нарушителя безопасности автоматизированной системы. В качестве ***нарушителя*** рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяют **4 уровня возможностей**, на каждом уровне нарушитель является специалистом высшей квалификации, знает всё об автоматизированной системе и, в частности, о средствах её защиты.

1. Возможность ведения диалога в АС – запуск программ из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.
2. Возможность создания и запуска собственных программ с новыми функциями по обработке информации.
3. Возможность управления функционированием АС, т.е. воздействие на базовое программное обеспечение системы и на состав и конфигурацию её оборудования.
4. Весь объём возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Нетрудно видеть, что уровни являются иерархическими – каждый последующий уровень включает возможности всех предыдущих.

В концепции предлагается оценивать технические средства защиты от НСД по следующим основным характеристикам:

1. Степень полноты и качество охвата правил разграничения доступа реализованной системы разграничения доступа. Оцениваются:
   - чёткость и непротиворечивость правил доступа;
   - надёжность идентификации правил доступа.
2. Состав и качество обеспечивающих средств для системы разграничения доступа. При проведении оценки учитываются:
   - средства идентификации и опознания субъектов и порядок и порядок их использования;
   - полнота учёта действий субъектов;

   - способы поддержания привязки субъекта к его процессу.
3. Гарантии правильности функционирования системы разграничения доступа и обеспечивающих её средств. При оценке используется соответствующая документация.

Обеспечение защиты СВТ и АС осуществляется ***системой разграничения доступа*** (СРД) субъектов к объектам доступа и ***обеспечивающими средствами для СРД***.

Основными функциями СРД являются:

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

Обеспечивающие средства для СРД выполняют следующие **функции**:

- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса;
- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Сама система разграничения доступа может быть **реализована** следующим образом:

- в виде распределённой системы или локально в ядре защиты;
- в рамках операционной системы или прикладных программ;
- в средствах реализации сетевого взаимодействия или на уровне приложений;
- с использованием криптографии или методов непосредственного контроля доступа;
- путём программной или аппаратной реализации.

Организация работ по защите СВТ и АС от НСД к информации должна быть частью общей организации работ по обеспечению безопасности информации. При этом обеспечение защиты основывается на требованиях по защите к разрабатываемым СВТ и АС, формулируемых заказчиком и согласуемых с разработчиком. Такие требования

задаются либо в виде желаемого уровня защищенности СВТ или АС, либо в виде перечня требований, соответствующего этому уровню.

Проверка выполнения технических требований по защите проводится аналогично с другими техническими требованиями в процессе испытаний (предварительных, государственных и др.). По результатам успешных испытаний оформляется ***сертификат***, удостоверяющий соответствие СВТ или АС требованиям по защите и дающий право разработчику на использование и (или) распространение их как защищенных.

Отмечается, что **разработка мероприятий по защите** должна проводиться одновременно с разработкой СВТ и АС и выполняться за счет финансовых и материально-технических средств (ресурсов), выделенных на разработку СВТ и АС.

3.3.3. Средства вычислительной техники. Защита от НСД к информации. Показатели защищённости от НСД к информации

Руководящий документ [30] устанавливает классификацию средств вычислительной техники по уровню защищённости от НСД к информации на базе перечня показателей защищённости и совокупности описывающих их требований.

Средство вычислительной техники (СВТ) рассматривается в документе как совокупность программных и технических элементов АС, способных функционировать самостоятельно или в составе других систем.

Устанавливаются **7 классов защищённости** СВТ от НСД к информации, разбитые на **4 группы**:

I. 7 класс – СВТ, которые были представлены к оценке, однако не удовлетворяют требованиям более высоких классов.
II. 6 и 5 классы – ***дискреционная защита***.
III. 4, 3 и 2 классы – ***мандатная защита***.
IV. 1 класс – ***верифицированная защита***.

Требования ужесточаются с уменьшением номера класса.

Каждый класс характеризуется фиксированным набором показателей защищённости. Классы являются иерархически упорядоченными: каждый последующий класс содержит требования всех предыдущих.

В общем случае требования предъявляются к следующим **показателям защищённости**:

1. Дискреционный принцип контроля доступа.
2. Мандатный принцип контроля доступа.
3. Очистка памяти.
4. Изоляция модулей.
5. Маркировка документов.
6. Защита ввода и вывода на отчуждаемый физический носитель информации.
7. Сопоставление пользователя с устройством (например, с консолью).
8. Идентификация и аутентификация.
9. Гарантии проектирования.
10. Регистрация.

11. Взаимодействие пользователя с комплексом средств защиты (подразумевается чёткое определение всех возможных интерфейсов).
12. Надежное восстановление.
13. Целостность КСЗ.
14. Контроль модификации.
15. Контроль дистрибуции (имеется в виду контроль точности копирования при изготовлении копий с образца носителя данных).
16. Гарантии архитектуры (означает, что реализованная модель безопасности обеспечивает гарантированный перехват монитором безопасности обращений всех попыток доступа в системе).
17. Тестирование.
18. Руководство для пользователя.
19. Руководство по комплексу средств защиты.
20. Тестовая документация.
21. Конструкторская (проектная) документация.

Оценка класса защищённости СВТ осуществляется путём проведения сертификационных испытаний.

3.3.4. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации

Руководящий документ [29] устанавливает классификацию АС, подлежащих защите от НСД к информации, и задаёт требования по защите информации в автоматизированных системах различных классов.

В соответствии с документом, **классификация АС** включает следующие **этапы**:

1. Разработка и анализ исходных данных.
2. Выявление основных признаков АС, необходимых для классификации.
3. Сравнение выявленных признаков АС с классифицируемыми.
4. Присвоение АС соответствующего класса защиты информации от НСД.

Исходными данными для классификации АС являются:

1. Перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности.
2. Перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий.
3. Матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС.
4. Режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации. Устанавливаются **9 классов защищённости** АС от НСД к информации, каждый класс характеризуется определённой минимальной совокупностью требований по защите. Классы подразделяются на **3 группы**:

- ***III группа – классы 3Б и 3А***

  Классы соответствуют автоматизированным системам, в которых работает один пользователь, допущенный ко всей информации в АС, размещённой на носителях одного уровня конфиденциальности.

- ***II группа – классы 2Б и 2А***
  Классы данной группы соответствуют автоматизированным системам, в которых пользователи имеют одинаковые права доступа ко всей информации в АС, обрабатываемой или хранимой на носителях различного уровня конфиденциальности.
- ***I группа – классы 1Д, 1Г, 1В, 1Б и 1А***
  В соответствующих автоматизированных системах одновременно обрабатывается или хранится информация разных уровней конфиденциальности. Не все пользователи имеют доступ ко всей информации в АС.

Для каждого из классов фиксируется набор **требований**, составленный из следующего **общего списка**:

1. Подсистема управления доступом

1.1. Идентификация, проверка подлинности и контроль доступа субъектов:
- в систему;
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;
- к программам;
- к томам, каталогам, файлам, записям, полям записей.

1.2. Управление потоками информации

2. Подсистема регистрации и учёта

2.1. Регистрация и учёт:
- входа (выхода) субъектов доступа в (из) систему (узел сети);
- выдачи печатных (графических) выходных документов;
- запуска (завершения) программ и процессов;
- доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;
- изменения полномочий субъектов доступа;
- создаваемых защищаемых объектов доступа.

2.2. Учёт носителей информации.

2.3. Очистка освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.

2.4. Сигнализация попыток нарушения защиты.

3. Криптографическая подсистема

3.1. Шифрование конфиденциальной информации.

3.2. Шифрование информации, принадлежащей различным субъектам доступа (или группам субъектов), на различных ключах.

3.3. Использование аттестованных (сертифицированных) криптографических средств.

4. Подсистема обеспечения целостности

4.1. Обеспечение целостности программных средств и обрабатываемой информации.

4.2. Физическая охрана СВТ и носителей информации.

4.3. Наличие администратора (службы) защиты информации в АС.

4.4. Периодическое тестирование средств защиты информации (СЗИ) от НСД.

4.5. Наличие средств восстановления СЗИ от НСД.

4.6. Использование сертифицированных средств защиты.

Проверка соответствия требованиям по защите информации от НСД для АС производится в рамках сертификационных или аттестационных испытаний.

3.3.5. Средства вычислительной техники. Межсетевые экраны. Защита от НСД. Показатели защищённости от НСД к информации

Руководящий документ [31] устанавливает классификацию межсетевых экранов по уровню защищённости от НСД к информации на базе перечня показателей защищённости и совокупности описывающих их требований.

Показатели защищённости применяются к межсетевым экранам (МЭ) для определения уровня защищённости, который они обеспечивают при межсетевом взаимодействии.

Устанавливаются ***5 классов защищённости МЭ***, однозначно сопоставленных с классами автоматизированных систем (табл. 3.3.5).

Таблица 3.3.5. Соответствие классов защищённости МЭ и АС

Класс МЭ	Класс АС
5	1Д
4	1Г
3	1В
2	1Б
1	1А

Тем самым, для каждого класса защищённости АС определён класс МЭ, который должен применяться для осуществления безопасного взаимодействия АС с внешней средой.

Принадлежность к тому или иному классу МЭ определяется путём анализа соответствия следующим показателям защищённости:

1. Управление доступом (фильтрация данных и трансляция адресов). Для различных классов защищённости фильтрация производится на разных уровнях модели ISO/OSI.
2. Идентификация и аутентификация (входящих и исходящих запросов).
3. Регистрация.
4. Администрирования: идентификация и аутентификация.
5. Администрирование: регистрация.
6. Администрирование: простота использования.
7. Целостность.

8. Восстановление.
9. Тестирование (возможность проведения регламентного тестирования).
10. Руководство администратора защиты.
11. Тестовая документация.
12. Конструкторская (проектная) документация.

Ключевая особенность рассмотренного документа состоит в том, что классификация межсетевых экранов производится в том числе и по уровням модели ISO/OSI, на которых осуществляется фильтрация. Данный подход впервые был предложен именно в этом руководящем документе.

3.3.6. Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей

Руководящий документ [32] устанавливает классификацию программного обеспечения по уровню контроля отсутствия в нём недекларированных возможностей. Под ***недекларированными возможностями*** понимаются возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Одной из возможных реализаций недекларированных возможностей являются ***программные закладки*** – преднамеренно внесённые в программное обеспечение (ПО) функциональные объекты, которые при определённых условиях инициируют выполнение не описанных в документации функций ПО, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации.

Устанавливаются **4 уровня контроля**, каждый из которых характеризуется определённой совокупностью минимальных требований. В общем случае к ПО предъявляются следующие **требования**:

- **Требования к документации**
  - ***1. Контроль состава и содержания документации***
  - 1.1. Спецификация.
  - 1.2. Описание программы.
  - 1.3. Описание применения.
  - 1.4. Пояснительная записка.
  - 1.5. Тексты программ, входящих в состав программного обеспечения.
- **Требования к содержанию испытаний**
  - ***2. Контроль исходного состояния программного обеспечения.***
  - ***3. Статический анализ исходных текстов программ.***
  - 3.1. Контроль полноты и отсутствия избыточности исходных текстов.
  - 3.2. Контроль соответствия исходных текстов ПО его объектному (загрузочному) коду.
  - 3.3. Контроль связей функциональных объектов по управлению.
  - 3.4. Контроль связей функциональных объектов по информации.
  - 3.5. Контроль информационных объектов.
  - 3.6. Контроль наличия заданных конструкций в исходных текстах.

  - 3.7. Формирование перечня маршрутов выполнения функциональных объектов.
  - 3.8. Анализ критических маршрутов выполнения функциональных объектов (***критическим*** считается маршрут, при выполнении которого существует возможность неконтролируемого нарушения установленных правил обработки информационных объектов).
  - 3.9. Анализ алгоритма работы функциональных объектов на основе блок-схем, построенных по исходным текстам контролируемого программного обеспечения.
  - ***4. Динамический анализ исходных текстов программ***
  - 4.1. Контроль выполнения функциональных объектов.
  - 4.2. Сопоставление фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа.
  - ***5. Отчётность***

    Предъявляются требования к документам, разрабатываемым в ходе и по результатам проведённых испытаний.

Испытания, проводимые в соответствии с данным документом, должны содержать проверки, относящиеся к двум основным категориям – статическому и динамическому анализу. ***Статический анализ*** исходных текстов программ – это совокупность методов контроля соответствия реализованных и декларированных в документации функциональных возможностей ПО, основанных на структурном анализе и декомпозиции исходных текстов программ. В свою очередь, ***динамический анализ*** основывается на идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа. Статически и динамический методы анализа дополняют друг друга: результаты статического анализа используются при проведении динамического анализа.

3.4. Общие критерии

3.4.1. Введение

Как для «Оранжевой книги» [26], так и для в целом аналогичных ей руководящих документов Гостехкомиссии России [27-31], характерны многочисленные **недостатки**. Перечислим наиболее существенные из них:

- Документы ориентированы на обеспечение защиты информации от угроз нарушения конфиденциальности и, в определённой степени, целостности. Угрозы нарушения доступности практически не рассматриваются.
- Используемый «табличный» подход не позволяет учесть специфику конкретных систем или продуктов, в том числе порядок обработки информации в автоматизированной системе. Так, например, понятие «политика безопасности» в РД Гостехкомиссии России не упоминается.
- Документы содержат перечень механизмов, наличие которых необходимо для отнесения СВТ или АС к тому или иному классу защищённости. При этом совершенно не формализованы методы проверки корректности и адекватности реализации функциональных требований.

- Формулировки ряда требований чрезвычайно туманны и допускают неоднозначную интерпретацию.

В целом, РЛ Гостехкомиссии России и «Оранжевая книга», как и все другие оценочные стандарты первого поколения, создавались для давно ушедшей в прошлое материально-технической базы и по целому ряду аспектов являются морально устаревшими.

Стандарт ***ISO/IEC 15408-1999 "Common Criteria for Information Technology Security Evaluation"*** был разработан совместными усилиями специалистов Канады, США, Великобритании, Германии, Нидерландов и Франции в период с 1990 по 1999 год, развитие стандарта непрерывно продолжается. Исторически за стандартом закрепилось разговорное название ***"Common Criteria" – «Общие критерии»***.

В России аутентичный перевод «Общих критериев» версии 2.0 принят в качестве ГОСТ в 2002 году и введён в действие с 1 января 2004 г. Точное название документа: ***ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»***.

Документ состоит из трёх частей [33-35]:

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

В перспективе «Общие критерии» должны заменить РД Гостехкомиссии России во всех системах сертификации средств защиты информации. В настоящий момент оба поколения стандартов используются одновременно, причём «Общие критерии» применяются исключительно при проведении сертификации продуктов, не предназначенных для обработки информации, составляющей государственную тайну.

3.4.2. Основные идеи «Общих критериев»

Основное свойство «Общих критериев» (ОК) - это максимально возможная **универсальность**: под ***объектом оценки*** (ОО) понимается произвольный продукт информационных технологий или система с руководствами администратора и пользователя. ***Продукт*** рассматривается как совокупность программных, программно-аппаратных или аппаратных средств информационных технологий, предоставляющая определённые функциональные возможности и предназначенная для непосредственного использования или включения в состав различных систем. В свою очередь, ***система*** – это специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации.

Предполагается, что общие критерии могут быть использованы следующими **категориями пользователей**:

1. ***Потребители.***
   ОК позволяют определить, вполне ли оцениваемый продукт или система удовлетворяют их потребностям в безопасности.
2. ***Разработчики***
   Конструкции ОК могут быть использованы для формирования утверждения о соответствии объекта оценки установленным требованиям.

3. ***Оценщики***
   Стандарт может быть использован при формировании заключения о соответствии ОО предъявляемым к ним требованиям безопасности.

Объект оценки рассматривается в контексте **среды безопасности**, в которую включаются:

- ***законодательная среда*** – законы и нормативны акты, затрагивающие ОО;
- ***административная среда*** – положения политик безопасности, затрагивающих ОО и учитывающих его особенности;
- ***процедурная среда*** – меры физической защиты, персонал и его специфика;
- ***программно-техническая среда*** – назначение ОО, предполагаемые области его применения.

При подготовке к оценке формализуются следующие **аспекты среды ОО**:

1. ***Предположения безопасности***
   Предположения выделяют ОО из общего контекста и задают границы его рассмотрения. Предполагается, что среда ОО удовлетворяет данным предположениям. При проведении оценки предположения безопасности принимаются без доказательств.
2. ***Угрозы безопасности***
   Выделяются угрозы, наличие которых в рассматриваемой среде установлено или предполагается. Угроза характеризуется следующими параметрами:
   - источник угрозы;
   - предполагаемый способ реализации угрозы;
   - уязвимости, которые являются предпосылкой для реализации угрозы;
   - активы, которые являются целью нападения;
   - нарушаемые свойства безопасности активов;
   - возможные последствия реализации угрозы.
3. ***Политики безопасности***
   Излагаются положения политики безопасности, применяемые в организации, которые имеют непосредственное отношение к ОО.

На основании сформулированных предположений безопасности, при учёте угроз и политик формулируются ***цели безопасности*** для ОО, направленные на обеспечение противостояния угрозам и выполнение положений политики безопасности.

Для достижения поставленных целей к ОО и его среде предъявляются ***требования безопасности***. Вторая и третья части «Общих критериев» представляют собой каталоги требований безопасности следующих типов:

- ***Функциональные требования*** (Часть 2) – соответствуют активному аспекту защиты и предъявляются к функциям безопасности ОО и реализующим их механизмам.
- ***Требования доверия*** (Часть 3) – предъявляются к технологии и процессу разработки, эксплуатации и оценки ОО и призваны гарантировать адекватность реализации механизмов безопасности.

При формулировании требований к ОО могут быть разработаны два документа:

1. ***Профиль защиты*** – не зависящая от конкретной реализации совокупность требований информационных технологий для некоторой категории ОО.

Профиль защиты (ПЗ) непривязан к конкретному ОО и представляет собой обобщённый стандартный набор функциональных требований и требований доверия для определённого класса продуктов или систем. Например, может быть разработан профиль защиты на межсетевой экран корпоративного уровня или на биллинговую систему.

Именно каталог утверждённых профилей защиты должен послужить заменой традиционных руководящих документов Гостехкомиссии России.

2. ***Задание по безопасности*** – документ, содержащий требования безопасности ля конкретного ОО и специфицирующий функции безопасности и меры доверия, предлагаемые объектом оценки для выполнения установленных требований. В задании по безопасности (ЗБ) может быть заявлено соответствие одному или нескольким профилям защиты.

ЗБ можно рассматривать как техническое задание на подсистему обеспечения информационной безопасности для ОО.

Задание по безопасности служит основой для проведения оценки ОО с целью демонстрации соответствия его требованиям безопасности.

Нетрудно видеть, что по сравнению с традиционными стандартами «Общие критерии» представляют собой принципиально более гибкий и универсальный инструмент. Однако стандарт не претендует на всеобъемлющую универсальность и, в частности, имеет следующие **ограничения**:

1. ОК не содержат критериев оценки, касающихся администрирования механизмов безопасности, непосредственно не относящихся к мерам безопасности информационных технологий (управление персоналом, вопросы физической безопасности и т.д.). Соответствующие аспекты в рамках «Общих критериев» могут рассматриваться исключительно в виде предположений безопасности. Предполагается, что оценка соответствующих механизмов должна проводиться с использованием других стандартов.
2. Вопросы защиты информации от утечки по техническим каналам, такие как контроль ПЭМИН, непосредственно не затрагиваются, хотя многие концепции ОК потенциально применимы и в данной области.
3. В ОК не рассматриваются ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки.
4. Процедуры использования результатов оценки при аттестации продуктов и систем находятся вне области действия ОК.
5. В ОК не входят критерии оценки специфических свойств криптографических алгоритмов. Независимая оценка математических свойств криптографических компонентов, встроенных в ОО, должна проводиться как самостоятельная независимая процедура.

3.4.3. Структура и содержание профиля защиты

Структура профиля защиты приведена на рис. 3.4.3.

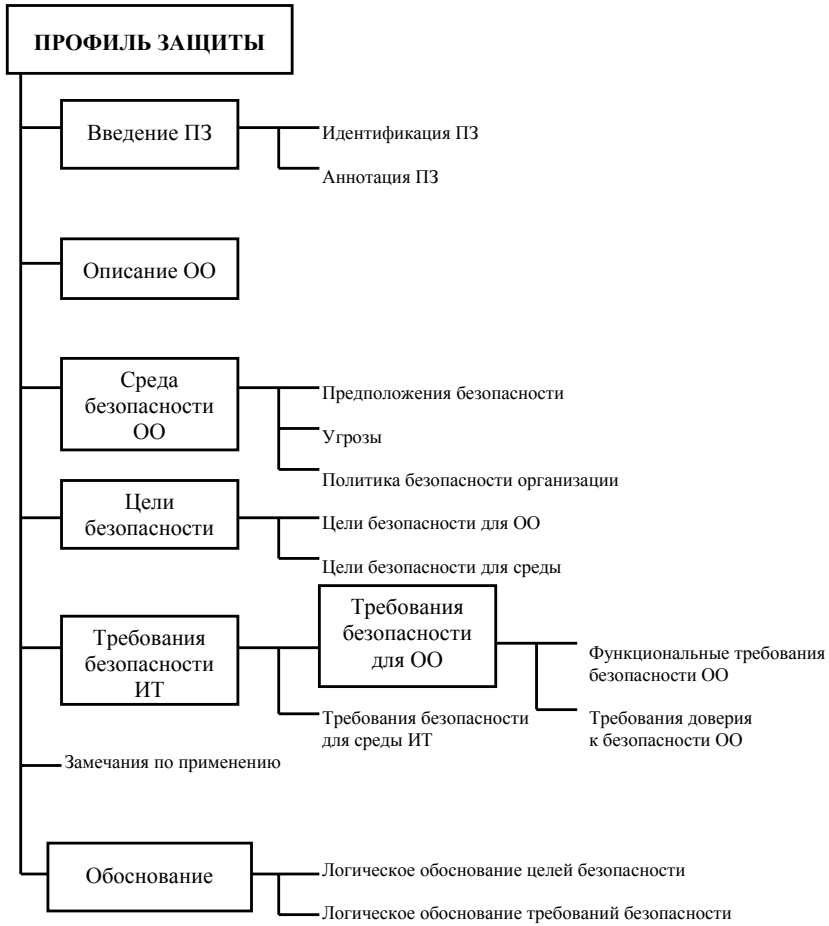

Рис. 3.4.3. Структура профиля защиты

Введение ПЗ должно содержать информацию управления документооборотом и обзорную информацию, необходимые для работы с реестром ПЗ:

- **идентификация ПЗ** должна обеспечить маркировку и описательную информацию, ***необходимые***, чтобы идентифицировать, каталогизировать, регистрировать ПЗ и ссылаться на него;
- **аннотация ПЗ** должна дать общую характеристику ПЗ в описательной форме. Она должна быть достаточно подробной, чтобы потенциальный пользователь ПЗ мог решить, представляет ли ПЗ для него интерес. Аннотация должна быть также применима для размещения в виде самостоятельного реферата в каталогах и реестрах ПЗ.

Описание ОО служит цели лучшего понимания его требований безопасности и даёт представление о типе продукта и основных характерных особенностях ИТ применительно к ОО. Описание ОО предоставляет контекст для оценки. Информация, содержащаяся в описании ОО, будет использована в процессе оценки для выявления противоречий. Поскольку ПЗ обычно не ссылается на конкретную реализацию, то характерные особенности ОО могут быть представлены в виде предположений.

Изложение ***среды безопасности ОО*** должно содержать описание аспектов безопасности среды, в которой предполагается использовать ОО, и ожидаемый способ его применения. Это изложение должно включать:

1. Описание ***предположений,*** содержащее аспекты безопасности среды, в которой ОО будет использоваться или предполагается к использованию. Оно должно включать в себя:
   - информацию относительно предполагаемого использования ОО, включая такие аспекты, как предполагаемая область применения, потенциальная значимость активов и возможные ограничения использования;
   - информацию относительно среды применения ОО, включая аспекты физического окружения, персонала и внешних связей.
2. Описание ***угроз***, включающее все те угрозы активам, против которых требуется защита средствами ОО или его среды. Заметим, что необходимо приводить не все угрозы, которые могут встретиться в среде, а только те из них, которые влияют на безопасную эксплуатацию ОО. Если цели безопасности ОО следуют только из политики безопасности организации и предположений, то описание угроз может быть опущено.
3. Описание ***политики безопасности организации***, идентифицирующее и, при необходимости, объясняющее все положения политики безопасности организации или правила, которым должен подчиняться объект оценки. Если цели безопасности следуют только из угроз и предположений безопасности, описание политики безопасности организации может быть опущено.

Изложение ***целей безопасности*** должно определять цели безопасности как для ОО, так и для его среды. Цели безопасности должны учитывать все установленные аспекты среды безопасности. Цели безопасности должны отражать изложенное намерение противостоять всем установленным угрозам и быть подходящими для этого, а также охватывать все предположения безопасности и установленную политику безопасности организации.

Цели безопасности для ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым необходимо противостоять средствами ОО, или с политикой безопасности организации, которой должен отвечать ОО.

Цели безопасности для среды ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым не полностью противостоит ОО, или с политикой безопасности организации и предположениями, не полностью удовлетворяемыми ОО.

Цели безопасности для среды могут повторять, частично или полностью, некоторые предположения, сделанные при изложении среды безопасности ОО.

При изложении ***требований безопасности ОО*** должны быть определены функциональные требования и требования доверия, которым должны удовлетворять ОО и свидетельства поддержки его оценки для достижения целей безопасности ОО.

При изложении ***функциональных требований безопасности ОО*** следует определять функциональные требования к ОО, где это возможно, как функциональные компоненты, выбираемые из части 2 ОК. В случае необходимости, требования формулируются в явном виде, однако при их изложении необходимо сохранять стилистику «Общих критериев».

При выборе компонентов функциональных требований из части 2 ОК, над ними могут быть осуществлены следующие **операции**:

- ***итерация***, позволяющая неоднократно использовать компонент при различном выполнении в нем операций;
- ***назначение***, позволяющее специфицировать параметр, устанавливаемый при использовании компонента;
- ***выбор***, позволяющий специфицировать пункты, которые выбираются из перечня, приведенного в компоненте;
- ***уточнение***, позволяющее осуществлять дополнительную детализацию при использовании компонента.

Требования доверия к безопасности ОО обычно формулируются как один из приведённых в части 3 ОК ***оценочных уровней доверия*** (ОУД) – стандартных наборов требований доверия. При этом допускается:

- ***усиливать*** выбранный уровень доверия компонентами из других ОУД;
- явным образом формулировать требования доверия, не содержащиеся в части 3 ОК.

Необязательное изложение ***требований безопасности для среды ИТ*** должно определять требования безопасности ИТ, которым должна отвечать среда ИТ этого ОО. Если безопасность ОО не зависит от среды ИТ, то эта часть ПЗ может быть опущена.

Хотя требования безопасности среды, не относящиеся к ИТ, часто бывают полезны на практике, не требуется, чтобы они являлись формальной частью ПЗ, поскольку они не связаны непосредственно с реализацией ОО.

Раздел ПЗ ***Замечания по применению*** является необязательным и может содержать дополнительную информацию, которая считается уместной или полезной для создания, оценки и использования ОО.

Обоснование ПЗ поддерживает утверждения о том, что ПЗ является полной и взаимосвязанной совокупностью требований, и что соответствующий ему ОО обеспечит эффективный набор контрмер безопасности ИТ в определенной среде безопасности. Обоснование должно **включать**:

- ***логическое обоснование целей безопасности***, демонстрирующее, что изложенные цели безопасности сопоставлены со всеми идентифицированными аспектами среды безопасности ОО и пригодны для их охвата
- ***логическое обоснование требований безопасности***, демонстрирующее, что совокупность требований безопасности ОО и его среды пригодна для достижения целей безопасности и сопоставима с ними.

При изложении **логического обоснования требований безопасности** должно быть продемонстрировано следующее:

1. Сочетание отдельных компонентов функциональных требований и требований доверия для ОО и его среды ИТ в совокупности отвечает изложенным целям безопасности.
2. Данный набор требований безопасности образует единое и внутренне непротиворечивое целое. В частности, должны быть удовлетворены все существующие ***зависимости*** между функциональными требованиями.
3. Выбор требований безопасности строго обоснован. Каждое из перечисленных ниже условий должно быть строго обосновано:
   - выбор требований, не содержащихся в частях 2 или 3 ОК;
   - выбор требований доверия, не включенных в какой-либо ОУД;
   - случаи неудовлетворения зависимостей.
4. Выбранный для ПЗ уровень стойкости функций и заявленная в явном виде стойкость функций согласуются с целями безопасности для ОО.

3.4.4. Структура и содержание задания по безопасности

Структура задания по безопасности приведена на рис. 3.4.4. В целом структура ЗБ аналогична ПЗ, все изменения связаны с включением информации, относящейся к специфике реализации конкретного ОО.

В целом ЗБ должно быть оформлено как документ, максимально ориентированный на пользователя – с минимумом ссылок на внешние материалы.

Раздел ***Соответствие ОК*** должен содержать все поддающиеся оценке **утверждение о соответствии ОО Общим критериям**. Такие утверждения могут звучать следующим образом:

- ***соответствие части 2***, если в ЗБ при изложении функциональных требований безопасности используются исключительно компоненты из части 2 ОК;
- ***расширение части 2***, если в изложение функциональных требований включены компоненты, отсутствующие в части2 ОК;
- ***соответствие части 3,*** если требования доверия представлены в виде ОУД из части 3 ОК или пакета требований доверия, включающего только компоненты доверия из части 3 ОК;
- ***усиление части 3,*** если требования доверия представлены в виде ОУД или пакета требований доверия и включают другие компоненты доверия из части 3 ОК.
- ***расширение части 3,*** если требования доверия представлены в виде ОУД, дополненного требованиями доверия не из части 3 ОК, или пакета требований доверия, который включает требования доверия, не содержащиеся в части 3 ОК или полностью состоит из них.
- ***соответствие ПЗ*** - ОО соответствует ПЗ только в том случае, если он соответствует всем частям этого ПЗ.

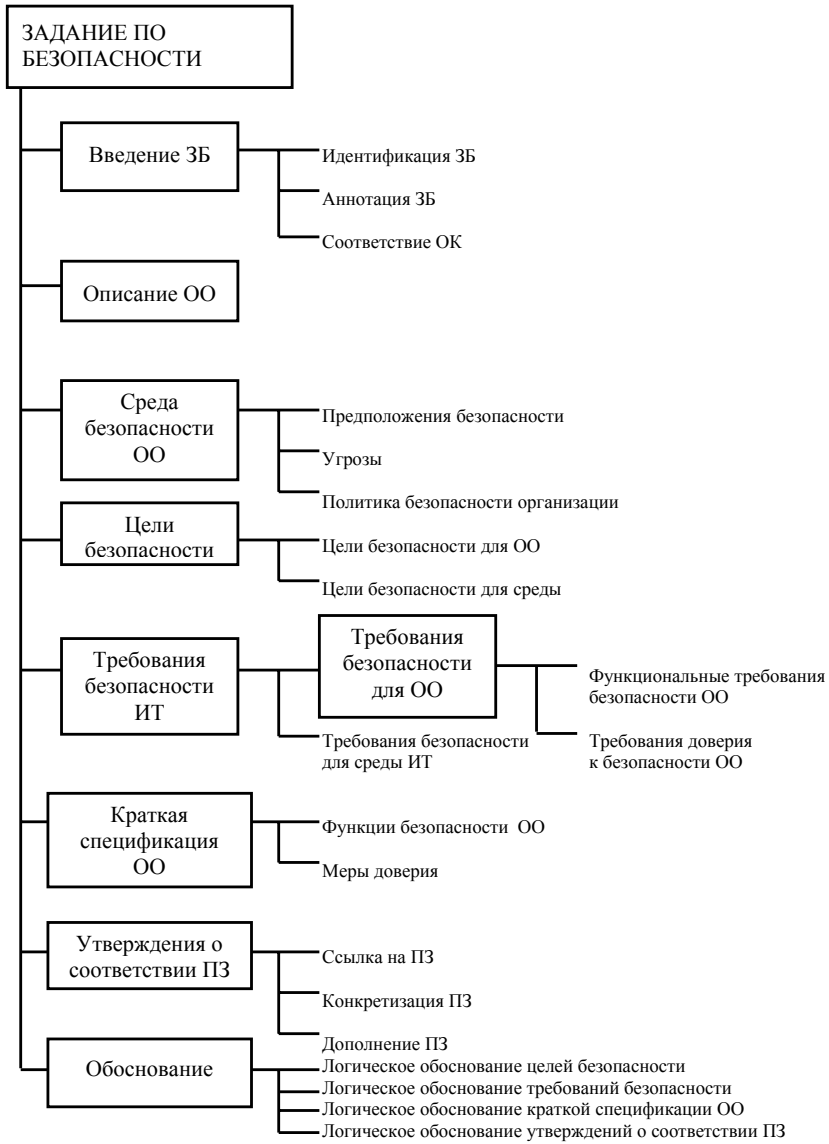

Рис. 3.4.4. Структура задания по безопасности

Краткая спецификация ОО должна определить отображение требований безопасности для ОО. Эта спецификация должна предоставить описание функций безопасности и мер доверия к ОО, которые отвечают требованиям безопасности ОО.

Краткая спецификация должна включать:

1. ***Изложение функций безопасности ОО***, которое должно охватывать все функции безопасности ИТ и определять, каким образом эти функции удовлетворяют функциональным требованиям безопасности ОО. Изложение должно включать двунаправленное сопоставление функций и требований с четким указанием, какие функции каким требованиям удовлетворяют, и что удовлетворены все требования. Каждая функция безопасности должна участвовать в удовлетворении, по меньшей мере, одного функционального требования безопасности ОО.

   Функции безопасности ИТ должны быть определены неформальным образом на уровне детализации, необходимом для понимания их предназначения. Все ссылки в ЗБ на механизмы безопасности должны быть сопоставлены с соответствующими функциями безопасности так, чтобы было видно, какие механизмы безопасности используются при реализации каждой функции.
2. ***Изложение мер доверия***, которое должно специфицировать меры доверия к ОО, заявленные для удовлетворения изложенных требований доверия. Меры доверия должны быть сопоставлены с требованиями таким образом, чтобы было понятно, какие меры в удовлетворении каких требований участвуют

   Там, где это возможно, меры доверия могут быть определены путем ссылки на соответствующие планы обеспечения качества, жизненного цикла или управления.

В ***утверждение о соответствии ПЗ*** включаются материалы, необходимые для подтверждения факта соответствия.

Если сделано утверждение о соответствии одному или нескольким ПЗ, то изложение утверждений о соответствии должно содержать **следующий материал** для каждого ПЗ:

- ***Ссылку на ПЗ***, идентифицирующую ПЗ, соответствие которому утверждается, плюс любые дополнительные материалы, которые могут потребоваться в соответствии с этим утверждением. Обоснованное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.
- ***Конкретизацию ПЗ***, идентифицирующую те требования безопасности ИТ, в которых выполняются операции, разрешенные в ПЗ, или дополнительно уточняются требования ПЗ.
- ***Дополнение ПЗ***, идентифицирующее цели и требования безопасности ОО, которые дополняют цели и требования ПЗ.

Случай, когда в ЗБ утверждается о частичном соответствии ПЗ, не приемлем для оценки в рамках ОК.

Логическое обоснование краткой спецификации ОО, показывает, что функции безопасности и меры доверия к ОО пригодны, чтобы отвечать требованиям безопасности ОО. Должно быть продемонстрировано следующее:

- сочетание специфицированных для ОО функций безопасности ИТ при совместном использовании удовлетворяет функциональным требованиям безопасности ОО;

- справедливы сделанные утверждения о стойкости функций безопасности ОО либо заявление, что в таких утверждениях нет необходимости;
- строго обосновано утверждение, что изложенные меры доверия соответствуют требованиям доверия.

Уровень детализации логического обоснования должен соответствовать уровню детализации определения функций безопасности.

Логическое обоснование утверждений о соответствии ПЗ объясняет любые различия между целями и требованиями безопасности ЗБ и любого ПЗ, соответствие которому утверждается. Эта часть ЗБ может быть опущена, если не сделано утверждений о соответствии ПЗ, или если цели и требования безопасности ЗБ и каждого ПЗ, соответствие которому утверждается, полностью совпадают.

3.4.5. Функциональные требования безопасности

Систематизированный каталог функциональных требований безопасности сосредоточен во второй части ОК [34]. Функциональные требования разбиты на 11 классов, 66 семейств и 135 компонентов.

Структура функционального класса приведена на рис. 3.4.5.1.

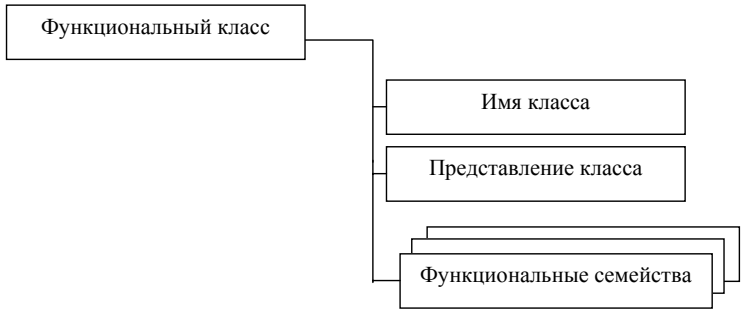

Рис. 3.4.5.1. Структура функционального класса

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.

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

Структура функционального семейства приведена на рис. 3.4.5.2.

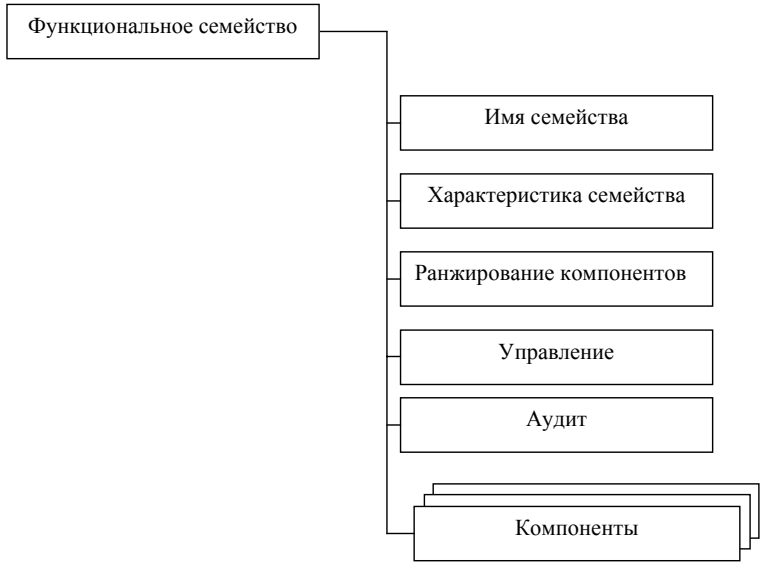

Рис. 3.4.5.2. Структура функционального семейства

Каждое функциональное семейство имеет уникальное ***имя***. Первые три символа идентичны краткому имени класса, далее следуют символ подчеркивания и краткое имя семейства в виде XXX_YYY.

Характеристика семейства – это описание функционального семейства, в котором излагаются его цели безопасности и общее описание функциональных требований. ***Цели безопасности*** семейства характеризуют задачу безопасности, которая может быть решена с помощью ОО, включающего компонент из этого семейства. ***Описание функциональных требований*** обобщает все требования, которые включены в компоненты.

Цель ***ранжирования компонентов*** – предоставить пользователям информацию для выбора подходящего функционального компонента из семейства.

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

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*).

Требования ***аудита*** содержат события, потенциально подвергаемые аудиту, для их отбора разработчиками ПЗ/ЗБ при условии включения в ПЗ или 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 на разных **уровнях детализации**, 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.

Структура функционального компонента приведена на рисунке 3.4.5.3.

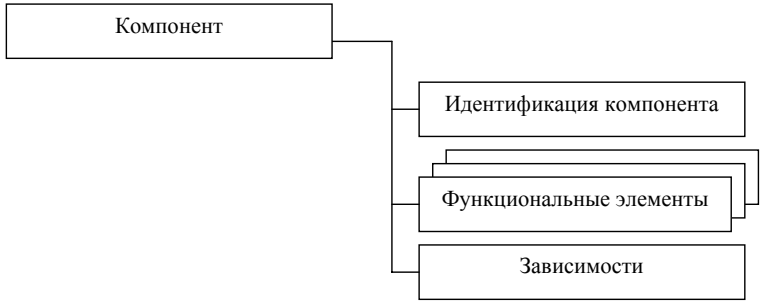

Рис. 3.4.5.3. Структура функционального компонента

Идентификация компонента включает описательную информацию, необходимую для идентификации, категорирования, записи и реализации перекрестных ссылок компонента. Для каждого функционального компонента представляется следующая информация:

- 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.

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

Функциональный элемент – это наименьшее функциональное требование безопасности, идентифицируемое и признаваемое в ОК. При формировании ПЗ или ЗБ не разрешается выбирать только часть элементов компонента – необходимо использовать всю их совокупность.

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.

Зависимости среди функциональных компонентов возникают, когда компонент не самодостаточен и нуждается либо в функциональных возможностях другого компонента, либо во взаимодействии с ним для поддержки собственного выполнения. Список зависимостей идентифицирует минимум функциональных компонентов или компонентов доверия, необходимых для удовлетворения требований безопасности, ассоциированных с данным компонентом. Компоненты, которые иерархичны по отношению к компоненту из списка, также могут быть использованы для удовлетворения зависимости.

Зависимости между компонентами, указанные в части 2 ОК, являются обязательными, и их необходимо удовлетворить при разработке профиля защиты или задания по безопасности. В тех редких случаях, когда эти зависимости удовлетворить невозможно, соответствующее строгое обоснование должно быть приведено в ПЗ или ЗБ.

Классы и семейства представлены во второй части ОК в алфавитном порядке. В начале каждого класса имеется рисунок, показывающий таксономию этого класса, перечисляя семейства в этом классе и компоненты в каждом семействе. Рисунок также иллюстрирует иерархию компонентов внутри каждого семейства.

Пример представления таксономии класса и иерархии компонентов в его семействах приведен на рисунке 3.4.5.4.

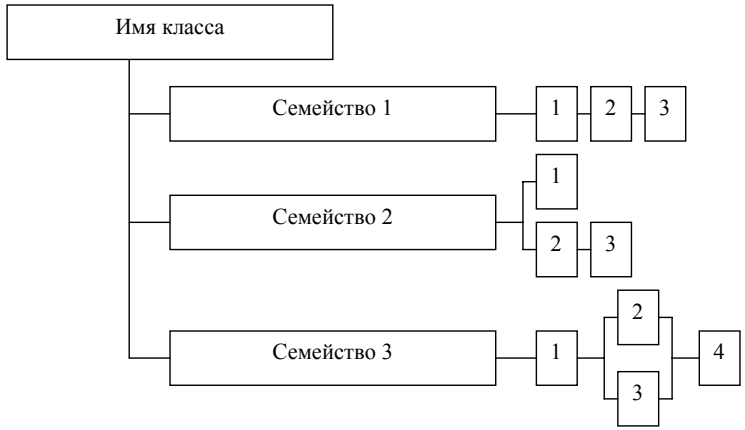

Рис. 3.4.5.4. Пример представления класса

Семейство 1 на рис. 3.4.5.4 содержит три иерархических компонента, где компоненты 2 и 3 могут быть применены для выполнения зависимостей вместо компонента 1. Компонент 3 иерархичен к компоненту 2 и может применяться для выполнения зависимостей вместо компонента 2.

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

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

В таблице 3.4.5 приведена краткая характеристика всех 66 семейств функциональных требований.

Таблица 3.4.5. Семейства функциональных требований

№ п/п	Семейство	Наименование	Характеристика
Класс *FAU* - ***аудит безопасности***			
1	FAU_ARP	Автоматическая реакция аудита безопасности	Определяются действия, которые необходимо предпринять при выявлении возможных нарушений безопасности.
2	FAU_GEN	Генерация данных аудита	– Выбираются события, потенциально подвергаемые аудиту и протоколированию. – Определяется минимум регистрируемых данных о событиях безопасности. – Осуществляется привязка событий к идентификаторам вызвавших их пользователей.
3	FAU_SAA	Анализ аудита безопасности	Устанавливаются требования к средствам аудита безопасности, функционирующим: – на базе правил; – на базе профилей поведения пользователей; – на базе сигнатур атак.
4	FAU_SAR	Просмотр аудита безопасности	– Определяются требования к представлению данных аудита. – Предоставляются права на просмотр записей аудита уполномоченным

№ п/п	Семейство	Наименование	Характеристика
			пользователям.
5	FAU_SEL	Выбор событий аудита безопасности	– Определяются требования по отбору реально протоколируемых событий из числа потенциально подвергаемых протоколированию. – Выделяются атрибуты, по которым производится отбор событий.
6	FAU_STG	Хранение данных аудита безопасности	– Определяются требования по защите данных аудита от НСД и повреждения. – Определяется последовательность действий, выполняемых системой при переполнении журнала аудита.
Класс *FCO – **связь***			
7	FCO_NRO	Неотказуемость отправления	Задаются требования по ассоциации атрибутов отправителя информации с элементами передаваемых данных.
8	FCO_NRR	Неотказуемость получения	Задаются требования по ассоциации атрибутов получателя информации с элементами передаваемых данных.
Класс *FCS - **криптографическая поддержка***			
9	FCS_CKM	Управление криптографическими ключами	Задаются требования к реализации механизмов генерации, распределения и уничтожения криптографических ключей.
10	FCS_COP	Криптографические операции	Декларируется использование тех или иных криптографических средств защиты информации.
Класс *FDP – **защита данных пользователя***			
11	FDP_ACC	Политика управления доступом	Идентифицируются применяемые политики управления доступом.
12	FDP_ACF	Функции управления доступом	Описываются правила работы функций, реализующих заявленные политики безопасности.
13	FDP_DAU	Аутентификация данных	Определяется порядок генерации и использования данных

№ п/п	Семейство	Наименование	Характеристика
			аутентификации.
14	FDP_ETC	Экспорт данных за пределы действия ФБО	Определяется порядок экспорта данных за пределы области действия функций безопасности объекта оценки.
15	FDP_IFC	Политика управления информационными потоками	– Устанавливаются имена и определяется области действия политик, управляющих информационными потоками. – Задаются требования к покрытию данными политиками всех операций перемещения информации.
16	FDP_IFF	Функции управления информационными потоками	– Требуется наличие правил управления информационными потоками. – Определяются правила контроля информационных потоков и управления ими.
17	FDP_ITC	Импорт данных из-за пределов действия ФБО	Определяется порядок импорта данных из-за пределов области действия функций безопасности объекта оценки.
18	FDP_ITT	Передача в пределах ОО	Определяется порядок защиты данных пользователя при их передаче между различными частями ОО по внутреннему каналу.
19	FDP_RIP	Защита остаточной информации	Задаются требования по уничтожению предыдущего содержания ресурсов АС при их освобождении.
20	FDP_ROL	Откат	Требуется обеспечение возможности отмены последней выполненной операции (или ряда операций) и возврата к предыдущему состоянию.
21	FDP_SDI	Целостность хранимых данных	Задаются требования по контролю целостности данных пользователя.
22	FDP_UCT	Защита конфиденциальности данных пользователя при передаче между ФБО	Определяются требования по обеспечению конфиденциальности данных пользователя при их передаче по внешнему каналу между ОО и доверенными

№ п/п	Семейство	Наименование	Характеристика
			внешними объектами ИТ.
23	FDP_UIT	Защита целостности данных пользователя при передаче между ФБО	– Определяются требования по защите целостности данных пользователя при передаче между ФБО. – Задаются требования к механизмам коррекции ошибок.
Класс *FIA* – ***идентификация и аутентификация***			
24	FIA_AFL	Отказы аутентификации	Задаётся реакция на неудачные запросы аутентификации.
25	FIA_ATD	Определение атрибутов пользователя	Определяются атрибуты пользователей, отличные от идентификаторов и используемые для реализации установленных политик.
26	FIA_SOS	Спецификация секретов	Задаются требования к механизмам проверки качества и генерации секретов (данных аутентификации).
27	FIA_UAU	Аутентификация пользователя	– Задаются требования к реализации механизмов аутентификации. – Определяются механизмы, доступные до осуществления аутентификации пользователя.
28	FIA_UID	Идентификация пользователя	– Задаётся порядок идентификации пользователя. – Определяются действия, которые могут быть выполнены до идентификации пользователя.
29	FIA_USB	Связывание пользователь-субъект	Определяется связь атрибутов безопасности пользователя с субъектом, действующим от имени пользователя.
Класс *FMT* – ***управление безопасностью***			
30	FMT_MOF	Управление отдельными функциями ФБО	Определяются пользователи, уполномоченные осуществлять управление режимами выполнения функций безопасности.
31	FMT_MSA	Управление атрибутами безопасности	– Определяются пользователи, уполномоченные осуществлять управление атрибутами

№ п/п	Семейство	Наименование	Характеристика
			безопасности. – Регламентируется порядок контроля безопасности параметров данных атрибутов.
32	FMT_MTD	Управление данными ФБО	– Определяются пользователи, уполномоченные осуществлять управление ФБО. – Определяются граничные значения данных функций безопасности и действия в случае выхода за допустимые границы.
33	FMT_REV	Отмена	Определяется порядок отмены атрибутов безопасности пользователей, субъектов и объектов.
34	FMT_SAE	Срок действия атрибута безопасности	Задаются мероприятия, выполняемы по окончании срока действия атрибутов безопасности.
35	FMT_SMR	Роли управления безопасностью	Задаются различные роли пользователей системы и создаются правила, управляющие отношениями между ролями.
Класс *FPR* – ***приватность***			
36	FPR_ANO	Анонимность	Задаётся возможность выполнения определённых действий без запроса идентификатора пользователя
37	FPR_PSE	Псевдонимность	Определяется возможность использования ресурсов без раскрытия идентификатора пользователя, но с сохранением подотчётности.
38	FPR_UNL	Невозможность ассоциации	Требуется невозможность ассоциирования пользователя с применяемым им сервисом (может потребоваться для защиты от построения поведенческих моделей пользователя).
39	FPR_UNO	Скрытность	Требуется предоставление пользователю возможности работы с определёнными сервисами незаметно для кого бы то ни было.
Класс *FPT* – ***защита ФБО***			

№ п/п	Семейство	Наименование	Характеристика
40	FPT_AMT	Тестирование базовой абстрактной машины	Задаются требования, к тестированию, демонстрирующему правильность предположений, обеспечиваемых программно-аппаратной платформой, лежащей в основе функций безопасности.
41	FPT_FLS	Безопасность при сбое	Перечисляются типы сбоев, которые не должны приводить к нарушению безопасности системы.
42	FPT_ITA	Доступность экспортируемых данных ФБО	Определяются правила предотвращения потери доступности экспортируемых данных функций безопасности.
43	FPT_ITC	Конфиденциальность экспортируемых данных ФБО	Определяются правила защиты от несанкционированного раскрытия экспортируемых данных функций безопасности.
44	FPT_ITI	Целостность экспортируемых данных ФБО	Определяются правила защиты от несанкционированной модификации экспортируемых данных функций безопасности.
45	FPT_ITT	Передача данных ФБО в пределах ОО	Регламентируются требования защиты данных функций безопасности при их передаче между разделенными частями ОО по внутреннему каналу
46	FPT_PHP	Физическая защита ФБО	Требуется наличие средств выявления и реагирования на несанкционированный физический доступ к компонентам ОО.
47	FPT_RCV	Надежное восстановление	Требуется наличие возможности корректного автоматического или ручного восстановления функций безопасности после сбоев.
48	FPT_RPL	Обнаружение повторного использования	Задаются требования по обнаружению повторного использования сущностей различных типов и последующими действиями по его устранению.
49	FPT_RVM	Посредничество при обращениях	Задаются требования по реализации концепции монитора безопасности обращений.
50	FPT_SEP	Разделение домена	Формулируются требования по организации защищённого домена для каждой функции безопасности.

№ п/п	Семейство	Наименование	Характеристика
51	FPT_SSP	Протокол синхронизации состояний	Требуется надёжное подтверждение при обмене данными между функциями безопасности в распределённой среде.
52	FPT_STM	Метки времени	Требуется предоставление надёжных меток времени в пределах ОО (что необходимо, например, для корректной работы механизмов протоколирования).
53	FPT_TDC	Согласованность данных ФБО между ФБО	Задаются требования по согласованности интерпретации данных, совместно используемых различными функциями безопасности и другими доверенными изделиями ИТ.
54	FPT_TRC	Согласованность данных ФБО при дублировании в пределах ОО	Определяются требования по синхронизации данных, дублируемых в пределах ОО.
55	FPT_TST	Самотестирование ФБО	Задаются требования по самотестированию функций безопасности в части типичных операций с известным результатом.
Класс *FRU* – ***использование ресурсов***			
56	FRU_FLT	Отказоустойчивость	Требуется корректное выполнение части функциональных возможностей в случае сбоев.
57	FRU_PRS	Приоритет обслуживания	Определяется порядок применения высокоприоритетных операций.
58	FRU_RSA	Распределение ресурсов	Задаются требования к механизму квотирования, используемому для достижения высокой доступности ресурсов.
Класс *FTA* – ***доступ к ОО***			
59	FTA_LSA	Ограничение области выбираемых атрибутов	Определяются ограничения на атрибуты безопасности сеанса, которые может выбирать пользователь.
60	FTA_MCS	Ограничение на параллельные сеансы	Задаются требования по ограничению числа параллельных сеансов, предоставляемых одному и тому же пользователю.
61	FTA_SSL	Блокирование сеанса	Определяется возможность

№ п/п	Семейство	Наименование	Характеристика
			блокирования и разблокирования интерактивного сеанса работы пользователя (по желанию пользователя или по инициативе функций безопасности).
62	FTA_TAB	Предупреждения перед предоставлением доступа к ОО	Определяются требования к отображению для пользователей предупреждающего сообщения относительно характера использования ОО.
63	FTA_TAH	История доступа к ОО	Задаются требования по отображению для пользователя при успешном открытии сеанса истории успешных и неуспешных попыток получить доступ от имени этого пользователя.
64	FTA_TSE	Открытие сеанса с ОО	Задаются параметры функций безопасности, на основании которых пользователю может быть отказано в доступе.
Класс *FTP* – ***доверенный маршрут/канал***			
65	FTP_ITC	Доверенный канал передачи между ФБО	– Определяются правила организации доверенного канала между функциями безопасности и другими доверенными продуктами ИТ. – Определяется порядок идентификации взаимодействующих сторон.
66	FTP_TRP	Доверенный маршрут	Определяется порядок организации канала защищённого взаимодействия между пользователями и функциями безопасности.

Наличие каталога функциональных требований не предполагает их окончательный и всеобъемлющий характер. В случае необходимости, функциональные требования безопасности, которые отсутствуют в каталоге, могут быть сформулированы в явном виде.

3.4.6. Требования доверия

Требования доверия, приведённые в третьей части ОК [35], сгруппированы в 10 классов, 44 семейства и 93 компонента.

Доверие – основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности. Доверие могло бы быть получено путем обращения к таким источникам, как бездоказательное утверждение, предшествующий аналогичный опыт или специфический опыт. Однако ОК обеспечивают доверие с использованием активного исследования. ***Активное исследование*** – это оценка продукта или системы ИТ для определения его свойств безопасности.

Методы оценки могут включать:

- анализ и проверку процессов и процедур;
- проверку, что процессы и процедуры действительно применяются;
- анализ соответствия между представлениями проекта ОО;
- анализ соответствия каждого представления проекта ОО требованиям;
- верификацию доказательств;
- анализ руководств;
- анализ разработанных функциональных тестов и полученных результатов;
- независимое функциональное тестирование;
- анализ уязвимостей, включающий предположения о недостатках;
- тестирование проникновением.

Наиболее общую совокупность требований доверия называют ***классом***. Каждый класс содержит семейства доверия, которые разделены на компоненты доверия, содержащие, в свою очередь, элементы доверия.

Структура класса доверия приведена на рис. 3.4.6.1.

Каждому классу доверия присвоено уникальное ***имя***. Имя указывает на тематические разделы, на которые распространяется данный класс доверия. Принятое условное обозначение включает в себя букву «*A*», за которой следуют еще две буквы латинского алфавита, относящиеся к имени класса.

Каждый класс доверия имеет вводный подраздел – ***представление класса***, в котором описаны состав и назначение класса.

Каждый класс доверия содержит по меньшей мере одно ***семейство доверия*** (см. рис. 3.4.6.1).

Каждому семейству доверия присвоено уникальное ***имя***. Имя содержит описательную информацию по тематическим разделам, на которые распространяется данное семейство доверия. Каждое семейство доверия размещено в пределах класса доверия, который содержит другие семейства той же направленности.

Представлена также уникальная ***краткая форма имени*** семейства доверия. Она является основным средством для ссылки на семейство доверия. Принятое условное обозначение включает в себя краткую форму имени класса и символ подчеркивания, за которым следуют три буквы латинского алфавита, относящиеся к имени семейства

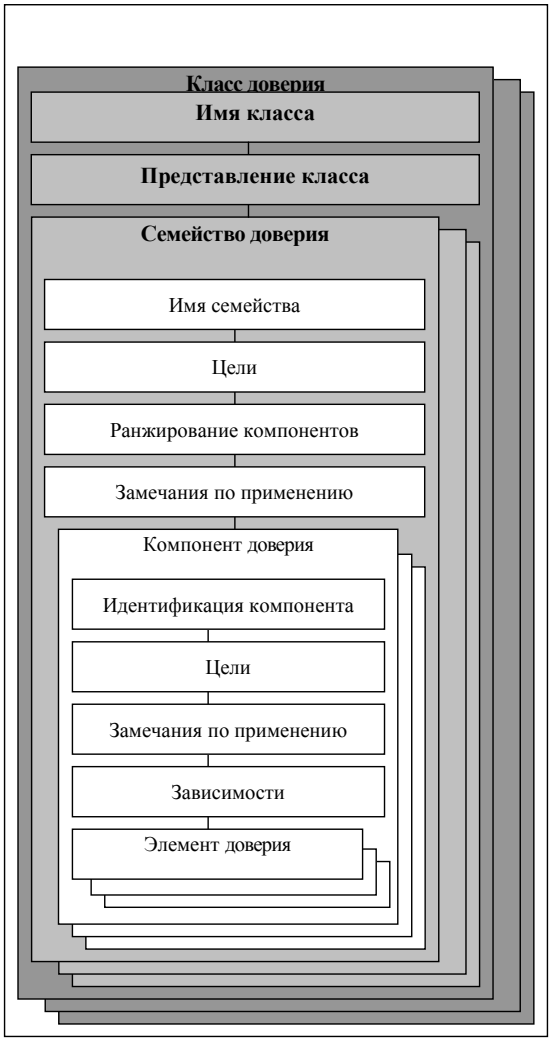

Рис. 3.4.6.1. Структура класса доверия

Описание ***целей*** для семейства доверия представлено в общем виде. Любые конкретные подробности, требуемые для достижения целей, включены в конкретный компонент доверия.

Подраздел ***«Ранжирование компонентов»*** семейства доверия содержит описание имеющихся компонентов и объяснение их разграничения. Его основная цель состоит в

указании различий между компонентами при принятии решения о том, что семейство является необходимой или полезной частью требований доверия для ПЗ/ЗБ.

Необязательный подраздел ***«Замечания по применению»*** содержит дополнительную информацию о семействе, например, предупреждения об ограничениях использования или областях, требующих особого внимания.

Структура компонента доверия приведена на рис. 3.4.6.2.

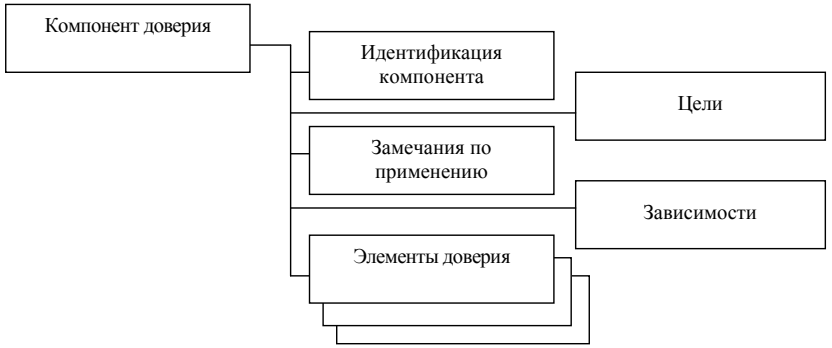

Рис. 3.4.6.2. Структура компонента доверия

Подраздел ***«Идентификация компонента»*** содержит описательную информацию, необходимую для идентификации, категорирования, регистрации и ссылок на компонент. Каждому компоненту доверия присвоено уникальное ***имя***. Имя содержит информацию о тематических разделах, на которые распространяется компонент доверия. Каждый компонент входит в состав конкретного семейства доверия, с которым имеет общую цель безопасности.

Представлена также уникальная ***краткая форма имени*** компонента доверия как основной способ ссылки на компонент. Принято, что за краткой формой имени семейства следует точка, а затем цифра. Цифры для компонентов внутри каждого семейства назначены последовательно, начиная с единицы

Необязательный подраздел ***«Цели»*** компонента доверия содержит конкретные цели этого компонента. Для компонентов доверия, которые имеют этот подраздел, он включает в себя конкретное назначение данного компонента и подробное разъяснение целей.

Необязательный подраздел ***«Замечания по применению»*** компонента доверия содержит дополнительную информацию для облегчения использования компонента.

Зависимости среди компонентов доверия возникают, когда компонент не самодостаточен, а предполагает присутствие другого компонента. Для каждого компонента доверия приведен полный список зависимостей от других компонентов доверия. При отсутствии у компонента идентифицированных зависимостей вместо списка указано: "*Нет зависимостей*". Компоненты из списка, могут, в свою очередь, иметь зависимости от других компонентов.

Список зависимостей определяет минимальный набор компонентов доверия, на которые следует полагаться. Компоненты, которые являются иерархически более высокими по отношению к компоненту в списке зависимостей, также могут использоваться для удовлетворения зависимости.

В отдельных ситуациях обозначенные зависимости могут быть неприменимы. Разработчик ПЗ или ЗБ может отказаться от удовлетворения зависимости, представив обоснование, почему данная зависимость неприменима.

Каждый компонент доверия содержит набор элементов доверия. ***Элемент доверия*** – это требование безопасности, при дальнейшем разделении которого не изменяется значимый результат оценки. Он является наименьшим требованием безопасности, распознаваемым в ОК.

Каждый **элемент доверия** принадлежит к одному из **трех типов**.

- ***Элементы действий разработчика*** определяют действия, которые должны выполняться разработчиком. Этот набор действий далее уточняется доказательным материалом, упоминаемым в следующем наборе элементов. Требования к действиям разработчика обозначены буквой "*D*" после номера элемента.
- ***Элементы содержания и представления свидетельств*** определяют требуемое свидетельство; что свидетельство должно демонстрировать; какую информацию свидетельство должно отражать. Требования к содержанию и представлению свидетельств обозначены буквой "*C*" после номера элемента.
- ***Элементы действий оценщика*** определяют действия, которые должны выполняться оценщиком. Этот набор действий непосредственно включает подтверждение того, что требования, предписанные элементами содержания и представления свидетельств, выполнены, а также конкретные действия и анализ, выполняемые в дополнение к уже проведенным разработчиком. Должны также выполняться не указанные явно действия оценщика, необходимые вследствие элементов действий разработчика, но не охваченные в требованиях к содержанию и представлению свидетельств. Требования к действиям оценщика обозначены буквой "*E*" после номера элемента.

К элементам доверия не применяются операции назначения и выбора, однако, при необходимости, допускается уточнение элементов этой части стандарта.

Все семейства доверия в части 3 ОК являются линейно иерархическими, хотя линейность не обязательна для семейств доверия, которые могут быть добавлены в дальнейшем.

В таблице 3.4.6.1. приведена краткая характеристика всех 44 семейств доверия.

Таблица 3.4.6.1. Семейства доверия

№ п/п	Семейство	Наименование	Характеристика
Класс *ACM* – ***управление конфигурацией*** (УК)			
1	ACM_AUT	Автоматизация УК	Устанавливается уровень автоматизации, используемый для управления элементами конфигурации
2	ACM_CAP	Возможности УК	Определяются функциональные характеристики системы управления конфигурацией
3	ACM_SCP	Область УК	Указываются те элементы ОО, для которых необходим контроль со стороны системы управления конфигурацией.
Класс *ADO* – ***поставка и эксплуатация***			
4	ADO _DEL	Поставка	Задаются процедуры, используемые для поддержки безопасности во время передачи ОО пользователю при первоначальной поставке и при последующих модификациях.
5	ADO _IGS	Установка, генерация и запуск	Обеспечивается, чтобы копия ОО была конфигурирована и активизирована администратором так, чтобы показать те же самые свойства защиты, что и у оригинала ОО.
Класс *ADV* – ***разработка***			
6	ADV _FSP	Функциональная спецификация	Предъявляются требования к составу и содержанию ***функциональной спецификации***, описывающей функции безопасности ОО.
7	ADV _HLD	Проект верхнего уровня	Предъявляются требования к составу и содержанию ***проекта верхнего уровня*** – проектной спецификации самого высокого уровня, которая уточняет функциональную спецификацию ФБО в основных составляющих частях ФБО.
8	ADV _IMP	Представление реализации	Предъявляются требования к ***представлению реализации*** – наименее абстрактному представлению ФБО. Оно фиксирует детализированное внутреннее содержание ФБО на уровне исходного текста, аппаратных схем и т.д.
9	ADV _INT	Внутренняя структура	Задаётся порядок внутреннего

№ п/п	Семейство	Наименование	Характеристика
		ФБО	структурирования функций безопасности ОО.
10	ADV _LLD	Проект нижнего уровня	Задаются требования к составу и содержанию ***проекта нижнего уровня*** – детализированной проектной спецификации, уточняющей проект верхнего уровня до уровня детализации, который может быть использован как основа для программирования и/или проектирования аппаратуры.
11	ADV _RCR	Соответствие представлений	Требуется демонстрация отображения между всеми смежными парами имеющихся представлений ФБО, от краткой спецификации ОО до наименее абстрактного из имеющихся представлений ФБО.
12	ADV _SPM	Моделирование политики безопасности	Требуется необходимость использования ***моделей политики безопасности*** – структурных представлений политик безопасности ПБО, используемых для обеспечения повышенного доверия тому, что функциональная спецификация соответствует политикам безопасности из ПБО.
Класс *AGD* – ***руководства***			
13	AGD_ADM	Руководство администратора	Задаются требования к составу и содержанию руководства администратора.
14	AGD_USR	Руководство пользователя	Задаются требования к составу и содержанию руководства пользователя.
Класс *ALC* – ***поддержка жизненного цикла***			
15	ALC_DVS	Безопасность разработки	Определяются физические, процедурные, относящиеся к персоналу и другие меры безопасности, используемые применительно к среде разработки.
16	ALC_FLR	Устранение недостатков	– Требуется, чтобы недостатки, обнаруженные потребителями ОО, отслеживались и исправлялись в ходе сопровождения ОО

№ п/п	Семейство	Наименование	Характеристика
			разработчиком. – Оцениваются политики и процедуры, которые разработчик предусмотрел для выявления и устранения недостатков и распространения исправлений потребителям.
17	ALC_LCD	Определение жизненного цикла	Задаются требования к технологии разработки, используемой разработчиком для создания ОО.
18	ALC_TAT	Инструментальные средства и методы	Задаются требования к инструментальным средствам разработки, используемым для анализа и создания ОО.
Класс *ATE* – ***тестирование***			
19	ATE _COV	Покрытие	Предъявляются требования к анализу полноты функциональных тестов, выполненных разработчиком для ОО.
20	ATE _DPT	Глубина	Определяется уровень детализации, на котором разработчик проверяет ОО.
21	ATE _FUN	Функциональное тестирование	Задаются требования к содержанию функционального тестирования, выполняемого разработчиком.
22	ATE _IND	Независимое тестирование	Определяется объём и порядок независимого контроля результатов функционального тестирования.
Класс *AVA* – ***оценка уязвимостей***			
23	AVA_CCA	Анализ скрытых каналов	Определяется порядок выявления скрытых каналов передачи информации.
24	AVA_MSU	Неправильное применение	Определяется порядок анализа способности администратора или пользователя, используя руководства, определить, что ОО конфигурирован или эксплуатируется небезопасным способом.
25	AVA_SOF	Стойкость функций безопасности ОО	Определяется порядок анализа стойкости функций безопасности ОО, которые реализованы с

№ п/п	Семейство	Наименование	Характеристика
			помощью вероятностного или перестановочного механизма (например, пароля или хэш-функции).
26	AVA_VLA	Анализ уязвимостей	Определяется порядок анализа недостатков, которые могли быть внесены на различных этапах разработки.
Класс *AMA* – ***поддержка доверия***			
27	AMA_AMP	План поддержки доверия	Идентифицируются планы и процедуры, которые выполняются разработчиком для обеспечения поддержки доверия, установленного к оцененному ОО, после изменений в ОО или его среде.
28	AMA_CAT	Отчет о категорировании компонентов ОО	Определяется порядок категорирования компонентов ОО (например, подсистем ФБО) по их отношению к безопасности.
29	AMA_EVD	Свидетельство поддержки доверия	Определяется порядок поддержки разработчиком доверия к ОО в соответствии с планом поддержки доверия.
30	AMA_SIA	Анализ влияния на безопасность	Задаётся порядок проводимого разработчиком анализа влияния на безопасность всех изменений, воздействующих на ОО после его оценки.
Класс *APE* – ***оценка профиля защиты***			
31	APE_DES	Описание ОО	Определяется порядок контроля состава и содержания соответствующих разделов профиля защиты.
32	APE_ENV	Среда безопасности	
33	APE_INT	Введение ПЗ	
34	APE_OBJ	Цели безопасности	
35	APE_REQ	Требования безопасности ИТ	
36	APE_SRE	Требования безопасности ИТ, сформулированные в явном виде	
Класс *ASE* – ***оценка задания по безопасности***			
37	ASE_DES	Описание ОО	Определяется порядок контроля состава и содержания
38	ASE_ENV	Среда безопасности	

№ п/п	Семейство	Наименование	Характеристика
39	ASE_INT	Введение ЗБ	соответствующих разделов задания по безопасности.
40	ASE_OBJ	Цели безопасности	
41	ASE_PPC	Утверждения о соответствии ПЗ	
42	ASE_REQ	Требования безопасности ИТ	
43	ASE_SRE	Требования безопасности ИТ, сформулированные в явном виде	
44	ASE_TSS	Краткая спецификация ОО	

На практике при разработке профилей защиты и заданий по безопасности рекомендуется оформлять требования доверия к ОО в виде одного из определённых в части 3 ОК оценочных уровней доверия.

Оценочный уровень доверия (ОУД) представляет собой рассчитанную на многократное применение комбинацию требований доверия, содержащую не более одного компонента из каждого семейства доверия.

В стандарте определены 7 оценочных уровней доверия. С возрастанием порядкового номера предъявляемые требования усиливаются.

Оценочный уровень доверия 1 (ОУД1) предусматривает ***функциональное тестирование***. ОУД1 применим в тех случаях, когда требуется некоторая уверенность в правильном функционировании ОО, а угрозы безопасности не рассматриваются как серьезные. Он может быть полезен там, где требуется независимое подтверждение утверждения о том, что было уделено должное внимание защите персональных данных или подобной информации. Предполагается, что оценка ОУД1 может успешно проводиться без помощи разработчика ОО и с минимальными затратами. Анализ поддерживается независимым тестированием ФБО.

Оценочный уровень доверия 2 (ОУД2) предусматривает ***структурное тестирование***. ОУД2 содержит требование сотрудничества с разработчиком для получения информации о проекте и результатах тестирования без существенного увеличения стоимости или затрат времени. Анализ поддерживается независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций и свидетельством поиска разработчиком явных уязвимостей (например, из общедоступных источников).

Оценочный уровень доверия 3 (ОУД3) предусматривает ***методическое тестирование и проверку***. ОУД3 позволяет достичь максимального доверия путем применения надлежащего проектирования безопасности без значительного изменения существующей практики качественной разработки. Предполагается проведение всестороннего исследования ОО и процесса его разработки без существенных затрат на

изменение технологии проектирования. Анализ поддерживается независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации и проекте верхнего уровня, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций и свидетельством поиска разработчиком явных уязвимостей (например, из общедоступных источников).

Оценочный уровень доверия 4 (ОУД4) предусматривает ***методическое проектирование, тестирование и просмотр***. ОУД4 применим, когда разработчикам или пользователям требуется независимо получаемый уровень доверия от умеренного до высокого в ОО общего назначения и имеется готовность нести дополнительные, связанные с безопасностью производственные затраты. Это самый высокий уровень, на который обычно экономически целесообразно ориентироваться для существующих типов продуктов. Анализ поддерживается независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации и проекте верхнего уровня, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, демонстрирующим противодействие попыткам проникновения нарушителей с низким потенциалом нападения.

Оценочный уровень доверия 5 (ОУД5) предусматривает ***полуформальное проектирование и тестирование***. ОУД5 применим, когда разработчикам или пользователям требуется независимо получаемый высокий уровень доверия для запланированной разработки со строгим подходом к разработке, не влекущим излишних затрат на применение узко специализированных методов проектирования безопасности. Тем самым, предполагается, что ОО будут проектироваться и разрабатываться с намерением достичь ОУД5. Анализ поддерживается независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации, проекте верхнего уровня и проекте нижнего уровня, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, демонстрирующим противодействие попыткам проникновения нарушителей с умеренным потенциалом нападения. Анализ также включает проверку правильности анализа разработчиком скрытых каналов.

Оценочный уровень доверия 6 (ОУД6) предусматривает ***полуформальную верификацию проекта и тестирование***. ОУД6 позволяет разработчикам достичь высокого доверия путем применения специальных методов проектирования безопасности в строго контролируемой среде разработки с целью получения высококачественного ОО для защиты высоко оцениваемых активов от значительных рисков. Анализ поддерживается независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации, проекте верхнего уровня и проекте нижнего уровня, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, демонстрирующим противодействие попыткам проникновения нарушителей с высоким потенциалом

нападения. Анализ также включает проверку правильности систематического анализа разработчиком скрытых каналов.

Оценочный уровень доверия 7 (ОУД7) предусматривает ***формальную верификацию проекта и тестирование***. ОУД7 применим при разработке безопасных ОО для использования в ситуациях чрезвычайно высокого риска и/или там, где высокая ценность активов оправдывает более высокие затраты. Практическое применение ОУД7 в настоящее время ограничено ОО, которые строго ориентированы на реализацию функциональных возможностей безопасности и для которых возможен подробный формальный анализ. Анализ поддерживается независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации, проекте верхнего уровня, проекте нижнего уровня и представлении реализации, полным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, демонстрирующим противодействие попыткам проникновения нарушителей с высоким потенциалом нападения. Анализ также включает проверку правильности систематического анализа разработчиком скрытых каналов.

Сводное описание оценочных уровней доверия приведено в таблице 3.4.6.2. Все уровни являются иерархически упорядоченными, и каждый ОУД представляет более высокое доверие, чем любой из предыдущих. Увеличение доверия от ОУД к ОУД достигается заменой какого-либо компонента доверия иерархически более высоким компонентом из того же семейства доверия (т.е. увеличением строгости, области и/или глубины оценки) и добавлением компонентов доверия из других семейств доверия (т.е. добавлением новых требований).

Таблица 3.4.6.2. Сводное описание оценочных уровней доверия

Класс доверия	**Семейство доверия**	**Компоненты доверия из оценочного уровня доверия**						
		ОУД 1	**ОУД 2**	**ОУД 3**	**ОУД 4**	**ОУД 5**	**ОУД 6**	**ОУД 7**
Управление конфигурацией	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Поставка и эксплуатация	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Разработка	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Руководства	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД 1	ОУД 2	ОУД 3	ОУД 4	ОУД 5	ОУД 6	ОУД 7
Поддержка жизненного цикла	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Тестирование	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Помимо заявленных в части 3 ОК ОУД, можно представлять другие комбинации компонентов доверия. Операция ***усиления*** оценочных уровней доверия допускает добавление компонентов доверия (из семейств доверия, до этого не включенных в ОУД) или замену компонентов доверия в ОУД другими, иерархически более высокими компонентами доверия из того же самого семейства доверия. Исключение из ОУД какого-либо составляющего его компонента доверия является недопустимым. В случае, если производится усиление ОУД, необходимо строго обосновать полезность и дополнительную ценность добавленного к ОУД компонента доверия. ОУД может быть также расширен за счёт применения требований доверия, сформулированных в явном виде.

3.4.7. Общие критерии. Сопутствующие документы

Рассмотренные три части общих критериев представляют собой законченный и самодостаточный стандарт. Дополнительные документы, используемые в рамках «Общих критериев», являются вспомогательными и призваны в первую очередь обеспечить лёгкую интерпретацию положений «Общих критериев» для тех или иных практических вариантов их применения.

Наибольший интерес среди сопутствующих «Общим критериям» материалов представляет документ ***«Руководящий документ. Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий»*** [36], более известный как ***«Общая методология оценки»*** (ОМО). Документ охватывает все виды деятельности по оценке, соответствующие классам доверия из части 3 ОК, входящим в оценочные уровни доверия 1-4, кроме связанных с оценкой профилей защиты и заданий по безопасности.

«Общая методология» описывает минимум действий, выполняемых оценщиком при проведении оценки по ОК, с использованием критериев и свидетельств оценки, определенных в ОК. Документ предназначен, прежде всего, для оценщиков,

использующих ОК, и экспертов органов по сертификации, подтверждающих действия оценщиков.

Основные принципы ОМО:

Принципами ОМО являются:

- ***Объективность*** - результаты оценки основываются на фактических свидетельствах и не зависят от личного мнения оценщика.
- ***Беспристрастность*** - результаты оценки являются непредубежденными, когда требуется субъективное суждение.
- ***Воспроизводимость*** - действия оценщика, выполняемые с использованием одной и той же совокупности поставок для оценки, всегда приводят к одним и тем же результатам.
- ***Корректность*** - действия оценщика обеспечивают точную техническую оценку.
- ***Достаточность*** - каждый вид деятельности по оценке осуществляется до уровня, необходимого для удовлетворения всех заданных требований доверия.
- ***Приемлемость*** - каждое действие оценщика способствует повышению доверия, по меньшей мере, пропорционально затраченным усилиям.

Взаимосвязь между ОМО и частью 3 ОК показана на рис. 3.4.7.1.

Рис. 3.4.7.1. Взаимосвязь между ОК и ОМО

Тем самым, ОМО в основном представляет собой детализированную последовательность действий оценщика при проведении проверок по каждому из компонентов доверия части 3 ОК для ОУД 1-4. Для более высоких ОУД методология считается в настоящее время неопределённой.

Процесс оценки состоит из выполнения оценщиком задачи получения исходных данных для оценки, задачи оформления результатов оценки и подвидов деятельности по оценке (рис. 3.4.7.2).

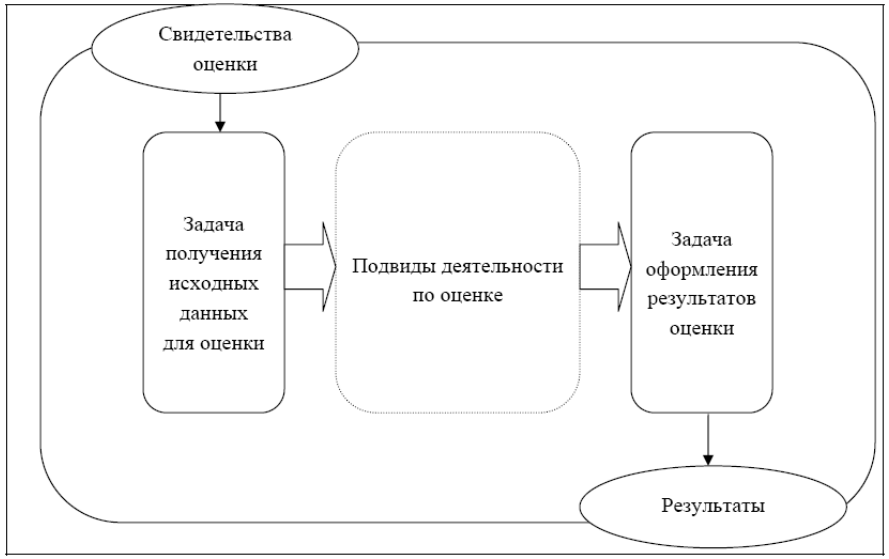

Рис. 3.4.7.2. Процесс оценки

По каждому элементу действий оценщик выносит ***вердикт*** – ***положительный*** или ***отрицательный***. ***Общий вердикт*** является положительным тогда и только тогда, когда все составляющие вердикта положительные.

Результаты оценки оформляются в виде ***технического отчёта об оценке*** (ТОО), имеющего следующую **структуру**:

1. ***Введение***
   - идентификаторы системы сертификации;
   - идентификаторы контроля конфигурации ТОО (название, дата, номер версии и т.д.);
   - идентификаторы контроля конфигурации ЗБ и ОО;
   - ссылка на ПЗ;
   - идентификатор разработчика;
   - идентификатор заявителя;
   - идентификатор оценщика.
2. ***Описание архитектуры ОО***
   - высокоуровневое описание ОО и его главных компонентов, основанное на проекте верхнего уровня.
3. ***Оценка***
   - методы, технологии, инструментальные средства и стандарты, применяемые при оценке;
   - сведения об ограничениях, принятых при проведении оценки;
   - правовые аспекты оценки, заявления о конфиденциальности и т.д.

4. ***Результаты оценки***

   Для каждого вида деятельности приводятся:
   - название рассматриваемого вида деятельности;
   - вердикт, сопровождаемый обоснованием, для каждого компонента доверия, определяющего этот вид деятельности, как результат выполнения соответствующего действия ОМО и составляющих его шагов оценивания.
5. ***Выводы и рекомендации***
   - общий вердикт;
   - рекомендации, которые могут быть полезны для органа по сертификации.
6. ***Перечень свидетельств оценки***

   Для каждого использованного при проведении оценки свидетельства указываются:
   - составитель;
   - название;
   - уникальная ссылка.
7. ***Перечень сокращений и глоссарий терминов***
8. ***Сообщения о проблемах***
   - полный перечень сообщений о проблемах;
   - их текущее состояние.

Сообщения о проблемах (СП) представляют собой механизм для запроса разъяснений или для определения проблемы по тому или иному аспекту оценки. При отрицательном вердикте оценщик обязан представить СП для отражения результата оценки. При этом СП должны иметь следующую **структуру**:

- идентификатор оцениваемого ОО;
- задача/подвид деятельности по оценке, при выполнении которой/которого проблема была выявлена;
- суть проблемы;
- оценка ее серьезности (например, приводит к отрицательному вердикту, задерживает выполнение оценки или требует решения до завершения оценки);
- организация, ответственная за решение вопроса;
- рекомендуемые сроки решения;
- влияние на оценку отрицательного результата решения проблемы.

Адресаты рассылки СП и процедуры обработки сообщения определяются правилами, действующими в системе сертификации.

Документ ***«Безопасность информационных технологий. Типовая методика оценки профилей защиты и заданий по безопасности»*** [37] предназначен для заявителей, испытательных центров (лабораторий) и органов по сертификации проводящих проверку соответствии ПЗ/ЗБ, представляемых на испытания, требованиям «Общих критериев». В целом документ представляет собой дополнение «Общей методологии оценки», регламентирующее порядок проведения оценки профилей защиты и заданий по безопасности в соответствии с положениями классов доверия *APE* и *ASE* части 3 ОК.

Документ ***«Руководящий документ Руководство по разработке профилей защиты и заданий по безопасности»*** [38] содержит практические рекомендации для разработчиков ПЗ и ЗБ. Приводятся примеры типовых угроз, положений политики безопасности организации, предположений, целей, и требований безопасности. В документе также содержатся подробные методические рекомендации по формированию профилей защиты для межсетевого экрана, СУБД и доверенного центра инфраструктуры открытых ключей.

Помимо трёх рассмотренных, используются следующие **документы**:

– ***«Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности»*** [39]**.**

  Документ определяет общий порядок разработки, оценки, регистрации и публикации ПЗ и ЗБ.

– ***«Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты»*** [40]**.**

  Документ определяет порядок ведения реестра профилей защиты.

– ***«Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты»*** [41]**.**

  Документ определяет порядок формирования ***семейств ПЗ***, т.е. совокупностей упорядоченных взаимосвязанных профилей защиты, относящихся к определённому типу продуктов или систем.

Отметим, что в настоящее время в России отсутствует единый универсальный реестр профилей защиты. Как правило, при проведении сертификационных испытаний по «Общим критериям» используются задания по безопасности, для которых соответствие каким-либо профилям защиты не декларируется.

3.5. Стандарты в области управления информационной безопасностью

3.5.1. Общие положения

При рассмотрении ограничений «Общих критериев» мы обращали внимание на то, что они не затрагивают вопросов, касающихся администрирования механизмов безопасности, непосредственно не относящихся к мерам безопасности информационных технологий. Действительно, при построении системы управления информационной безопасностью на предприятии возникает целый ряд вопросов, заслуживающих отдельного рассмотрения.

Наиболее распространёнными управленческими стандартами на сегодняшний день являются документы, разработанные Британским институтом стандартов (BSI – British Standards Institution). Стандарты BS 7799-1, BS 7799-2 и BS 7799-3 крайне популярны во всём мире, первые два из них имеют международный статус стандартов ISO (последние версии данных стандартов имеют обозначения ISO/IEC 17799:2005 и ISO/IEC 27001:2005 соответственно).

По сравнению с общими критериями, данные документы носят гораздо более неформальный характер и представляют собой скорее набор практических рекомендаций по развёртыванию и поддержанию системы управления информационной безопасностью.

3.5.2. ISO/IEC 17799:2005

Стандарт ***ISO/IEC 17799:2005 "Information technology – Security techniques – Code of practice for information security management"*** [41] (Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью) представляет собой набор практических рекомендаций по построению комплексной корпоративной системы управления информационной безопасностью.

Согласно положениям стандарта, информационная безопасность рассматривается как процесс защиты информационных активов организации от различного рода угроз, который достигается путём реализации тех или иных ***сервисов безопасности***[1]**.** ***Требования к системе безопасности*** определяются по результатам предварительно проведённого анализа рисков, исходя из требований нормативных и законодательных актов, а также путём анализа специфических потребностей бизнеса. Сервисы выбираются таким образом, чтобы минимизировать идентифицированные информационные риски.

Именно каталог рекомендуемых сервисов безопасности и составляет основное содержание стандарта. Сервисы сгруппированы по следующим **тематическим разделам**:

1. Политика безопасности.
2. Организация информационной безопасности.
3. Управление активами.
4. Безопасность человеческих ресурсов.
5. Физическая безопасность и безопасность окружающей среды.
6. Управление телекоммуникациями и операциями.
7. Управление доступом.
8. Приобретение, разработка и внедрение информационных систем.
9. Управление инцидентами в сфере информационной безопасности.
10. Управление непрерывностью бизнеса.
11. Соответствие.

Для каждого сервиса приведены его ***определение***, ***руководство по реализации*** и ***дополнительная информация***.

Политика информационной безопасности рассматривается как базовый высокоуровневый документ, утверждённый высшим руководством организации и определяющий общий подход к организации и управлению информационной безопасности. Политика также содержит ссылки на низкоуровневые стандарты, руководства и процедуры, определяющие практические аспекты реализации механизмов безопасности. Пересмотр политики осуществляется через запланированные промежутки времени или в случае принципиальных изменений в информационной системе.

Требования по ***организации информационной безопасности*** включают в себя вопросы разделения обязанностей и распределения ответственности между всеми участниками информационного взаимодействия, существующего в организации.

[1] Устоявшийся перевод англоязычного термина "***control***" на русский язык в настоящее время отсутствует. Наиболее распространённые варианты перевода - «***сервис***», «***контрмера***», «***механизм контроля***». В дальнейшем изложении мы будем придерживаться первого варианта.

Отдельно рассматриваются вопросы взаимодействия с органами власти, контрагентами и другими сторонними организациями, а также возникающие в ходе такого взаимодействия вопросы конфиденциальности.

Управление активами предполагает проведение инвентаризации активов и обеспечение корректного их использования. В качестве одного из базовых механизмов обеспечения информационной безопасности предлагается проведение категорирования информации с точки зрения её ценности, секретности, критичности для организации, или же по требованиям законодательных и нормативных актов.

Вопросы ***безопасности человеческих ресурсов*** призваны обеспечить соблюдении установленного режима информационной безопасности сотрудниками и контрагентами. Во всех случаях права и обязанности сторон в сфере информационной безопасности должны быть строго оговорены в трудовом договоре. Регламентируются порядок найма и корректного увольнения сотрудников, а также вопросы обучения и образовательных тренингов в области информационной безопасности

Физическая безопасность и безопасность окружающей среды достигаются путём применения комплекса механизмов управления физическим доступом к активам организации, использования противопожарных систем, систем кондиционирования, а также путём своевременного и полноценного технического обслуживания сооружений и инфраструктуры. Рассматриваются вопросы корректной утилизации активов и повторного использования оборудования.

Управление телекоммуникациями и операциями реализуется путём чёткой формализации всех процедур, связанных с обработкой информации в АС. Все изменения в процедурах и самих средствах обработки информации должны строго документироваться. Определяются механизмы борьбы с вредоносным программным обеспечением и методы обеспечения безопасности мобильного кода. Предлагаются подходы к обеспечению безопасности специфических сетевых сервисов, таких, например, как механизмы электронной платежей. Отдельно рассматриваются вопросы безопасности носителей информации.

При рассмотрении вопросов ***управления доступом*** особое внимание уделяется рекомендациям по корректной реализации механизмов парольной защиты. Определяется порядок организации удалённого доступа пользователей к информационной системе, приводятся рекомендации по работе с мобильными вычислительными устройствами.

В ходе ***приобретения, разработки и внедрения информационных систем*** предполагается устанавливать акцент на обеспечении целостности информационных активов и программных компонентов системы, достигаемой, в частности, с использованием криптографических механизмов. Предлагаются также механизмы защиты от утечки информации на различных этапах жизненного цикла информационной системы.

Управление инцидентами в сфере информационной безопасности может осуществляться силами специалистов организации или с привлечением уполномоченных органов безопасности. Данная деятельность в общем случае включает в себя сбор улик, проведение расследования и анализ результатов расследования в целях недопущения повторных инцидентов и повышения общей защищённости информационной системы.

Обеспечение непрерывности бизнеса является одной из основных задач системы управления информационной безопасностью и должно реализовать защиту критических

бизнес-процессов от сбоев или стихийных бедствий. Разрабатываемые планы непрерывности бизнеса должны гарантировать доступность критических информационных ресурсов и сервисов на требуемом уровне. Планы непрерывности бизнеса должны тщательно тестироваться и своевременно обновляться при изменении структуры информационной системы или бизнес-модели организации.

Соответствие требованиям законодательных актов, отраслевых стандартов и других нормативных документов является обязательным для всех информационных систем. Требования безопасности также могут быть определены в договорных обязательствах. Рассматриваются также вопросы обеспечения защиты от злоупотреблений пользователей различными сервисами и информационными ресурсами.

В России аутентичный перевод стандарта в настоящее время планируется к принятию в качестве ГОСТ.

3.5.3. ISO/IEC 27001:2005

Стандарт ***ISO/IEC 27001:2005 "Information technology – Security techniques – Information security management systems - Requirements"*** [43] (Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.) представляет собой расширение ISO/IEC 17799:2005, устанавливающее требования по созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и совершенствованию корпоративных ***систем управления информационной безопасностью*** (СУИБ).

Реализация СУИБ осуществляется путём внедрения четырёхфазной модели ***PDCA*** (Plan-Do-Check-Act, Планирование – Реализация – Оценка - Корректировка). Структура модели показана на рис. 3.5.3.

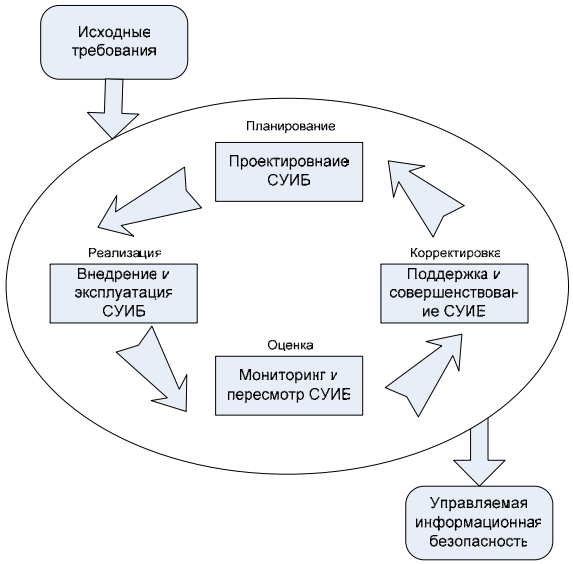

Рис. 3.5.3. Модель PDCA

Система управления информационной безопасностью получает в качестве исходных данных требования информационной безопасности и ожидания заинтересованных сторон и путём применения необходимых мер и процессов реализует необходимые механизмы безопасности.

Предварительным условием начала работ по ***планированию*** СУИБ является принятие ***политики безопасности***, устанавливающей общие принципы обеспечения информационной безопасности в организации и задающей область действия СУИБ. Планирование осуществляется путём проведения оценки рисков и выбора сервисов безопасности, соответствующих требованиям, идентифицированным по результатам анализа рисков. Каталог сервисов безопасности, полностью соответствующих приведённым в ISO/IEC 17799:2005, содержится в ***приложении А*** к стандарту ISO/IEC 27001:2005.

На этапе ***реализации*** необходимо, решив вопросы финансирования и распределения обязанностей, реализовать выбранные на этапе планирования сервисы безопасности и обеспечить корректную их эксплуатацию. Необходимо предусмотреть наличие механизмов оценки эффективности сервисов безопасности и реализовать программы обучения пользователей вопросам информационной безопасности. При осуществлении эксплуатации СУИБ необходимо тщательно контролировать и корректно отрабатывать инциденты, связанные с информационной безопасностью.

Проведение ***оценки*** СУИБ предполагает проведение анализа эффективности функционирования как отдельных сервисов безопасности, так и СУИБ в целом. Отслеживание изменений, происходящих в системе, должно сопровождаться пересмотром результатов анализа рисков. Внутренний аудит СУИБ должен проводиться через запланированные интервалы времени.

Фаза ***корректировки*** должна обеспечить непрерывное совершенствование системы управления информационной безопасностью с учётом изменяющихся рисков и требований. В ряде случаев проведение корректировки может потребовать возврата к предыдущим фазам модели – например, к этапам планирования и реализации.

Реализация СУИБ сопровождается разработкой **системы документации**, которая должна включать следующие материалы:

- положения политики безопасности организации;
- область действия СУИБ;
- процедуры и сервисы безопасности, поддерживающие СУИБ;
- описание применяемых методов оценки рисков;
- отчёты, содержащие результаты оценки рисков;
- план управления рисками;
- методики оценки эффективности применяемых сервисов безопасности;
- декларация применимости;
- записи, подтверждающие эффективность функционирования СУИБ и предоставляющие свидетельства её соответствия положениям стандарта.

Аналогично ISO/IEC 17799:2005, стандарт ISO/IEC 27001:2005 в ближайшее время должен быть принят в Российской Федерации в качестве ГОСТ.

3.5.4. BS 7799-3:2006

Британский стандарт ***BS 7799-3:2006 "Information security management systems – Part 3: Guidelines for information security risk management"*** [44] (Системы управления информационной безопасностью – Часть 3: руководство по управлению рисками в информационной безопасности) пока не имеет международного статуса, однако рассматривается возможность его принятия в качестве стандарта ISO. Поскольку на момент написания этих строк русскоязычный перевод стандарта отсутствует, и документ не получил должного освещения в отечественной литературе, остановимся на нём несколько подробнее.

Стандарт представляет собой набор руководств и рекомендаций, направленных на удовлетворение требований стандарта ISO/IEC 27001:2005 в части управления рисками, которое рассматривается как непрерывный четырёхфазный процесс (рис. 3.5.4).

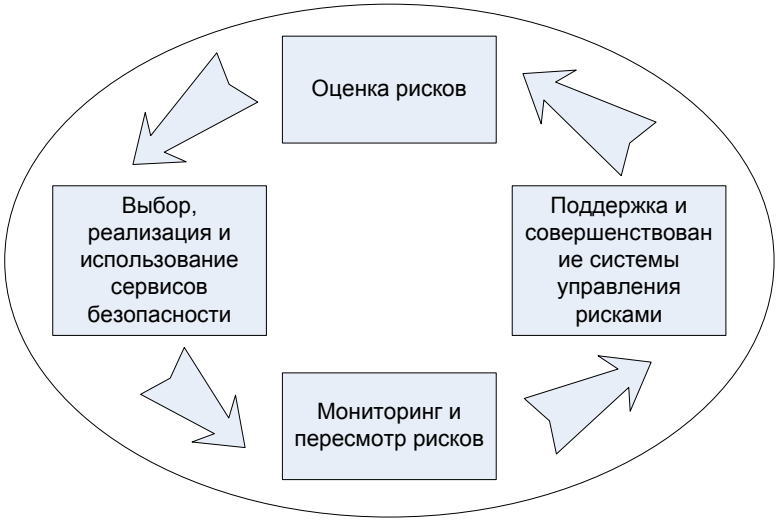

Рис. 3.5.4. Модель управления рисками

Отметим, что стандарт не содержит требований по использованию какой-либо конкретной **методики оценки рисков**. Предъявляются лишь **требования** к этой методике – так, она должна обеспечивать:

- возможность определения критериев для принятия риска;
- возможность идентификации приемлемых уровней риска;
- возможность проведения идентификации и оценки рисков;
- покрытие всех аспектов системы управления информационной безопасностью.

Процесс ***оценки рисков*** в общем случае включает в себя анализ и вычисление рисков. Проведение ***анализа рисков*** предполагает **следующие действия**:

- идентификация активов;
- идентификация бизнес-требований и требований законодательства, имеющих отношение к активам организации.

- Оценка активов, учитывающая идентифицированные ранее требования к ним и возможный ущерб, возникающий в случае реализации в отношении этих активов угроз нарушения конфиденциальности, целостности или доступности.
- Идентификация угроз и уязвимостей, связанных с активами организации.
- Оценка вероятности реализации угроз и уязвимостей.

Вычисление рисков, в свою очередь, **включает**:

- непосредственно вычисление рисков, выполненное по некоторой методике;
- соотнесение вычисленных значений рисов с установленной шкалой приемлемых уровней риска.

По результатам анализа рисков необходимо выбрать одну из четырёх возможных стратегий **управления рисками**[2]:

1. ***Уменьшение риска***. Риск считается неприемлемым, и для его уменьшения выбираются и реализуются те или иные сервисы безопасности.
2. ***Осознанное и обоснованное принятие риска***. Риск в данном случае считается допустимым. Обычно это означает, что стоимость внедрения сервисов безопасности значительно превосходит финансовые потери в случае реализации угрозы.
3. ***Передача риска***. Риск считается неприемлемым и на определённых условиях – например, в рамках страхования – передаётся сторонней организации.
4. ***Избежание риска.*** Риск считается неприемлемым, и в качестве корректирующих мер осуществляются изменения в бизнес-модели организации – например, отказ от осуществления того или иного вида деятельности.

Вне зависимости от того, какие стратегии управления рисками будут выбраны, после их реализации всегда будут существовать ***остаточные риски***, которые также подлежат оценке. Тот факт, что остаточные риски являются неприемлемыми, служит основанием поиска более эффективных механизмов управления рисками.

Деятельность, связанная с реализацией результатов управления рисками, должна сопровождаться разработкой ***плана управления рисками***, содержащего:

1. ограничения и зависимости между сервисами безопасности;
2. приоритеты;
3. сроки и ключевые промежуточные этапы реализации;
4. требуемые ресурсы;
5. ссылки на разрешения использования требуемых ресурсов;
6. критические маршруты выполнения плана.

Непрерывный процесс управления рисками в организации должен контролироваться уполномоченным **специалистом** или **командой специалистов**, которые должны удовлетворять следующим **требованиям**:

- способность реализовать систематический и организованный подход к выявлению известных рисков и предпринимать адекватные действия;
- ориентация на бизнес-процессы организации и учёт актуальных в данный момент приоритетов бизнеса;

[2] Наиболее корректным переводом двух англоязычных терминов – "***risk management***" и "***risk treatment***" является «***управление рисками***». О каком из двух понятий идёт речь, обычно очевидно по контексту.

- настойчивость и независимость суждений, способность учитывать альтернативные точки зрения;
- способность решать вопросы на всех уровнях корпоративной иерархии организации;
- хорошее понимание рисков, технологий и сервисов информационной безопасности.

Большинство сервисов безопасности для обеспечения их корректного и эффективного функционирования требуют непрерывной ***поддержки*** и ***мониторинга***. Соответствующая деятельность может, например, **включать**:

- анализ файлов системных журналов;
- модификацию параметров, связанную с произошедшими в системе изменениями;
- повторный анализ корректности использования сервисов безопасности;
- обновление сервисов, политик и процедур.

Результаты первоначальной оценки рисков должны регулярно пересматриваться. ***Возникновение изменений*** в значениях рисков может быть связано со следующими **факторами**:

- изменения в бизнес-модели организации;
- появление новых данных относительно корректности и эффективности используемых сервисов безопасности;
- изменения, связанные с политической обстановкой, социальными факторами или окружающей средой;
- возникновение новых, ранее неизвестных угроз и уязвимостей.

Результаты повторного анализа рисков, проводимого с учётом возникших изменений, должны накапливаться в специальной базе данных, позволяющей отследить динамику происходящих изменений.

В приложении к стандарту содержатся примеры активов, угроз, уязвимостей, а также приводится типовая методика оценки рисков.

3.6. Выводы

Мы рассмотрели основные оценочные и управленческие стандарты, используемые при проектировании, реализации, оценке, поддержке, управлении и эксплуатации автоматизированных систем. Современные стандарты являются бесценным источником оптимальных и заведомо эффективных решений, а потому их использование во многих случаях может чрезвычайно упростить практическую деятельность специалиста в области информационной безопасности. Тот факт, что в России стандартизация в данной области идёт по пути поэтапного принятия международных стандартов, не может не сказываться самым позитивным образом на развитии отрасли в целом.

Библиография

1. **П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю**. **Щербаков** Теоретические основы компьютерной безопасности. – М.: «Радио и связь». – 2000.
2. **Ronald R. Krutz, Russell Dean Vines**. The CISSP Prep Guide—Mastering the Ten Domains of Computer Security. – John Wiley and Sons, Inc., 2001.
3. **А.А. Грушо, Е.Е. Тимонина.** Теоретические основы защиты информации. – М.: «Яхтсмен», 1996.
4. **М. Ховард, Д**. **Лебланк.** Защищённый код. – М.: «Русская редакция». – 2004.
5. **И.В.Котенко, М.М.Котухов, А.С.Марков.** Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей. - СПб.: ВУС, 2000.
6. **Ed Tittel, JamesM. Stewart, Mike Chapple**. CISSP: Certified Informations Systems Security Professional. Study guide. 2-nd Edition. – Sybex, 2003.
7. **Кевин Митник**. Искусство обмана. – М.: Компания АйТи, 2004.
8. **Брюс Шнайер**. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003.
9. **Вильям Столингс**. Криптография и защита сетей. – М.: Вильямс, 2001 г.
10. **Niels Ferguson, Bruce Schneier**. Practical Cryptography. - John Wiley and Sons, Inc., 2003.
11. **С.В. Лебедь**. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – М.: Издательство МГТУ имени Н.Э. Баумана, 2002 г.
12. **С.С. Корт**. Теоретические основы защиты информации. – М.: Гелиос АРВ, 2004.
13. **D. Clark, D. Wilson.** A compassion of Commercial and Military Computer Security Policies. – Thr 1987 IEEE Symposium on Security and Privacy, 1987.
14. **Bruce Schneier**. Applied cryptography. Protocols, Algorithms, and Source Code in C. – John Wiley & Sons, 1996.
15. **A.J. Menezes, P.C. van Oorschot, S.A. Vanstone.** Handbook of Applied Cryptography. – CRC Press, 1996.
16. **M. Harrison, W. Ruzzo, J. Ullman**. Protection in operating systems. – Communication of ACM, 1976.
17. **Ben Mankin**. The formalization of Protection Systems. – University of Bath, 2004.
18. **П.Н. Девянин**. Модели безопасности компьютерных систем. – М.: Академия, 2005.
19. **Д.П. Зегжда, А.М. Ивашко**. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000.
20. **D.E. Bell, L.J. LaPadula.** Secure Computer Systems: Unified Exposition and Multics Interpretation.
21. **KJ Biba**. Integrity Considerations for Secure Computer Systems, The Mitre Corporation, Technical Report, No.MTR-3153, 1977.
22. **Грушо А.А.** О существовании скрытых каналов. – Дискретная математика, т. 11, вып. 1, 1999.

23. **Kemmerer R.A.** Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels. – ACM Transactions on Computer Systems, 1:3, pp. 256-277, August 1983.
24. **А.С. Марков, С.В. Миронов, В.Л. Цирлов**. Выявление уязвимостей а программном коде. – Открытые системы, №12, 2005.
25. **В.А. Галатенко**. Стандарты информационной безопасности. Курс лекций. – М.: Интернет-Университет Информационных технологий, 2004.
26. **Trusted Computer System Evaluation Criteria**. – US Department of Defense, 1983.
27. **Руководящий документ**. Защита от несанкционированного доступа к информации. Термины и определения. - Гостехкомиссия России, 1992.
28. **Руководящий документ**. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. – Гостехкомиссия России, 1992.
29. **Руководящий документ**. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - Гостехкомиссия России, 1992.
30. **Руководящий документ**. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. - Гостехкомиссия России, 1992.
31. **Руководящий документ**. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. - Гостехкомиссия России, 1997.
32. **Руководящий документ**. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. - Гостехкомиссия России, 1999.
33. **ГОСТ Р ИСО/МЭК 15408-1-2002.** Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – М.: Госстандарт России, 2002.
34. **ГОСТ Р ИСО/МЭК 15408-2-2002.** Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – М.: Госстандарт России, 2002.
35. **ГОСТ Р ИСО/МЭК 15408-3-2002.** Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – М.: Госстандарт России, 2002.
36. **Руководящий документ**. Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий. – ФСТЭК России, 2005.
37. **Безопасность информационных технологий**. Типовая методика оценки профилей защиты и заданий по безопасности. – ФСТЭК России, 2005.

38. **Руководящий документ** Руководство по разработке профилей защиты и заданий по безопасности. – Гостехкомиссия России, 2003.
39. **Руководящий документ**. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности – Гостехкомиссия России, 2003.
40. **Руководящий документ.** Безопасность информационных технологий. Руководство по регистрации профилей защиты – Гостехкомиссия России, 2003.
41. **Руководящий документ.** Безопасность информационных технологий. Руководство по формированию семейств профилей защиты – Гостехкомиссия России, 2003.
42. **ISO/IEC 17799:2005** Information technology – Security techniques – Code of practice for information security management, 2005.
43. **ISO/IEC 27001:2005** Information technology – Security techniques – Information security management systems - Requirements, 2005.
44. **BS 7799-3:2006** Information security management systems – Part 3: Guidelines for information security risk management, 2006.

Приложение 1. Глоссарий «Общих критериев»

Ниже приведены термины и определения основных понятий и терминов, необходимых при работе с «Общими критериями». Глоссарий полностью соответствует ГОСТ Р ИСО/МЭК 15408-1:2002. Приведены также их англоязычные эквиваленты.

Активы: Информация или ресурсы, подлежащие защите контрмерами ОО.	**assets**
Атрибут безопасности: Информация, связанная с субъектами, пользователями и/или объектами, которая используется для осуществления ПБО.	**security attribute**
Аутентификационные данные: Информация, используемая для верификации предъявленного идентификатора пользователя.	**authentication data**
Базовая СФБ: Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения.	**SOF-basic**
Внешний объект ИТ: Любые продукт или система ИТ, доверенные или нет, находящиеся вне ОО и взаимодействующие с ним.	**external IT entity**
Внутренний канал связи: Канал связи между разделенными частями ОО.	**internal communication channel**
Выбор: Выделение одного или нескольких элементов из перечня в компоненте.	**selection**
Высокая СФБ: Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.	**SOF-high**
Данные ФБО: Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО.	**TSF data**
Данные пользователя: Данные, созданные пользователем и для пользователя, которые не влияют на выполнение ФБО.	**user data**
Доверенный канал: Средство взаимодействия между ФБО и удаленным доверенным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании ПБО.	**trusted channel**
Доверенный маршрут: Средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую степень уверенности в поддержании ПБО.	**trusted path**
Доверие: Основание для уверенности в том, что сущность отвечает своим целям безопасности.	**assurance**
Зависимость: Соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть, как правило, удовлетворено, чтобы и другие требования могли бы отвечать своим целям.	**dependency**

Задание по безопасности: Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО.	**security target**
Идентификатор: Представление уполномоченного пользователя (например, строка символов), однозначно его идентифицирующее. Таким представлением может быть либо полное или сокращенное имя этого пользователя, либо его псевдоним.	**identity**
Интерфейс функций безопасности ОО: Совокупность интерфейсов, как интерактивных (человеко-машинные интерфейсы), так и программных (интерфейсы прикладных программ), с использованием которых осуществляется доступ к ресурсам ОО при посредничестве ФБО или получение от ФБО какой-либо информации.	**TOE security functions interface**
Итерация: Более чем однократное использование компонента при различном выполнении операций.	**iteration**
Класс: Группа семейств, объединенных общим назначением.	**class**
Компонент: Наименьшая выбираемая совокупность элементов, которая может быть включена в ПЗ, ЗБ или пакет**.**	**component**
Механизм проверки правомочности обращений: Реализация концепции монитора обращений, обладающая следующими свойствами: защищенностью от проникновения; постоянной готовностью; простотой, достаточной для проведения исчерпывающего анализа и тестирования.	**reference validation mechanism**
Модель политики безопасности ОО: Структурированное представление политики безопасности, которая должна быть осуществлена ОО.	**TOE security policy model**
Монитор обращений: Концепция абстрактной машины, осуществляющей политики управления доступом ОО.	**reference monitor**
Назначение: Спецификация определенного параметра в компоненте**.**	**assignment**
Неформальный: Выраженный на естественном языке.	**informal**
Область действия ФБО: Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО.	**TSF scope of control**
Объект: Сущность в пределах ОДФ, которая содержит или получает информацию, и над которой субъекты выполняют операции.	**object**
Объект оценки: Подлежащие оценке продукт ИТ или система с руководствами администратора и пользователя.	**target of evaluation**
Орган оценки: Организация, которая посредством системы оценки обеспечивает реализацию ОК для определенного сообщества и в связи с этим устанавливает стандарты и контролирует качество оценок, проводимых организациями в пределах данного сообщества.	**evaluation authority**
Оценка: Оценка ПЗ, ЗБ или ОО по определенным критериям.	**evaluation**

Оценочный уровень доверия: Пакет компонентов доверия из части 3 настоящего стандарта, представляющий некоторое положение на предопределенной в стандарте шкале доверия.	**evaluation assurance level**
Пакет: Предназначенная для многократного использования совокупность функциональных компонентов или компонентов доверия (например, ОУД), объединенных для удовлетворения совокупности определенных целей безопасности.	**package**
Передача в пределах ОО: Передача данных между разделенными частями ОО.	**internal TOE transfer**
Передача за пределы области действия ФБО: Передача данных сущностям, не контролируемым ФБО.	**transfers outside TSF control**
Передача между ФБО: Передача данных между ФБО и функциями безопасности других доверенных продуктов ИТ.	**inter-TSF transfers**
Политика безопасности организации: Одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.	**organisational security policies**
Политика безопасности ОО: Совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОО.	**TOE security policy**
Политика функции безопасности: Политика безопасности, осуществляемая ФБ.	**security function policy**
Полуформальный: Выраженный на языке с ограниченным синтаксисом и определенной семантикой.	**semiformal**
Пользователь: Любая сущность (человек-пользователь или внешний объект ИТ) вне ОО, которая взаимодействует с ОО.	**user**
Потенциал нападения: Прогнозируемый потенциал для успешного (в случае реализации) нападения, выраженный в показателях компетентности, ресурсов и мотивации нарушителя.	**attack potential**
Продукт: Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.	**product**
Профиль защиты: Независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.	**protection profile**
Расширение: Добавление в ЗБ или ПЗ функциональных требований, не содержащихся в части 2 настоящего стандарта, и/или требований доверия, не содержащихся в части 3 настоящего стандарта.	**extension**
Ресурс ОО: Все, что может использоваться или потребляться в ОО.	**TOE resource**

Роль: Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и ОО. **role**

Связность: Свойство ОО, позволяющее ему взаимодействовать с объектами ИТ, внешними по отношению к ОО. Это взаимодействие включает обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации. **connectivity**

Секрет: Информация, которая должна быть известна только уполномоченным пользователям и/или ФБО для осуществления определенной ПФБ. **secret**

Семейство: Группа компонентов, которые объединены одинаковыми целями безопасности, но могут отличаться акцентами или строгостью. **family**

Система: Специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации. **system**

Система оценки: Административно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют ОК. **evaluation scheme**

Средняя СФБ: Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения. **SOF-medium**

Стойкость функции безопасности: Характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности. **strength of function**

Субъект: Сущность в пределах ОДФ, которая инициирует выполнение операций. **subject**

Уполномоченный пользователь: Пользователь, которому в соответствии с ПБО разрешено выполнять какую-либо операцию. **authorised user**

Усиление: Добавление одного или нескольких компонентов доверия из части 3 настоящего стандарта в ОУД или пакет требований доверия. **augmentation**

Уточнение: Добавление деталей в компонент. **refinement**

Функции безопасности ОО: Совокупность всех функций безопасности ОО, направленных на осуществление ПБО. **TOE security functions**

Функция безопасности: Функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО. **security function**

Формальный: Выраженный на языке с ограниченным синтаксисом и определенной семантикой, основанной на установившихся математических понятиях**.** **formal**

Человек-пользователь: Любое лицо, взаимодействующее с ОО. **human user**

Цель безопасности: Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям. **security objective**

Элемент: Неделимое требование безопасности. **element**

Приложение 2. Пример задания по безопасности

1. Введение

1.1. Идентификация ЗБ

Название: Межсетевой экран *Protector*. Задание по безопасности.

Обозначение: ЗБ Protector/МЭ.01-05.

Версия документа: 1.0.

Соответствие ПЗ: не декларируется.

Соответствие ОК: ОО соответствует части 2 и части 3 ОК в соответствии с ОУД 3.

Оценочный уровень доверия: ОУД3.

Предприятие-разработчик: ООО «Безопасность».

Идентификация ОК: ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

Ключевые слова: управление доступом, межсетевой экран, шлюзы прикладного уровня, сетевые фильтры, фильтры с виртуальным соединением, профиль защиты.

1.2. Аннотация ЗБ

Данное Задание по безопасности описывает и обосновывает функциональные требования и требования доверия для межсетевого экрана корпоративного уровня *Protector* (разработка компании ООО «Безопасность»).

МЭ *Protector* (далее по тексту - МЭ) представляет собой программный продукт, осуществляющий непосредственную защиту корпоративных ресурсов при получении из внешнего (неконтролируемого в рамках предприятия или организации либо с иными требованиями по безопасности) информационного пространства и/или предоставлении информационных сервисов для пользователей внешнего информационного пространства.

1.3. Соглашения

Общие критерии допускают выполнение определенных в части 2 ОК операций над функциональными требованиями. В настоящем ЗБ используются операции «уточнение», «выбор», «назначение» и «итерация».

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

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

Операция «назначение» используется для присвоения конкретного значения ранее не конкретизированному параметру. Операция «назначение» обозначается **полужирным текстом**.

Операция «итерация» используется для более чем однократного использования компонента функциональных требований безопасности ИТ при различном выполнении

разрешенных операций (уточнение, выбор, назначение). Выполнение «итерации» сопровождается помещением номера итерации, заключенного в круглые скобки, после мнемонического (краткого) имени.

Соглашения по использованию выделений шрифтом при выполнении операций над функциональными требованиями приведены в табл. 1.

Таблица 1: ***Соглашение по использованию выделения шрифтом***

Соглашение	Цель	Операция
Полужирный	Выделение текста полужирным шрифтом применяется к результату операции назначения.	Назначение
Полужирный курсив	Выделение текста полужирным курсивом применяется к результату операции уточнения.	Уточнение
Подчеркивание	Выделение текста подчеркиванием применяется к результату операции выбора в требованиях ОК.	Выбор

1.4. Термины

В данном ЗБ используются следующие термины и определения:

Межсетевым экраном называется локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей во внутреннее информационное пространство и/или выходящей из него, и обеспечивает защиту ИС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении во (из) внутреннее информационное пространство.

Информационным пространством называется информационная и телекоммуникационная инфраструктура, способная предоставлять и получать информационные сервисы.

Внешним информационным пространством называется информационное пространство, неконтролируемое в рамках политики безопасности организации вследствие наличия иного собственника каких-либо компонент информационного пространства либо с более слабыми требованиями к сервисам безопасности, чем в рассматриваемой информационной системе.

Внутренним информационным пространством называется информационное пространство, защищаемое МЭ. Основным признаком внутреннего информационного пространства является возможность проведения согласованной политики безопасности в пределах этого пространства и на межсетевом экране.

Информационным обменом называется получение и/или предоставление информационных сервисов. Внешним информационным обменом называется информационный обмен с внешним информационным пространством.

Правила фильтрации – перечень условий, по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных), и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

Экранирование – функция МЭ, позволяющая поддерживать безопасность объектов внутреннего информационного пространства, игнорируя несанкционированные запросы из внешнего информационного пространства.

Безопасным состоянием ОО называется состояние, в котором ОО корректно выполняет фильтрацию IP-пакетов и данных протоколов прикладного уровня, реализует защиту от атак спуфинга и фрагментации и осуществляет трансляцию сетевых адресов в соответствии с правилами, установленными уполномоченным администратором информационной безопасности, реализуя при этом полный аудит сетевой активности.

2. Описание объекта оценки

ЗБ Protector/МЭ.01-05 определяет набор требований безопасности, предъявляемых к объекту оценки – межсетевому экрану корпоративного уровня Protector.

МЭ предназначен для контроля внешнего информационного обмена путем обеспечения описанных в ЗБ сервисов безопасности. МЭ играет роль посредника в осуществлении внешнего информационного обмена. Сервисы безопасности МЭ обеспечиваются на сетевом, сеансовом уровне и уровне приложений. МЭ предусматривает возможность эффективного управления политиками фильтрации за счёт использования системы графического интерфейса пользователя.

МЭ представляет собой программный продукт, функционирующий под управлением операционной системы Microsoft Windows 2003.

3. Среда безопасности ОО

3.1. Предположения безопасности

A.SINGLEPT (Единая точка входа) ОО является единственной точкой контроля внешнего информационного обмена.

A.SECURE (Контроль физического доступа) ОО, связанная с ним консоль, активное сетевое и кроссовое оборудование, а также система электропитания защищены физически и доступны только для обслуживающего персонала.

A.COMMS (Защита передаваемых данных) Защита передаваемых в процессе внешнего информационного обмена данных обеспечивается дополнительными средствами безопасности, либо было явно принято решение о том, что такая защита не требуется.

A.USER (Пользователи) ОО не предоставляет информационных сервисов общего назначения. ОО осуществляет идентификацию и аутентификацию пользователей, осуществляющих внешний информационный обмен. Доступ к ресурсам ОО осуществляется только уполномоченным администратором (администраторами) в соответствии с регламентом эксплуатации ОО.

A.ENV_MANAGE (Среда управления) Управление настройками ОО, включая безопасность содержащейся в нем информации, а также выделение уровней системных ресурсов осуществляется в соответствии с документацией, поставляемой в комплекте с ОО.

A.NOEVIL (Обслуживающий персонал) Предполагается, что уполномоченные администраторы квалифицированно выполняют обязанности по реализации документированной политики доступа.

3.2. Предотвращаемые угрозы

3.2.1. Угрозы, предотвращаемые ОО

T.LACCESS

1. **Аннотация угрозы** – лицо, не имеющее соответствующих полномочий, может получить логический доступ к ОО.

2. **Источники угрозы** – пользователи ИС, имеющие доступ к ОО из внутреннего информационного пространства.

3. **Способ реализации угрозы** – доступ к консоли управления ОО и осуществление модификации его настроек с использованием штатных утилит администрирования.

4. **Используемые уязвимости** – некорректное разграничение логического доступа к ОО.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – невозможность контроля за информацией, поступающей во внутреннее информационное пространство и/или выходящей из него.

T.AUTH

1. **Аннотация угрозы** – внешний пользователь может предпринять попытку НСД, выдавая себя за другого пользователя путем активного или пассивного перехвата аутентификационной информации.

2. **Источники угрозы** – пользователи, имеющие доступ к ОО из внешнего информационного пространства.

3. **Способ реализации угрозы** – активный или пассивный перехват аутентификационной информации, передаваемой по сети, осуществляемый с использованием анализаторов сетевого трафика.

4**. Используемые уязвимости** – недостатки реализации процедур аутентификации сеансов связи с уполномоченным администратором.

5. **Вид активов, потенциально подверженных угрозе** – конфигурационные файлы, информация.

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

7. **Возможные последствия реализации угрозы** – невозможность контроля за информацией, поступающей во внутреннее информационное пространство и/или выходящей из него.

T.ISPOOF

1. **Аннотация угрозы** - внешний пользователь может предпринять попытку НСД, выдавая себя за внутреннего пользователя путем подделки IP-адреса.

2. **Источники угрозы** – пользователи ИС, имеющие доступ к ОО из внутреннего информационного пространства.

3. **Способ реализации угрозы** – использование штатных утилит сетевого взаимодействия в целях установления соединения из внешнего информационного пространства с использованием IP-адреса, соответствующего субъекту внутреннего информационного пространства.

4. **Используемые уязвимости** – недостатки механизма разграничения субъектов внутреннего и внешнего информационного пространства.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7**. Возможные последствия реализации угрозы** – получение доступа к защищаемой информации неуполномоченным пользователем.

T.SSPOOF

1. **Аннотация угрозы -** пользователь может предпринять попытку НСД, используя запрещенный сервис, имитируя при этом использование разрешенного сервиса.

2. **Источники угрозы** – пользователи, имеющие доступ к ОО из внешнего информационного пространства.

3. **Способ реализации угрозы** – попытка установления соединения из внешнего информационного пространства с использованием запрещённого сервиса, имитирующего разрешённый сервис.

4. **Используемые уязвимости** – недостатки механизма идентификации сетевых сервисов.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7**. Возможные последствия реализации угрозы** – получение доступа к защищаемой информации неуполномоченным пользователем.

T.NATTACK

1. **Аннотация угрозы** - нарушитель может предпринять попытку НСД к защищаемым ОО сегментам ИС либо отдельным компьютерам, находящимся в указанных сегментах. Целью нападения может быть НСД к информационным ресурсам либо реализация отказа в обслуживании.

2. **Источники угрозы** – пользователи, имеющие доступ к ОО из внешнего информационного пространства.

3. **Способ реализации угрозы** – несанкционированная попытка установления соединения с защищаемыми ОО сегментами ИС либо отдельными компьютерами, находящимися в указанных сегментах, из внешнего информационного пространства, осуществляемая с использованием стандартных средств сетевого взаимодействия.

4. **Используемые уязвимости –** недостатки механизмов разграничения доступа пользователей к защищаемым объектам сети.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – получение доступа к защищаемой информации неуполномоченным пользователем.

T.EVAL

1. **Аннотация угрозы** - нарушитель может предпринять попытку получения информации о структуре защищаемых сегментов ИС, разрешенных сервисах, способах их реализации либо существующих уязвимостях.

2. **Источники угрозы** – пользователи, имеющие доступ к ОО из внешнего информационного пространства.

3. **Способ реализации угрозы** – сбор информации о структуре защищаемых сегментов ИС, разрешенных сервисах, способах их реализации либо существующих уязвимостях путём сканирования сети. Данные действия могут выполняться в ручном режиме путём последовательного опроса сетевых сервисов или с использованием автоматизированных сканеров безопасности.

4. **Используемые уязвимости** – недостатки механизмов сокрытия структуры внутреннего информационного пространства.

5. **Вид активов, потенциально подверженных угрозе** – информация о структуре внутреннего информационного пространства.

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

7. **Возможные последствия реализации угрозы** – сбор предварительной информации для осуществления НСД к ресурсам внутреннего информационного пространства.

T.AUDIT

1. **Аннотация угрозы –** нарушитель может осуществить повреждение или подмену записей аудита с целью помешать расследованию либо оперативному пресечению попытки НСД.

2. **Источники угрозы** – пользователи, имеющие доступ к ОО из внутреннего информационного пространства.

3. **Способ реализации угрозы** – получение доступа к записям аудита с использованием штатных средств ОС и осуществление их модификации или удаления.

4. **Используемые уязвимости –** недостатки механизмов защиты записей аудита.

5. **Вид активов, потенциально подверженных угрозе** – записи аудита.

6. **Нарушаемые свойства безопасности активов –** целостность.

7. **Возможные последствия реализации угрозы** – возможность совершения неконтролируемых действий пользователями ИС.

T.DCORRUPT

1**. Аннотация угрозы** - нарушитель может изменить конфигурацию ОО либо иных данных, обеспечивающих безопасность (например, контрольных записей либо контрольных сумм).

2. **Источники угрозы** – пользователи, имеющие доступ к ОО из внутреннего информационного пространства.

3. **Способ реализации угрозы** – несанкционированное получение доступа к параметрам конфигурации ОО или иным данным, обеспечивающим безопасность, с целью их модификации или удаления.

4. **Используемые уязвимости** – недостатки механизмов защиты параметров конфигурации ОО или иных данных, обеспечивающих безопасность.

5. **Вид активов, потенциально подверженных угрозе** – параметры конфигурации ОО и иные данные, обеспечивающие безопасность.

6**. Нарушаемые свойства безопасности активов** – целостность.

7. **Возможные последствия реализации угрозы** – возможность нарушения установленных правил защиты.

T.CRASH

1. **Аннотация угрозы** - может быть предпринята успешная попытка НСД вследствие нарушения работоспособности ОО либо его окружения.

2. **Источники угрозы** – пользователи, имеющие доступ к ОО из внешнего информационного пространства.

3. **Способ реализации угрозы** – реализация НСД к ресурсам внутреннего информационного пространства вследствие нарушения работоспособности ОО либо его окружения.

4. **Используемые уязвимости** – недостатки механизмов защиты ресурсов внутреннего информационного пространства на случай неработоспособности ОО.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – возможность реализации несанкционированного доступа к защищаемой информации.

3.2.2. Угрозы, предотвращаемые средой

T.INSTALL

1. **Аннотация угрозы** - ОО может быть доставлен и установлен таким образом, что появится возможность нарушения безопасности.

2. **Источники угрозы** – пользователи, осуществляющие доставку и установку ОО.

3. **Способ реализации угрозы** – некорректная доставка и установка ОО, создающая возможность для нарушения безопасности.

4. **Используемые уязвимости** – недостатки механизмов контроля за поставкой и установкой ОО.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – возможность реализации несанкционированного доступа к защищаемой информации.

T.OPERATE

1. **Аннотация угрозы** - нарушение безопасности может произойти из-за неправильного управления или эксплуатации ОО.

2. **Источники угрозы** – администраторы, осуществляющие настройку и эксплуатацию ОО.

3. **Способ реализации угрозы** – ошибки при настройке или эксплуатации ОО, создающие возможность для нарушения безопасности.

4**. Используемые уязвимости** – недостатки механизмов контроля конфигурации ОО.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – возможность реализации несанкционированного доступа к защищаемой информации.

T.INSHARE

1. **Аннотация угрозы** - внутренние пользователи могут несанкционированно передать конфиденциальную информацию в процессе внешнего информационного обмена, либо реализовать отказ в обслуживании, используя разрешенные информационные сервисы.

2**. Источники угрозы** – пользователи ИС, имеющие доступ к ресурсам внутреннего информационного пространства.

3. **Способ реализации угрозы** – несанкционированная передача конфиденциальной информации или реализация отказа в обслуживании с использованием разрешённых информационных сервисов.

4**. Используемые уязвимости** – недостатки механизмов контроля содержимого информационных потоков, реализуемых с использованием разрешённых информационных сервисов.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – возможность реализации несанкционированного доступа к защищаемой информации и атак на отказ в обслуживании.

T.INALL

1. **Аннотация угрозы** - пользователи могут осуществлять НСД с компьютера, на базе которого функционирует ОО, к ресурсам компьютеров, подключенных к защищенным сегментам внутренней сети.

2. **Источники угрозы** – пользователи ИС, имеющие физический доступ к ОО.

3. **Способ реализации угрозы** – осуществление несанкционированного доступа к ресурсам внутреннего информационного пространства с компьютера, на котором функционирует ОО, за счёт физического доступа к данному компьютеру.

4. **Используемые уязвимости** – недостатки механизмов контроля физического доступа к ОО.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – возможность реализации несанкционированного доступа к защищаемой информации.

T.SERVICES

1. **Аннотация угрозы** - может быть реализована попытка НСД с использованием уязвимостей логики протоколов высокого уровня.

2. **Источники угрозы** – пользователи, имеющие физический доступ к ОО из внутреннего или внешнего информационного пространства.

3. **Способ реализации угрозы** – реализация попытки НСД с использованием уязвимостей логики протоколов высокого уровня. ОО может отказать в доступе к конкретным сервисам либо их отдельным компонентам, однако в случае разрешения появляется возможность атак на соответствующие сервисы. Такие атаки могут выполняться в ручном режиме или с использованием сканеров безопасности.

4. **Используемые уязвимости** – некорректности функционирования логики протоколов высокого уровня.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – возможность реализации несанкционированного доступа к защищаемой информации.

T.COMMS

1. **Аннотация угрозы** - нарушитель может перехватить конфиденциальную информацию, передаваемую в процессе внешнего информационного обмена.

2. **Источники угрозы** – пользователи, имеющие доступ к ОО из внешнего информационного пространства.

3. **Способ реализации угрозы** – перехват информации, передаваемой по каналам связи в ходе внешнего информационного обмена, за счёт использования анализаторов сетевого трафика.

4. **Используемые уязвимости** – недостатки механизмов канальной защиты передаваемой информации.

5. **Вид активов, потенциально подверженных угрозе** – информация.

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

7. **Возможные последствия реализации угрозы** – возможность реализации несанкционированного доступа к защищаемой информации.

3.3. Политика безопасности

P.OWNER Организация является владельцем информации и полностью распоряжается доступом к ней, регламентируя правила работы внутренних пользователей с внешними информационными сервисами и правила работы внешних пользователей с сервисами, предоставляемыми организацией.

P.INT_ROLE Права внутренних пользователей на получение внешних информационных сервисов определяются исходя из их должностных обязанностей и регламентируют разрешенные пользователям сервисы, доступные компоненты сервисов, время их получения, объем получаемых сервисов.

P.EXT_ROLE Права внешних пользователей на получение информационных сервисов, предоставляемых для них организацией, определяются исходя из целей и задач организации, реализуемых в процессе внешнего информационного обмена, и регламентируют разрешенные сервисы либо их компоненты, время их получения, объем получаемых сервисов и приоритетность их обработки.

P.ADM_ROLE Права администратора ОО определяются исходя из необходимости осуществлять поддержку корректной работы ОО в соответствии с заданными правилами внешнего информационного обмена. Полномочия администратора ОО не распространяются на системное окружение, обеспечивающее работу ОО.

P.AUTH При осуществлении внешнего информационного обмена может проводиться предварительная аутентификация внешних пользователей, на основе результатов которой может приниматься решение о разрешении либо запрете на получение сервиса.

P.EVAL Внешние пользователи имеют только ту информацию о системе, которая им необходима для получения разрешенных им информационных сервисов. Внешним пользователям не разрешено проводить исследование структуры системы, предоставляющей информационные сервисы, перехватывать служебную либо аутентификационную информацию. Реализация попыток получения такой информации интерпретируется как попытка НСД.

P.ACCOUNT Пользователи должны нести ответственность за безопасность действий, выполняемых ими в процессе работы, путем неукоснительного выполнения утвержденных правил внешнего информационного обмена.

P.AUDIT Ведется аудит внешнего информационного обмена как в отношении действий внешних, так и в отношении действий внутренних пользователей. Пользователи могут (но не должны обязательно) уведомляться о проведении аудита их деятельности.

P.MAINTENANCE Перед проведением обслуживающих и профилактических работ вся критически важная информация ОО должна быть защищена.

4. Цели безопасности

4.1. Цели безопасности для ОО

O.ACCESS (***Посредничество в предоставлении доступа***) ОО обеспечивает контроль внешнего информационного обмена, разрешая или запрещая передачу информации на основе правил управления доступом, определяемых атрибутами субъектов внешнего информационного обмена либо задаваемых уполномоченным администратором ОО.

O.ADMIN (***Доступ администратора***) Доступ к ОО предоставляется только уполномоченному администратору, которому предоставляется возможность конфигурирования и администрирования ОО в соответствии с утвержденными регламентами.

O.ACCOUNT (***Контроль действий отдельных пользователей***) Решение о предоставлении доступа принимается на основе уникального идентификатора пользователя. Аутентификация является механизмом, устанавливающим подлинность пользователя.

O.PROTECT (***Защита собственно ОО***) ОО обладает способностью отделять данные, необходимые для его работы (служебную и конфигурационную информацию), от обрабатываемых данных. ОО должен быть защищен от атак внешних пользователей. Сеансы связи с уполномоченным администратором должны обеспечиваться средствами контроля целостности.

O.AUDIT (***Аудит***) Необходимо, чтобы записи аудита внешнего информационного обмена не только собирались в необходимом объеме, но и представлялись в виде, удобном для просмотра администратором, и были защищены от модификации или удаления.

4.2. Цели безопасности для среды

O.INSTALL Необходимо обеспечить установку, инсталляцию и администрирование ОО таким образом, чтобы обеспечить безопасное состояние защищаемой системы.

O.SECURE Необходимо осуществление контроля физического доступа к ОО.

O.TRAIN Необходимо, чтобы уполномоченные администраторы были обучены способам администрирования ОО, знали и могли реализовать утвержденную политику внешнего информационного обмена.

O.SUPPORT Необходимо обеспечить сопровождение установленного ОО в части решения проблем, возникающих в процессе эксплуатации ОО, оперативного мониторинга и исправления недостатков в программном обеспечении.

5. Требования безопасности

В данном разделе приводятся функциональные требования и требования доверия, которым должен удовлетворять МЭ.

5.1. Функциональные требования

Функциональные требования состоят из компонентов части 2 ОК, приведенных в Таблице 2.

Таблица 2: ***Компоненты функциональных требований ОО***

Компонент	**Название**
FDP_ACC.2	Полное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_IFC.2	Полное управление информационными потоками
FDP_IFF.1	Простые атрибуты безопасности
FDP_ITC.2	Импорт данных пользователя с атрибутами безопасности
FDP_RIP.2	Полная защита остаточной информации
FDP_SDI.2	Мониторинг целостности хранимых данных и предпринимаемые действия
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_SOS.1	Верификация секретов
FIA_UAU.1	Выбор момента аутентификации
FIA_UAU.3	Аутентификация, защищенная от подделок
FIA_UAU.5	Сочетание механизмов аутентификации
FIA_UID.2	Идентификация до любых действий пользователя
FPT_AMT.1	Тестирование абстрактной машины
FPT_FLS.1	Сбой с сохранением безопасного состояния
FPT_RCV.1	Ручное восстановление
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_STM.1	Надежные метки времени
FPT_TDC.1	Базовая согласованность данных ФБО между ФБО
FPT_TST.1	Тестирование ФБО
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_SMR.1	Роли безопасности
FAU_ARP.1	Сигналы нарушителя безопасности
FAU_GEN.1	Генерация данных аудита
FAU_SAA.1	Анализ потенциального нарушения
FAU_SAR.1	Просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.4	Предотвращение потери данных аудита
FPR_ANO.1	Анонимность
FPR_PSE.1	Псевдонимность

FPR_UNL.1	Невозможность ассоциации
FTP_ITC.1	Доверенный канал передачи между ФБО

5.1.1. Защита данных пользователя (FDP)

FDP_ACC.2 (1) – Полное управление доступом

FDP_ACC.2.1 ФБО должны осуществлять **управление доступом путем фильтрации информационных сервисов** для **субъектов внешнего и внутреннего информационного пространства** и всех операций субъектов на объектах, на которые распространяется ПФБ.

FDP_ACC.2.2 ФБО должны обеспечить, чтобы на операции любого субъекта из ОДФ на любом объекте из ОДФ распространялась какая-либо ПФБ управления доступом.

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

FDP_ACC.2 (2) – Полное управление доступом

FDP_ACC.2.1 ФБО должны осуществлять ***управление доступом путем фильтрации информационных сервисов при получении информации от субъектов внешнего информационного пространства.***

FDP_ACC.2.2 ФБО должны обеспечить ***полный контроль информационных потоков при осуществлении внешнего информационного обмена.***

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

FDP_ACC.2 (3) – Полное управление доступом

FDP_ACC.2.1 ФБО должны осуществлять ***управление доступом путем фильтрации информационных сервисов при выдаче информации субъектам внешнего информационного пространства***.

FDP_ACC.2.2 ФБО должны обеспечить ***проверку соответствия информационных сервисов, запрашиваемых в процессе информационного обмена и определенных политикой безопасности, на уровне примитивов прикладного уровня.***

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

FDP_ACC.2 (4) – Полное управление доступом

FDP_ACC.2.1 ФБО должны осуществлять ***управление доступом путем фильтрации информационных сервисов при информационном обмене ОО с субъектами внешнего и внутреннего информационного пространства для аутентификации, обеспечения работы служебных сервисов для управления и диагностики работы сетевых устройств.***

FDP_ACC.2.2 ФБО должны обеспечить ***осуществление информационного обмена без маршрутизации информационных потоков на сетевом уровне модели ISO/OSI***.

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

FDP_ACF.1 – Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять **фильтрацию сервисов внешнего информационного обмена и политику управления доступом** к объектам, основываясь на **следующих атрибутах:**

- **сетевые адреса субъектов информационного обмена;**
- **корректность IP-пакетов и наличие в них дополнительных служебных полей;**
- **интерфейсы, через которые осуществляется информационный обмен;**
- **следующие атрибуты транспортного уровня модели OSI/ISO:**
  - **элементы протокола транспортного уровня;**
  - **параметры примитива транспортного уровня;**
- **следующие атрибуты прикладного уровня модели OSI/ISO:**
  - **идентификатор примитива прикладного уровня;**
  - **параметры примитива прикладного уровня;**
  - **заданная последовательность идентификаторов и/или параметров примитивов прикладного уровня;**
- **атрибуты субъектов, делающих запрос на получение информационного сервиса (идентификационная и аутентификационная информация);**
- **время/дата запроса сервисов внешнего информационного обмена.**

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

ОО производит фильтрацию на основе списков правил различных уровней модели ISO/OSI. Должна использоваться следующая последовательность анализа:

- **анализ правил в терминах атрибутов сетевого уровня;**
- **анализ правил в терминах атрибутов транспортного уровня;**
- **анализ правил в терминах атрибутов прикладного уровня.**

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах: **отсутствие правила на запрашиваемый сервис приводит к невозможности его предоставления.**

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

- **должны отклоняться запросы, исходящие из внешнего информационного пространства, но с адресацией из внутреннего информационного пространства;**
- **должны отклоняться запросы, исходящие из внутреннего информационного пространства, но с адресацией из внешнего информационного пространства;**
- **должны отклоняться широковещательные (broadcast) запросы;**
- **должны отклоняться запросы, содержащие некорректную информацию сетевого либо транспортного уровня, либо использование дополнительных служебных полей IP-пакетов;**
- **должны отклоняться запросы, содержащие недопустимые идентификаторы и/или параметры примитивов прикладного уровня;**
- **должны отклоняться запросы, содержащие недопустимые последовательности идентификаторов и/или параметров примитивов прикладного уровня.**

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

FDP_IFC.2 (1) – Полное управление информационными потоками

FDP_IFC.2.1 ФБО должны осуществлять **ПФБ управления информационными потоками на сетевом уровне** для **следующих субъектов**:

- **субъектов из внешнего/внутреннего информационного пространства, осуществляющих информационный обмен с субъектами из внутреннего/внешнего информационного пространства через ОО;**

и информации:

- **информационный поток, осуществляемый с использованием всех протоколов, кроме перечисленных в FDP_IFC.2 (2) и FDP_IFC.2 (3)**

и всех операций перемещения управляемой информации к управляемым субъектам и от них, на которые распространяется ПФБ.

FDP_IFC.2.2 ФБО должны обеспечить, чтобы в пределах ОДФ на все операции перемещения управляемой информации управляемым субъектам и от них распространялась какая-либо ПФБ управления информационными потоками.

Зависимости: FDP_IFF.1 Простые атрибуты безопасности

FDP_IFC.2 (2) – Полное управление информационными потоками

FDP_IFC.2.1 ФБО должны осуществлять **ПФБ управления информационными потоками на прикладном уровне без аутентификации для следующих субъектов:**

- **субъектов из внешнего/внутреннего информационного пространства, осуществляющих информационный обмен с субъектами из внутреннего/внешнего информационного пространства через ОО;**

и информации:

- **информационный поток, осуществляемый с использованием протоколов FTP, HTTP, SMTP**

и всех операций перемещения управляемой информации к управляемым субъектам и от них, на которые распространяется ПФБ.

FDP_IFC.2.2 ФБО должны обеспечить, чтобы в пределах ОДФ на все операции перемещения управляемой информации управляемым субъектам и от них распространялась какая-либо ПФБ управления информационными потоками.

Зависимости: FDP_IFF.1 Простые атрибуты безопасности

FDP_IFC.2 (3) – Полное управление информационными потоками

FDP_IFC.2.1 ФБО должны осуществлять **ПФБ управления информационными потоками на прикладном уровне с аутентификацией для следующих субъектов:**

- **субъектов из внешнего/внутреннего информационного пространства, осуществляющих информационный обмен с субъектами из внутреннего/внешнего информационного пространства через ОО;**

и информации:

- **информационный поток, осуществляемый с использованием протоколов Telnet, FTP, *HTTP и RLOGIN***

и всех операций перемещения управляемой информации к управляемым субъектам и от них, на которые распространяется ПФБ.

FDP_IFC.2.2 ФБО должны обеспечить, чтобы в пределах ОДФ на все операции перемещения управляемой информации управляемым субъектам и от них распространялась какая-либо ПФБ управления информационными потоками.

Зависимости: FDP_IFF.1 Простые атрибуты безопасности

FDP_IFF.1 – Простые атрибуты безопасности

FDP_IFF.1.1 ФБО должны осуществлять **политику безопасности управления информационными потоками,** основанную на следующих типах атрибутов безопасности субъектов и информации:

- **сетевые адреса субъектов информационного обмена;**
- **идентификаторы субъектов информационного обмена;**
- **интерфейсы, через которые осуществляется информационный обмен;**
- **элементы протокола транспортного уровня;**
- **запрашиваемые информационные сервисы.**

FDP_IFF.1.2 ФБО должны разрешать информационный поток между управляемыми субъектом и информацией посредством управляемой операции, если выполняются следующие правила:

- **сетевой адрес субъекта из внешнего информационного пространства транслируется во внутренний сетевой адрес, а сетевой адрес субъекта из внутреннего информационного пространства транслируется в сетевой адрес для установки соединения с внешней сетью;**
- **сетевой адрес субъекта из внутреннего информационного пространства транслируется во внешний сетевой адрес, а сетевой адрес субъекта из внешнего информационного пространства транслируется в сетевой адрес для установки соединения с внутренней сетью;**
- **идентификатор субъекта информационного обмена является допустимым для данной операции;**
- **интерфейсы, через которые осуществляется информационный обмен, являются допустимыми для данной операции;**
- **протокол транспортного уровня корректно настроен и разрешает данную операцию;**
- **запрашиваемый информационный сервис является разрешенным.**

FDP_IFF.1.6 ФБО должны явно запрещать информационный поток, основываясь на следующих правилах:

- **должны отклоняться запросы, исходящие из внешнего информационного пространства, но с адресацией из внутреннего информационного пространства;**
- **должны отклоняться запросы, исходящие из внутреннего информационного пространства, но с адресацией из внешнего информационного пространства;**
- **должны отклоняться широковещательные (broadcast) запросы;**
- **должны отклоняться запросы, содержащие некорректную информацию сетевого либо транспортного уровня, либо использование дополнительных служебных полей IP-пакетов;**
- **должны отклоняться запросы, содержащие недопустимые идентификаторы и/или параметры примитивов прикладного уровня;**
- **должны отклоняться запросы, содержащие недопустимые последовательности идентификаторов и/или параметров примитивов прикладного уровня.**

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

FDP_ITC.2 – Импорт данных пользователя с атрибутами безопасности

FDP_ITC.2.1 ФБО должны осуществлять **возможность импорта пользовательских идентификационных данных и аутентификационной информации** при импорте данных пользователя, контролируемом ПФБ, из-за пределов ОДФ.

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

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

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

Зависимости: FDP_ACC.1 Ограниченное управление доступом
FTP_ITC.1 Доверенный канал передачи между ФБО
FPT_TDC.1 Базовая согласованность данных ФБО между ФБО

FDP_RIP.2 – Полная защита остаточной информации

FDP_ RIP.2.1 ФБО должны обеспечить недоступность любого предыдущего информационного содержания ресурсов при распределении или освобождении ресурсов для всех объектов.

Зависимости: отсутствуют

FDP_SDI.2 – Мониторинг целостности хранимых данных и предпринимаемые действия

FDP_SDI.2.1 ФБО должны контролировать данные ***уполномоченного администратора ОО***, хранимые в пределах ОДФ, на наличие **ошибок целостности** для всех объектов, основываясь на следующих атрибутах:

- **файлы исполняемых модулей ОО;**
- **конфигурационных файлов и баз данных;**
- **файлов, содержащих аутентификационную информацию.**

FDP_SDI.2.2 При обнаружении ошибки целостности данных ФБО должны обеспечить **запуск процедуры оповещения администратора безопасности, а также выполнять прочие действия, предусмотренные разработчиком для восстановления ФБО и отраженные в сопроводительной документации**.

Зависимости: отсутствуют

5.1.2. Идентификация и аутентификация (FIA)

FIA_AFL.1 – Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет **задаваемое администратором число** неуспешных попыток аутентификации, относящихся к **пользователю**.

FIA_AFL.1.2 При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить **следующие действия: заблокировать доступ пользователя до снятия блокировки администратором безопасности. Должно быть сформировано соответствующее оповещение администратору безопасности**.

Зависимости: FIA_UAU.1 Выбор момента аутентификации

FIA_ATD.1 – Определение атрибутов пользователя

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

- **идентификаторы субъектов информационного обмена;**
- **идентифицированные роли безопасности субъектов информационного обмена, предусмотренные компонентом FMT_SMR.1;**
- **запрашиваемые информационные сервисы.**

Зависимости: отсутствуют

FIA_SOS.1 – Верификация секретов

FIA_SOS.1.1 ФБО должны предоставить механизм для верификации того, что секреты отвечают ***следующим требованиям: надежность паролей обеспечивается методами, устойчивыми к пассивному и активному перехвату информации***.

Зависимости: отсутствуют

FIA_UAU.1 – Выбор момента аутентификации

FIA_AFL.1 – Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет **задаваемое администратором число** неуспешных попыток аутентификации, относящихся к **пользователю**.

FIA_AFL.1.2 При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить **следующие действия: заблокировать доступ пользователя до снятия блокировки администратором безопасности. Должно быть сформировано соответствующее оповещение администратору безопасности**.

FIA_UAU.1.1 ФБО должны допускать выполнение **получения информационных сервисов, не требующих аутентификации в соответствии с утвержденной ПФБ,** от имени пользователя прежде чем пользователь аутентифицирован.

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.

Зависимости: FIA_UID.1 Выбор момента идентификации

FIA_UAU.3 – Аутентификация, защищенная от подделок

FIA_UAU.3.1 ФБО должны предотвращать применение любым пользователем ФБО аутентификационных данных, которые были подделаны.

FIA_UAU.3.2 ФБО должны предотвращать применение любым пользователем ФБО аутентификационных данных, которые были скопированы у какого-либо другого пользователя ФБО.

Зависимости: отсутствуют

FIA_UAU.5 – Сочетание механизмов аутентификации

FIA_UAU.5.1 ФБО должны предоставлять **следующий список сочетаемых механизмов аутентификации:**

- **пароль, одноразовый пароль, элемент псевдослучайной последовательности, криптографический ключ**

для поддержки аутентификации пользователя.

FIA_UAU.5.2 ФБО должны аутентифицировать любой представленный идентификатор пользователя согласно **следующему правилу:**

- **уполномоченный администратор в соответствии с принятой политикой безопасности вправе осуществлять выбор механизмов аутентификации и их правил из числа подключаемых модулей аутентификации, предоставленных разработчиком ФБО.**

Зависимости: отсутствуют

FIA_UID.2 – Идентификация до любых действий пользователя

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

Зависимости: отсутствуют

5.1.3. Защита ФБО (FPT)

FPT_AMT.1 – Тестирование абстрактной машины

FPT_AMT.1.1 ФБО должны выполнять пакет тестовых программ по запросу уполномоченного пользователя для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая положена в основу ФБО.

Зависимости: отсутствуют

FPT_FLS.1 – Сбой с сохранением безопасного состояния

FPT_FLS.1.1 ФБО должны ***обеспечивать невозможность НСД к ресурсам внутреннего информационного пространства*** при следующих типах сбоев**:**

- **любые сбои аппаратного обеспечения;**
- **любые сбои программного обеспечения;**
- **любые сбои внешнего сервера аутентификации;**
- **любые сбои ОС;**
- **любые сбои системы электропитания.**

Зависимости: ADV_SPM.1 Неформальная модель политики безопасности ОО

FPT_RCV.1 – Ручное восстановление

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

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

FPT_RVM.1 – Невозможность обхода ПБО

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

Зависимости: отсутствуют

FPT_SEP.1 – Отделение домена ФБО

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

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

Зависимости: отсутствуют

FPT_STM.1 – Надежные метки времени

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

Зависимости: отсутствуют

FPT_TDC.1 – Базовая согласованность данных ФБО между ФБО

FPT_TDC.1.1 ФБО должны обеспечить способность согласованно интерпретировать **следующие типы данных ФБО**:

- **атрибуты ПФБ, ассоциированные с данными;**
- **идентификационная и аутентификационная информация;**
- **информация аудита.**

совместно используемые ФБО и другим доверенным продуктом ИТ:

FPT_TDC.1.2 ФБО должны использовать **установленный уполномоченным администратором список правил интерпретации применяемых ФБО** при интерпретации данных ФБО, полученных от другого доверенного продукта ИТ.

Зависимости: отсутствуют

FPT_TST.1 – Тестирование ФБО

FPT_TST.1.1 ФБО должны выполнять пакет программ самотестирования при запуске, по запросу уполномоченного пользователя, **при восстановлении после сбоев** для демонстрации правильного выполнения ФБО.

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

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

Зависимости: отсутствуют

5.1.4. Управление безопасностью (FMT)

FMT_MSA.1 – Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять **политику безопасности управления доступом**, чтобы ограничить возможность модификации следующих атрибутов безопасности: **параметры конфигурации ОО** только **уполномоченными администраторами**.

Зависимости: FDP_ACC.1 Ограниченное управление доступом
FMT_SMR.1 Роли безопасности

FMT_MSA.3 – Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять **ПФБ управления доступом и информационными потоками**, чтобы обеспечить ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ.

FMT_MSA.3.2 ФБО должны предоставить возможность **уполномоченным администраторам** определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

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

FMT_MTD.1 – Управление данными ФБО

FMT_MTD.1.1 ФБО должны ограничить возможность запроса, модификации, удаления следующих данных:

- **информация аудита;**
- **конфигурационная информация**

только **уполномоченными администраторами.**

Зависимости: FMT_SMR.1 роли безопасности

FMT_SMR.1 – Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли:

- **уполномоченный администратор (пользователь) ОО.**

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

Зависимости: FMT_SMR.1 Роли безопасности

5.1.5. Аудит (FAU)

FAU_ARP.1 – Сигналы нарушения безопасности

FAU_ARP.1.1 ФБО должны предпринять **следующие действия:**

- **локальное оповещение администратора;**
- **удаленное оповещение администратора;**
- **программируемую реакцию на события в ОО**

при обнаружении возможного нарушения безопасности**.**

Зависимости: FAU_SAA.1 Анализ потенциального нарушения

FAU_GEN.1 – Генерация данных аудита

FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:
а) запуск и завершение выполнения функций аудита;
б) все события, потенциально подвергаемые аудиту, на базовом уровне аудита;
в) **следующие события:**

- **запуск и завершение выполнения функций аудита;**

- **все попытки получения сервисов прикладного уровня, блокированные ФБО;**
- **все запросы, адресованные непосредственно к ОО, в том числе для получения информации об архитектуре и конфигурации ФБО;**
- **все попытки изменения атрибутов безопасности; все запросы на получение доступа к аутентификационным данным;**
- **все запросы на использование механизмов аутентификации;**
- **завершение обработки запроса, вызванное рядом неудачных попыток аутентификации;**
- **использование функций, относящихся к администрированию ФБО;**
- **все попытки изменения параметров конфигурации ФБО.**

FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:
а) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный).
б) для каждого типа событий, потенциально подвергаемых аудиту, из числа функциональных компонентов, которые включены в ПЗ/ЗБ, **дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный)**

Зависимости: FPT_STM.1 Надёжные метки времени

FAU_SAA.1 – Анализ потенциального нарушения

FAU_SAA.1.1 ФБО должны быть способны применить набор правил мониторинга событий, подвергающихся аудиту, и указать на возможное нарушение ПБО, основываясь на этих правилах.

FAU_SAA.1.2 ФБО должны реализовать следующие правила при мониторинге событий, подвергающихся аудиту:
а) накопление или объединение известных **событий:**

- **все попытки получения сервисов прикладного уровня, блокированные ФБО;**
- **все запросы, адресованные непосредственно к ОО, в том числе для получения информации об архитектуре и конфигурации ФБО;**
- **все попытки изменения атрибутов безопасности; все запросы на получение доступа к аутентификационным данным;**
- **все запросы на использование механизмов**

аутентификации;

- **завершение обработки запроса, вызванное рядом неудачных попыток аутентификации;**
- **использование функций, относящихся к администрированию ФБО;**
- **все попытки изменения параметров конфигурации ФБО,**

указывающих на возможное нарушение безопасности**;**

б) **другие правила отсутствуют**.

Зависимости: FAU_GEN**.**1 Генерация данных аудита

FAU_SAR.1 – Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять **уполномоченным администраторам** возможность читать **всю информацию аудита** из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

Зависимости: FAU_GEN.1 Генерация данных аудита

FAU_SAR.3 – Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны предоставить возможность выполнить поиск, сортировку или упорядочение данных аудита, основанные на:

- **идентификаторах субъектов информационных сервисов сетевого, транспортного и прикладного уровня;**
- **дате, времени;**
- **логических комбинациях параметров, приведенных выше.**

Зависимости: FAU_SAR**.**1 Просмотр аудита

FAU_SEL.1 – Избирательный аудит

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

а)

- тип события;
- идентификатор пользователя;
- идентификатор объекта;
- идентификатор субъекта.

Зависимости: FAU_GEN**.**1 Генерация данных аудита
FMT_MTD.1 Управление данными ФБО

FAU_STG.1 – Защищенное хранение журнала аудита

FAU_STG.1.1 ФБО должны защищать хранимые записи аудита от

несанкционированного удаления.

FAU_STG.1.2 ФБО должны быть способны к предотвращению модификации записей аудита.

Зависимости: FAU_GEN.1 Генерация данных аудита

FAU_STG.4 – Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны выполнить запись поверх самых старых хранимых записей аудита, предотвращение событий, подвергающихся аудиту, исключая, предпринимаемые уполномоченным пользователем со специальными правами, при переполнении журнала аудита.

Зависимости: FAU_STG**.**1 Защищённое хранение журнала аудита

5.1.6. Приватность (FPR)

FPR_ANO.1 – Анонимность

FPR_ANO.1.1 ФБО должны обеспечить, чтобы **внешние субъекты информационного обмена** были не способны определить подлинное имя пользователя, связанного с **ОО**.

Зависимости: отсутствуют

FPR_PSE.1 – Псевдонимность

FPR_PSE.1.1 ФБО должны обеспечить, чтобы **внешние субъекты информационного обмена** были не способны определить подлинное имя пользователя, связанного с **субъектами, операциями и/или объектами внутреннего информационного пространства**.

FPR_PSE.1.2 ФБО должны быть способны предоставить **не менее одного** псевдонима подлинного имени пользователя для **субъектов внешнего информационного пространства**.

FPR_PSE.1.3 ФБО должны быть способны определить псевдоним пользователя и верифицировать его соответствие **согласно принятому алгоритму трансляции IP-адресов**.

Зависимости: отсутствуют

FPR_UNL.1 – Невозможность ассоциации

FPR_UNL.1.1 ФБО должны обеспечить, чтобы **пользователи и субъекты из внешнего информационного пространства** были не способны определить , что **запросы** связаны следующим образом: **однозначно связаны** с **тем или иным субъектом внутреннего информационного пространства.**

Зависимости: отсутствуют

5.1.7. Доверенный маршрут/канал (FTP)

FTP_ITC.1 – Доверенный канал передачи между ФБО

FTP_ITC.1.1 ФБО должны предоставлять канал связи между собой и ***удаленной консолью администратора***, который логически отличим от других каналов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту данных канала от модификации или раскрытия.

FTP_ITC.1.2 ФБО должны позволить ***удалённой консоли администратора*** инициировать связь через доверенный канал.

FTP_ITC.1.3 ФБО должны инициировать связь через доверенный канал для выполнения **функций администрирования**.

Зависимости: отсутствуют

5.2. Требования доверия к безопасности

Комбинация выбранных компонентов доверия к безопасности соответствует 3-му оценочному уровню доверия к безопасности (ОУД3), предусматривающему методическое тестирование и проверку.

5.2.1. Управление конфигурацией (ACM)

5.2.1.1. Средства контроля авторизации (ACM_CAP.3)

ACM_CAP.3.1D - Разработчик должен обеспечить маркировку для ОО.

ACM_CAP.3.2D - Разработчик должен использовать систему УК.

ACM_CAP.3.3D - Разработчик должен представить документацию УК.

ACM_CAP.3.1C - Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.3.2C - ОО должен быть помечен маркировкой.

ACM_CAP.3.3C - Документация УК должна включать список конфигурации и план УК.

ACM_CAP.3.4C - Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

ACM_CAP.3.5C - Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

ACM_CAP.3.6C - Система УК должна уникально идентифицировать все элементы конфигурации.

.CM_CAP.3.7C - План УК должен содержать описание, как используется система УК.

ACM_CAP.3.8C - Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

ACM_CAP.3.9C - Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

ACM_CAP.3.10C - Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

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

5.2.1.2. Охват УК объекта оценки (ACM_SCP.1)

ACM_SCP.1.1D - Разработчик должен представить документацию УК.

ACM_SCP.1.1C - Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора и документацию УК.

ACM_SCP.1.2C - Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.

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

5.2.2. Поставка и эксплуатация (ADO)

5.2.2.1. Процедуры поставки (ADO_DEL.1)

ADO_DEL.1.1D - Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

ADO_DEL.1.2.D - Разработчик должен использовать процедуры поставки.

ADO_DEL.1.1C - Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распределении версий ОО по местам использования.

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

5.2.2.2. Процедуры установки, генерации и запуска (ADO_IGS.1)

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

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

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

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

5.2.3. Разработка (ADV)

5.2.3.1. Неформальная функциональная спецификация (ADV_FSP.1)

ADV_FSP.1.1D - Разработчик должен представить функциональную спецификацию.

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

ADV_FSP.1.2C - Функциональная спецификация должна быть внутренне непротиворечивой.

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

ADV_FSP.1.4C - Функциональная спецификация должна полностью представить ФБО.

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

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

5.2.3.2. Детализация вопросов безопасности в проекте верхнего уровня (ADV_HLD.2)

ADV_HLD.2.1D - Разработчик должен представить проект верхнего уровня ФБО.

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

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

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

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

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

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

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

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

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

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

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

5.2.3.3. Неформальная демонстрация соответствия (ADV_RCR.1)

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

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

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

5.2.4. Руководства (AGD)

5.2.4.1. Руководство администратора (AGD_ADM.1)

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

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

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

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

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

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

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

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

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

AGD_ADM.1.1E - Оценщик должен подтвердить, что представленная информация выполняет все требования к содержанию и представлению свидетельства.

5.2.4.2. Руководство пользователя (AGD_USR.1)

AGD_USR.1.1D - Разработчик должен представить руководство пользователя.

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

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

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

AGD_USR.1.4C - Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая

обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.

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

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

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

5.2.5. Поддержка жизненного цикла (ALC)

5.2.5.1. Идентификация мер безопасности (ALC_DVS.1)

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

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

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

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

ALC_DVS.1.2E - Оценщик должен подтвердить применение мер безопасности.

5.2.6. Тестирование (ATE)

5.2.6.1. Анализ покрытия (ATE_COV.2)

ATE_COV.2.1D - Разработчик должен представить анализ покрытия тестами.

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

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

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

5.2.6.2. Тестирование: проект верхнего уровня (ATE_DPT.1)

ATE_DPT.1.1D - Разработчик должен представить анализ глубины тестирования.

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

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

5.2.6.3. Функциональное тестирование (ATE_FUN.1)

ATE_FUN.1.1D - Разработчик должен протестировать ФБО и задокументировать результаты.

ATE_FUN.1.2D - Разработчик должен представить тестовую документацию.

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

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

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

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

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

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

5.2.6.4. Выборочное независимое тестирование (ATE_IND.2)

ATE_IND.2.1D - Разработчик должен представить ОО для тестирования.

ATE_IND.2.1C - ОО должен быть пригоден для тестирования.

ATE_IND.2.2C - Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.

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

ATE_IND.2.2E - Оценщик должен протестировать необходимое подмножество ФБО, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

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

5.2.7. Оценка уязвимостей (AVA)

5.2.7.1. Экспертиза руководств (AVA_MSU.1)

AVA_MSU.1.1D - Разработчик должен представить руководства по применению ОО.

AVA_MSU.1.1C - Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.1.2C - Руководства должны быть полны, однозначны, непротиворечивы и обоснованы.

AVA_MSU.1.3C - Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.1.4C - Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль над процедурами, физическими мерами и персоналом).

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

AVA_MSU.1.2E - Оценщик должен повторить все процедуры конфигурирования и установки для подтверждения того, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

AVA_MSU.1.3E - Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

5.2.7.2. Оценка стойкости функции безопасности ОО (AVA_SOF.1)

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

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

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

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

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

5.2.7.3. Анализ уязвимостей разработчиком (AVA_VLA.1)

AVA_VLA.1.1D - Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску явных путей, которыми пользователь может нарушить ПБО.

AVA_VLA.1.2D - Разработчик должен задокументировать местоположение явных уязвимостей.

AVA_VLA.1.1C - Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

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

AVA_VLA.1.2E - Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета явных уязвимостей.

6. Краткая спецификация объекта оценки

6.1. Функции безопасности ОО

В данном разделе представлено описание функций безопасности ОО и их сопоставление с функциональными требованиями безопасности.

ОО реализует следующие функции безопасности:

SF.Administer Управление настройками МЭ
SF.Trafcontr Фильтрация IP-пакетов
SF.Antispoof Защита от спуфинга
SF.Defrag Защита от фрагментации
SF.NAT Трансляция адресов
SF.Auth Аутентификация
SF.Filter Фильтрация данных
SF.Audit Протоколирование
SF.Alert Сигнализация

6.1.1. Управление настройками МЭ (SF.Administer)

ОО предоставляет администратору возможность управления настройками МЭ, в том числе установки правил фильтрации и трансляции адресов. Настройка осуществляется уполномоченным администратором путём задания правил фильтрации и управления информационными потоками с использованием графического интерфейса пользователя.

SF.Administer удовлетворяет следующим функциональным требованиям безопасности:

FIA_AFL.1 Обработка отказов аутентификации. Данный компонент определяет порядок реагирования администратора на повторные попытки нападения на ОО.

FIA_SOS.1 Верификация секретов. Данный компонент предоставляет администратору возможность обеспечения стойкости парольной защиты при аутентификации.

FIA_UAU.5 Сочетание механизмов аутентификации. Данный компонент предоставляет администратору возможность гибкого управления используемыми механизмами аутентификации с учётом требований политики безопасности организации.

FIA_UID.2 Идентификация до любых действий пользователя. Данный компонент позволяет реализовать подотчётность администратора за счёт обязательной аутентификации до совершения любых действий в отношении ОО.

FPT_RCV.1 Ручное восстановление. Данный компонент позволяет администратору реализовать возврат ОО в безопасное состояние в случае сбоя.

FPT_SEP.1 Отделение домена ФБО. Данный компонент технологически разграничивает доверенных администраторов и субъектов, не являющихся доверенными, и ограничивает доступ администратора только к средствам конфигурирования ФБО.

FMT_MSA.1 Управление атрибутами безопасности. Данный компонент допускает ролевое участие в управлении идентифицированными атрибутами безопасности.

FMT_MSA.3 Инициализация статических атрибутов. Данный компонент определяет требования к значениям по умолчанию и предоставляет администраторам возможность определять альтернативные начальные значения атрибутов безопасности.

FMT_MTD.1 Управление данными ФБО. Данный компонент допускает уполномоченных администраторов к управлению данными ОО.

FMT_SMR.1 Роли безопасности. Данный компонент управляет назначением ролей администраторам.

FAU_SAR.1 Просмотр аудита. Данный компонент предусматривает предоставление уполномоченным администраторам возможности использования данных журнала аудита.

FTP_ITC.1 Доверенный канал передачи между ФБО. Данный компонент регламентирует предоставление администратору удалённой консоли управления, взаимодействующей с ОО по защищённому протоколу.

6.1.2. Фильтрация IP-пакетов (SF.Trafcontr)

ОО обеспечивает фильтрацию IP-пакетов в соответствии с установленными правилами перемещения информации между объектами внутреннего и внешнего информационного пространства. Фильтрация осуществляется путём анализа содержимого IP-пакетов и сравнения его с установленными уполномоченным администратором в соответствии с политикой безопасности организации правилами фильтрации.

SF.Trafcontr удовлетворяет следующим функциональным требованиям безопасности:

FDP_ACC.2(1), FDP_ACC.2(2), FDP_ACC.2(3), FDP_ACC.2(4) Полное управление доступом. Данные компоненты определяют порядок реализации механизмов фильтрации информационных потоков для организации управления доступом.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности. Данный компонент определяет параметры данных IP-пакетов, на основании которых осуществляется фильтрация.

FDP_IFC.2(1), FDP_IFC.2(2), FDP_IFC.2(3) Полное управление информационными потоками. Данные компоненты определяют информационные потоки, для которых осуществляется фильтрация IP-пакетов.

FDP_IFF.1 Простые атрибуты безопасности. Данный компонент показывает, как вводятся атрибуты безопасности, используемые при организации фильтрации.

FDP_RIP.2 Полная защита остаточной информации. Данный компонент затрагивает технические аспекты реализации механизма фильтрации IP-пакетов.

FIA_ATD.1 Определение атрибутов пользователя. Данный компонент определяет атрибуты безопасности, ассоциированные с пользователем и оказывающие влияние на механизм фильтрации IP-пакетов.

FIA_SOS.1 Верификация секретов. Данный компонент определяет требования к механизмам аутентификации, непосредственно связанным с процессом фильтрации IP-пакетов.

FIA_UAU.1 Выбор момента аутентификации. Данный компонент поддерживает корректность правил фильтрации за счёт задания требований к процедуре аутентификации.

FIA_UAU.3 Аутентификация, защищенная от подделок. Данный компонент накладывает дополнительные ограничения по стойкости на механизм аутентификации.

FIA_UAU.5 Сочетание механизмов аутентификации. Данный компонент обеспечивает гибкость и масштабируемость при реализации механизмов аутентификации.

FIA_UID.2 Идентификация до любых действий пользователя. Данный компонент обеспечивает целостность правил фильтрации IP-пакетов.

FPT_FLS.1 – Сбой с сохранением безопасного состояния. Данный компонент определяет порядок поддержки установленных правил фильтрации в случае сбоя одного из перечисленных типов.

FPT_RCV.1 Ручное восстановление. Данный компонент определяет порядок поддержки механизма фильтрации в случае возникновения нештатных ситуаций.

FPT_RVM.1 Невозможность обхода ПБО. Данный компонент гарантирует обязательное выполнение правил фильтрации для всех информационных потоков из внешнего во внутреннее и из внутреннего во внешнее информационное пространство.

FPT_STM.1 Надежные метки времени. Данный компонент поддерживает технический аспект реализации ряда механизмов фильтрации, предполагающих анализ временных зависимостей между компонентами IP-пакетов.

FPT_TDC.1 Базовая согласованность данных ФБО между ФБО. Данный компонент регламентирует порядок совместного использования данных ФБО между ФБО при реализации правил фильтрации.

FMT_MSA.1 Управление атрибутами безопасности. Данный компонент допускает ролевое участие пользователей в управлении механизмами фильтрации.

FMT_MSA.3 Инициализация статических атрибутов. Данный компонент определяет требования к значениям по умолчанию для атрибутов безопасности, используемых при реализации механизмов фильтрации.

FMT_MTD.1 Управление данными ФБО. Данный компонент допускает уполномоченных пользователей в соответствии с их ролями к управлению механизмом фильтрации.

FMT_SMR.1 Роли безопасности. Данный компонент определяет роли уполномоченных пользователей, допущенных к управлению механизмом IP-фильтрации.

FAU_ARP.1 Сигналы нарушения безопасности. Данный компонент определяет действия ОО при нарушении правил фильтрации IP-пакетов.

FTP_ITC.1 Доверенный канал передачи между ФБО. Данный компонент определяет порядок реализации удаленного взаимодействия ОО и администратора для настройки правил фильтрации.

6.1.3. Защита от спуфинга (SF.Antispoof)

ОО обеспечивает защиту от атак, использующих IP-спуфинг, т.е. подделку IP-адреса в соответствующем поле IP-пакета. Защита обеспечивается путём анализа логики сетевого взаимодействия.

SF.Antispoof удовлетворяет следующим функциональным требованиям безопасности:

FDP_ACC.2(1), FDP_ACC.2(2), FDP_ACC.2(3), FDP_ACC.2(4) Полное управление доступом. Данные компоненты определяет механизм управления доступом путём полного контроля информационных потоков с учётом анализа логики сетевого взаимодействия.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности. Данный компонент определяет атрибуты безопасности, анализ которых позволяет реализовать защиту от атак спуфинга.

FDP_IFC.2(1), FDP_IFC.2(2), FDP_IFC.2(3) Полное управление информационными потоками. Данные компоненты регламентируют исчерпывающий анализ информационных потоков, .что обеспечивает защиту от атак спуфинга.

FDP_IFF.1 Простые атрибуты безопасности. Данный компонент определяет типы атрибутов безопасности субъектов и информации, используемых при реализации политики безопасности управления информационными потоками с учётом защиты от атак IP-спуфинга.

6.1.4. Защита от фрагментации (SF.Defrag)

ОО обеспечивает защиту от атак, связанных с фрагментацией IP-пакетов. Защита обеспечивается путём анализа логики сетевого взаимодействия.

SF.Defrag удовлетворяет следующим функциональным требованиям безопасности:

FDP_ACC.2(1), FDP_ACC.2(2), FDP_ACC.2(3), FDP_ACC.2(4) Полное управление доступом. Данные компоненты определяют механизм управления доступом путём полного контроля информационных потоков с учётом анализа логики сетевого взаимодействия.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности. Данный компонент определяет атрибуты безопасности, анализ которых позволяет реализовать защиту от атак фрагментации.

FDP_IFC.2(1), FDP_IFC.2(2), FDP_IFC.2(3) Полное управление информационными потоками. Данные компоненты регламентируют исчерпывающий анализ информационных потоков, что обеспечивает защиту от атак фрагментации.

FDP_IFF.1 Простые атрибуты безопасности. Данный компонент определяет типы атрибутов безопасности субъектов и информации, используемых при реализации политики безопасности управления информационными потоками с учётом защиты от атак фрагментации.

6.1.5. Трансляция адресов (SF.NAT)

ОО выполняет трансляцию сетевых адресов с целью сокрытия информации об объектах внутреннего информационного пространства от субъектов доступа, действующих в пределах внешнего информационного пространства.

SF.NAT удовлетворяет следующим функциональным требованиям безопасности:

FPR_PSE.1 Псевдонимность. Данный компонент определяет порядок защиты структуры внутреннего информационного пространства от внешних субъектов информационного обмена путём реализации трансляции адресов.

FPR_UNL.1 Невозможность ассоциации. Данный компонент уточняет требования к механизмам защиты запросов, связанных с субъектами внутреннего информационного пространства.

6.1.6. Аутентификация (SF.Auth)

ОО обеспечивает аутентификацию уполномоченных администраторов (пользователей), реализующих право доступа к интерфейсу управления настройками и параметрами МЭ. Управление может осуществляться как локально, так и через удалённую консоль, взаимодействие которой с ОО осуществляется с использованием защищённого протокола передачи данных.

SF.Auth удовлетворяет следующим функциональным требованиям безопасности:

FDP_ITC.2 Импорт данных пользователей с атрибутами безопасности. Данный компонент определяет порядок импорта пользовательских идентификационных данных и аутентификационной информации при импорте данных пользователя, контролируемом ПФБ, из-за пределов ОДФ.

FIA_AFL.1 Обработка отказов аутентификации. Данный компонент накладывает ограничение на допустимое число попыток аутентификации и определяет действия ОО в случае нарушения допустимого числа попыток.

FIA_ATD.1 Определение атрибутов пользователя. Данный компонент определяет пользовательские атрибуты безопасности, используемые в процедуре аутентифиукации.

FIA_SOS.1 Верификация секретов. Данный компонент предъявляет требования к стойкости аутентификационных данных по отношению к специального вида атакам, направленным на перехват информации.

FIA_UAU.1 Выбор момента аутентификации. Данный компонент определяет границы применимости требования обязательной аутентификации всех пользователей ОО.

FIA_UAU.3 Аутентификация, защищенная от подделок. Данный компонент требует предотвращения применения поддельной аутентификационной информации.

FIA_UAU.5 Сочетание механизмов аутентификации. Данный компонент обеспечивает возможность гибкой настройки механизмов аутентификации с учётом требований политики безопасности организации.

FIA_UID.2 Идентификация до любых действий пользователя. Данный компонент требует обязательной аутентификации пользователя до начала любых действий, выполняемых при посредничестве ФБО.

FPR_ANO.1 Анонимность. Данный компонент регламентирует защиту аутентификационной информации пользователей от внешних субъектов информационного обмена.

FPR_PSE.1 Псевдонимность. Данный компонент регламентирует дополнительные механизмы защиты аутентификационной информации пользователей от внешних субъектов информационного обмена.

FPR_UNL.1 Невозможность ассоциации. Данный компонент требует, чтобы пользователи и субъекты из внешнего информационного пространства были не способны определить, что запросы на аутентификацию однозначно связаны с тем или иным субъектом внутреннего информационного пространства.

6.1.7. Фильтрация данных (SF.Filter)

ОО обеспечивает фильтрацию данных на прикладном уровне (для протоколов FTP, HTTP и SMTP). Фильтрация данных осуществляется путём сопоставления команд указанных протоколов прикладного уровня ISO/OSI с перечнем допустимых.

SF.Filter удовлетворяет следующим функциональным требованиям безопасности:

FDP_IFC.2(1), FDP_IFC.2(2), FDP_IFC.2(3) Полное управление информационными потоками. Данные компоненты регламентируют порядок управления информационными потоками на прикладном уровне для заданного перечня протоколов прикладного уровня.

6.1.8. Протоколирование (SF.Audit)

ОО осуществляет протоколирование связанных с безопасностью событий и предоставляет механизмы для их аудита. События безопасности заносятся в журнал аудита, доступ к которым предоставляется уполномоченным пользователям (администраторам).

SF.Audit удовлетворяет следующим функциональным требованиям безопасности:

FDP_SDI.2 Мониторинг целостности хранимых данных и предпринимаемые действия. Данный компонент требует обеспечения целостности хранимых данных аудита.

FPT_AMT.1 Тестирование абстрактной машины. Данный компонент регламентирует возможность выполнения тестовых программ, позволяющий путём анализа данных аудита, генерируемых в результате выполнения тестов, продемонстрировать правильность выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая положена в основу ФБО.

FPT_STM.1 Надежные метки времени. Данный компонент позволяет реализовать хронологически упорядоченное занесение данных аудита в системный журнал.

FPT_TDC.1 Базовая согласованность данных ФБО между ФБО. Данный компонент требует обеспечения возможности согласованной интерпретации информации аудита совместно используемыми ФБО и другими доверенными продуктами ИТ.

FPT_TST.1 Тестирование ФБО. Данный компонент определяет порядок протоколирования результатов самотестирования ФБО.

FMT_MTD.1 Управление данными ФБО. Данный компонент задаёт ограничения на запрос, модификацию и удаление информации аудита.

FAU_GEN.1 Генерация данных аудита. Данный компонент специфицирует события безопасности, потенциально подвергаемые аудиту.

FAU_SAA.1 Анализ потенциального нарушения. Данный компонент определяет правила мониторинга событий, подвергающихся аудиту.

FAU_SAR.1 Просмотр аудита. Данный компонент определяет правила и порядок доступа к информации аудита, а также форму представления данной информации.

FAU_SAR.3 Выборочный просмотр аудита. Данный компонент регламентирует возможность поиска, сортировки и упорядочения данных аудита.

FAU_SEL.1 Избирательный аудита. Данный компонент задаёт критерии включения событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту.

FAU_STG.1 Защищенное хранение журнала аудита. Данный компонент задаёт требования к защите данных аудита от несанкционированного удаления и к механизмам предотвращения их модификации.

FAU_STG.4 Предотвращение потери данных аудита. Данный компонент определяет порядок действий, выполняемых подсистемой протоколирования при переполнении журнала аудита.

6.1.9. Сигнализация (SF.Alert)

ОО имеет возможность уведомления администратора при наступлении определённых событий, связанных с безопасностью. Уведомление осуществляется либо путём занесения соответствующих записей в журнал аудита, либо путём непосредственной индикации через консоль управления.

SF.Alert удовлетворяет следующим функциональным требованиям безопасности:

FDP_SDI.2 Мониторинг целостности хранимых данных и предпринимаемые действия. Данный компонент регламентирует порядок оповещения администратора о событиях, связанных с нарушением целостности.

FIA_AFL.1 Обработка отказов аутентификации. Данный компонент требует формирования сообщения администратору в случае превышения допустимого числа неуспешных попыток аутентификации.

FAU_ARP.1 Сигналы нарушения безопасности. Данный компонент определяет реализуемые механизмы оповещения администратора при обнаружении возможного нарушения безопасности.

6.2. Меры обеспечения доверия безопасности

Согласно ОУД3 применены следующие меры доверия к безопасности ОО:

- **IF.CONF** управление конфигурацией;
- **IF.DEL** формализация процедур поставки и эксплуатации;
- **IF.DOC** предоставление проектной документации;
- **IF.MAN** предоставление руководств;
- **IF.TST** тестирование;
- **IF.VUL** анализ уязвимостей.

6.2.1. Управление конфигурацией (IF.CONF)

Меры управление конфигурацией (УК), предпринимаемые разработчиком, обеспечивают уникальную идентификацию ОО. Маркировка ОО наносится на упаковки, носители, отражается при запуске программы через графический интерфейс пользователя. Система УК поддерживается актуальной документацией.

IF.CONF удовлетворяет следующим требованиям доверия:

ACM_CAP.3 Средства контроля авторизации. Данный компонент задаёт требования к маркировке и документации УК.

ACM_SCP.1 Охват УК объекта оценки. Данный компонент уточняет требования к документации УК.

6.2.2. Формализация процедур поставки и эксплуатации (IF.DEL)

Разработчик устанавливает для ОО строгие правила поставки, установки, генерации и запуска ОО, гарантирующие выполнение сохранение уровня безопасности при выполнении указанных процедур.

IF.DEL удовлетворяет следующим требованиям доверия:

ADO_DEL.1 Процедуры поставки. Данный компонент задаёт требования к формализации процедур поставки ОО.

ADO_IGS.1 Процедуры установки, генерации и запуска. Данный компонент регламентирует порядок документирования процедур, необходимых для безопасной установки, генерации и запуска ОО.

6.2.3. Предоставление проектной документации (IF.DOC)

Проектная документация ОО, представляемая на оценку, включает неформальную функциональную спецификацию и проект верхнего уровня, а также документацию по безопасности разработки. В функциональной спецификации приводится неформальное описание ФБО и их внешних интерфейсов. Проект верхнего уровня включает описание структуры ФБО в терминах подсистем и идентифицирует все базовые программные, программно-аппаратные или аппаратные средства, требуемые для реализации ФБО. Документация по безопасности разработки отражает меры безопасности, необходимые для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.

IF.DOC удовлетворяет следующим требованиям доверия:

ADV_FSP.1 Неформальная функциональная спецификация. Данный компонент предъявляет требования к составу и содержанию неформальной функциональной спецификации.

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня. Данный компонент предъявляет требования к составу и содержанию проекта верхнего уровня.

ADV_RCR.1 Неформальная демонстрация соответствия. Данный компонент детализирует требования к анализу предоставляемой проектной документации.

ALC_DVS.1 Идентификация мер безопасности. Данный компонент определяет состав и содержание документации по безопасности разработки.

6.2.4. Предоставление руководств (IF.MAN)

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

IF.MAN удовлетворяет следующим требованиям доверия:

AGD_ADM.1 Руководство администратора. Данный компонент определяет требования к структуре и содержанию руководства администратора.

AGD_USR.1 Руководство пользователя. Данный компонент определяет требования к составу и содержанию руководства пользователя.

6.2.5. Тестирование (IF.TST)

Тестовая документация ОО описывает стратегию тестирования ФБО, тестовые сценарии, наборы тестов и результаты тестирования, позволяющие провести независимое тестирование ФБО и сделать заключение, выполняются ли ФБО в соответствии с документацией.

IF.TST удовлетворяет следующим требованиям доверия:

ATE_COV.2 Анализ покрытия. Данный компонент требует подтверждения соответствия между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

ATE_DPT.1 Тестирование: проект верхнего уровня. Данный компонент требует демонстрации достаточности тестов, идентифицированных в тестовой документации, для демонстрации того, что ФБО выполняются в соответствии с проектом верхнего уровня.

ATE_FUN.1 Функциональное тестирование. Данный компонент определяет объём и порядок функционального тестирования.

ATE_IND.2 Выборочное независимое тестирование. Данный компонент уточняет порядок подтверждения корректности тестовой документации.

6.2.6. Анализ уязвимостей (IF.VUL)

Анализ уязвимостей включает в себя экспертизу руководств и независимый анализ уязвимостей, в том числе тестирование проникновением. Анализ проводится на этапе оценки, результаты отражаются в ТОО.

IF.VUL удовлетворяет следующим требованиям доверия:

AVA_MSU.1 Экспертиза руководств. Данный компонент определяет требования к руководствам, относящиеся к вопросам безопасной эксплуатации ОО.

AVA_SOF.1 **Оценка стойкости функции безопасности ОО.** Данный компонент определяет порядок анализа стойкости механизмов функций безопасности ОО, для которых имеются утверждения относительно их стойкости.

AVA_VLA.1 Анализ уязвимостей разработчиком. Данный компонент определяет порядок проведения независимого комплексного анализа уязвимостей, проводимого разработчиком и подтверждаемого оценщиком.

7. Утверждение о соответствии профилю защиты

Соответствие данного Задания по безопасности какому-либо профилю защиты не декларируется.

8. Обоснование

8.1. Логическое обоснование целей безопасности

8.1.1. Логическое обоснование целей безопасности для ОО

В таблице 3 приведено отображение целей безопасности для ОО на угрозы и политики безопасности организации.

Таблица 3. ***Отображение целей безопасности для ОО на угрозы и политики безопасности организации***

Цели безопасности для ОО	Угрозы и политики безопасности организации
O.ACCESS	T.ISPOOF T.SSPOOF T.NATTACK T.DCORRUPT T.EVAL P.OWNER P.INT_ROLE P.EXT_ROLE P.MAINTENANCE
O.ADMIN	T.LACCESS T.ISPOOF T.SSPOOF T.DCORRUPT P.OWNER P.INT_ROLE P.ADM_ROLE
O.ACCOUNT	T.LACCESS P.AUTH P.ACCOUNT
O.PROTECT	T.DCORRUPT T.AUTH T.CRASH P.EVAL
O.AUDIT	T.NATTACK T.AUDIT T.DCORRUPT P.AUDIT

O.ACCEESS ***Посредничество в предоставлении доступа***. Данная цель безопасности необходима для противодействия угрозам T.ISPOOF, T.SSPOOF, T.NATTACK, T.DCORRUPT и T.EVAL с учётом политик P.OWNER, P.INT_ROLE, P.EXT_ROLE, P.MAINTENANCE, поскольку она обеспечивает весь комплекс механизмов контроля информационного обмена, разрешая или запрещая прохождение информационных потоков из внутренней информационной среды во внешнюю и из внешней во внутреннюю в соответствии с установленными правилами.

O.ADMIN ***Доступ администратора***. Данная цель безопасности необходима для противодействия угрозам T.LACCESS, T.ISPOOF, T.SSPOOF и T.DCORRUPT с учётом политик P.OWNER, P.INT_ROLE, P.ADM_ROLE, поскольку она определяет порядок

доступа к ОО уполномоченных администраторов в соответствии с установленными правилами.

O.ACCOUNT ***Контроль действий отдельных пользователей***. Данная цель безопасности необходима для противодействия угрозе T.LACCESS с учётом политик P.AUTH и P.ACCOUNT, поскольку она определяет порядок управления доступом на базе механизмов аутентификации.

O.PROTECT ***Самозащита ОО.*** Данная цель безопасности необходима для противодействия угрозам T.DCORRUPT, T.AUTH и T.CRASH с учётом политики P.EVAL, поскольку она определяет механизмы защиты ОО от атак извне.

O.AUDIT ***Аудит***. Данная цель безопасности необходима для противодействия угрозам T.NATTACK, T.AUDIT и T.DCORRUPT с учётом политики P.AUDIT, поскольку она определяет требования к механизмам сбора, накопления и представления информации аудита..

8.1.2. Логическое обоснование целей безопасности для среды

В таблице 4 приведено отображение целей безопасности для среды на предположения безопасности.

Таблица 4. *Отображение целей безопасности для среды на предположения безопасности*

Цели безопасности для среды	Предположения и угрозы
O.INSTALL	A.SINGLEPT A.COMMS A.USER A.ENV_MANAGE T.INSTALL T.OPERATE T.COMMS
O.SECURE	A.SECURE T.INALL
O.TRAIN	A.USER A.ENV_MANAGE A.NOEVIL T.INSHARE
O.SUPPORT	A.ENV_MANAGE A.NOEVIL T.SERVICES

O.INSTALL ***Средства контроля инсталляции и эксплуатации***. Данная цель безопасности необходима в связи с реализацией предположений безопасности A.SINGLEPT, A.COMMS, A.USER и A.ENV_MANAGE, поскольку она обеспечивает комплекс мероприятий, поддерживающих безопасное состояние системы. Цель необходима для противостояния угрозам T.INSTALL, T.OPERATE и T.COMMS.

O.SECURE ***Контроль физического доступа к ОО***. Данная цель безопасности необходима в связи с реализацией предположения безопасности A.SECURE, поскольку она регламентирует контроль физического доступа к ОО. Цель необходима для противостояния угрозе T.INALL.

O.TRAIN ***Обучение.*** Данная цель безопасности необходима в связи с реализацией предположений безопасности A.USER, A.ENV_MANAGE и A.NOEVIL, поскольку она регламентирует вопросы осознанного и квалифицированного администрирования ОО. T.INSHARE.

O.SUPPORT ***Сопровождение***. Данная цель безопасности необходима в связи с реализацией предположений безопасности A.ENV_MANAGE и A.NOEVIL, поскольку она определяет порядок сопровождения установленного ОО. Цель необходима для противостояния угрозе T.SERVICES.

8.2. Логическое обоснование требований безопасности

8.2.1. Логическое обоснование функциональных требований безопасности

В таблице 5 представлено отображение функциональных требований безопасности на цели безопасности для ОО.

Таблица 5. ***Отображение функциональных требований безопасности на цели безопасности для ОО***

Функциональные требования безопасности	Цели безопасности
FDP_ACC.2(1)	O.ACCESS
FDP_ACC.2(2)	O.ACCESS
FDP_ACC.2(3)	O.ACCESS
FDP_ACC.2(4)	O.ACCESS
FDP_ACF.1	O.ACCESS
FDP_IFC.2(1)	O.ACCESS
FDP_IFC.2(2)	O.ACCESS
FDP_IFC.2(3)	O.ACCESS
FDP_IFF.1	O.ACCESS
FDP_ITC.2	O.ACCOUNT
FDP_RIP.2	O.ACCESS
FDP_SDI.2	O.PROTECT O.AUDIT
FIA_AFL.1	O.PROTECT O.ADMIN O.ACCOUNT
FIA_ATD.1	O.ACCESS O.ACCOUNT
FIA_SOS.1	O.ACCESS O.ADMIN O.ACCOUNT
FIA_UAU.1	O.ACCOUNT

Функциональные требования безопасности	Цели безопасности
	O.ACCESS
FIA_UAU.3	O.ACCOUNT O.ACCESS
FIA_UAU.5	O.ACCOUNT O.ADMIN O.ACCESS
FIA_UID.2	O.ACCOUNT O.ADMIN O.ACCESS
FPT_AMT.1	O.PROTECT O.AUDIT
FPT_FLS.1	O.PROTECT
FPT_RCV.1	O.ACCESS O.ADMIN
FPT_RVM.1	O.ACCESS
FPT_SEP.1	O.PROTECT O.ADMIN
FPT_STM.1	O.ACCESS O.AUDIT
FPT_TDC.1	O.ACCESS O.AUDIT
FPT_TST.1	O.PROTECT O.AUDIT
FMT_MSA.1	O.ACCESS O.ADMIN
FMT_MSA.3	O.ACCESS O.ADMIN
FMT_MTD.1	O.ACCESS O.ADMIN O.AUDIT
FMT_SMR.1	O.ACCESS O.ADMIN
FAU_ARP.1	O.ACCESS
FAU_GEN.1	O.AUDIT
FAU_SAA.1	O.AUDIT
FAU_SAR.1	O.AUDIT O.ADMIN
FAU_SAR.3	O.AUDIT
FAU_SEL.1	O.AUDIT
FAU_STG.1	O.AUDIT
FAU_STG.4	O.AUDIT

Функциональные требования безопасности	Цели безопасности
FPR_ANO.1	O.ACCOUNT
FPR_PSE.1	O.ACCOUNT O.ACCESS
FPR_UNL.1	O.ACCOUNT
FTP_ITC.1	O.ACCESS O.ADMIN O.AUDIT

FDP_ACC.2(1), FDP_ACC.2(2), FDP_ACC.2(3), FDP_ACC.2(4) ***Полное управление доступом***. Данные компоненты выбраны для обеспечения базовых определений функций управления доступом ОО. Они непосредственно поддерживают цель безопасности O.ACCESS – посредничество в предоставлении доступа.

FDP_ACF.1 ***Управление доступом, основанное на атрибутах безопасности***. Данный компонент выбран для обеспечения функций управления доступом ОО. Он непосредственно поддерживает цель безопасности O.ACCESS – посредничество в предоставлении доступа.

FDP_IFC.2(1), FDP_IFC.2(2), FDP_IFC.2(3) Полное ***управление информационными потоками***. Данные компоненты выбраны для обеспечения постоянной доступности всех сервисов внешнего информационного обмена, предоставляемых ОО, посредством управления информационными потоками. Они поддерживают цель безопасности O.ACCESS.

FDP_IFF.1 ***Простые атрибуты безопасности***. Информация и субъекты информационного обмена должны иметь атрибуты безопасности, с учетом которых ОО осуществляет функцию управления информационными потоками. Данный компонент специфицирует также основные реализуемые правила и описывает, как вводятся атрибуты безопасности. Он поддерживает цель безопасности O.ACCESS

FDP_ITC.2 ***Импорт данных пользователей с атрибутами безопасности***. Данный компонент выбран для обеспечения возможности импорта пользовательских данных и однозначной ассоциации их с атрибутами безопасности пользователя. Он поддерживает цель безопасности O.ACCOUNT.

FDP_RIP.2 ***Полная защита остаточной информации***. Данный компонент выбран для того, чтобы избежать получения пользователем данных, обрабатываемых ОО, доступ к которым не санкционирован явно. Данный компонент поддерживает цель безопасности O.ACCESS.

FDP_SDI.2 ***Мониторинг целостности хранимых данных и предпринимаемые действия***. Данный компонент выбран для обеспечения контроля целостности программной и информационной частей ОО. Он поддерживает цели безопасности O.PROTECT и O.AUDIT.

FIA_AFL.1 ***Обработка отказов аутентификации***. Данный компонент выбран для реагирования на повторные попытки нападения на ОО, особенно на попытки угадать

идентификаторы и аутентификационные данные. Он непосредственно поддерживает цели безопасности O.PROTECT, а также O.ADMIN и O.ACCOUNT.

FIA_ATD.1 ***Определение атрибутов пользователя***. Данный компонент выбран для того, чтобы установить поддерживаемые ОО для каждого пользователя атрибуты безопасности. Поддерживает цели безопасности O.ACCESS и O.ACCOUNT.

FIA_SOS.1 ***Верификация секретов***. Данный компонент выбран для того, чтобы установить требования к стойкости паролей, используемых для аутентификации пользователя. Поддерживает цели безопасности O.ACCESS, O.ADMIN и O.ACCOUNT.

FIA_UAU.1 ***Выбор момента аутентификации***. Данный компонент выбран для определения необходимости и момента времени аутентификации пользователя в соответствии с политикой безопасности. Поддерживает непосредственно цель безопасности O.ACCOUNT, а также O.ACCESS.

FIA_UAU.3 ***Аутентификация, защищенная от подделок***. Данный компонент выбран для того, чтобы ОО мог обнаружить и предотвратить использование фальсифицированных или несанкционированно скопированных аутентификационных данных пользователем. Поддерживает цели безопасности O.ACCOUNT и O.ACCESS.

FIA_UAU.5 ***Сочетание механизмов аутентификации***. Данный компонент выбран для обеспечения применения пользователями различных механизмов аутентификации в особых случаях. Непосредственно поддерживает цель безопасности O.ACCOUNT, а также O.ADMIN и O.ACCESS.

FIA_UID.2 ***Идентификация до любых действий пользователя***. Данный компонент выбран для определения условий, при которых от пользователей должна требоваться собственная аутентификация до выполнения при посредничестве ОО каких-либо других действий от имени пользователя. Компонент поддерживает цели безопасности O.ACCOUNT, O.ADMIN и O.ACCESS.

FPT_AMT.1 ***Тестирование абстрактной машины***. Данный компонент выбран для поддержки тестирования предположений безопасности базовой абстрактной машины, от которых зависит нормальное функционирование ОО. Тестирование осуществляется посредством периодического запуска тестирующих функций. Компонент поддерживает цели безопасности O.PROTECT и O.AUDIT.

FPT_FLS.1 ***Сбой с сохранением безопасного состояния***. Данный компонент выбран для того, чтобы ОО обеспечивал невозможность доступа к защищаемым ресурсам в случае его сбоя. Он непосредственно поддерживает цель безопасности O.PROTECT.

FPT_RCV.1 ***Ручное восстановление***. Данный компонент выбран для обеспечения автоматического возвращения ОО в штатное состояние в случае определенного сбоя, в соответствии с определенным набором сбоев. Он поддерживает цели безопасности O.ACCESS и O.ADMIN.

FPT_RVM.1 ***Невозможность обхода ПБО***. Данный компонент включен для обеспечения недоступности информационного обмена с внешним информационным пространством в обход ФБО до введения ФБО в действие. Поддерживает цель безопасности O.ACCESS.

FPT_SEP.1 ***Отделение домена ФБО***. Данный компонент включен для обеспечения защиты самого ОО от нападений со стороны субъектов, не являющихся доверенными. Кроме этого данный компонент необходим для ограничения доступа

администратора только к средствам конфигурирования ФБО. Компонент поддерживает цель безопасности O.PROTECT – самозащита ОО и O.ADMIN – доступ администратора.

FPT_STM.1 ***Надежные метки времени***. Данный компонент включен для обеспечения требований по предоставлению надежных меток времени в процессе функционирования ОО. Поддерживает цели безопасности O.ACCESS и O.AUDIT

FPT_TDC.1 ***Базовая согласованность данных ФБО между ФБО***. Данный компонент выбран для обеспечения непротиворечивости данных ФБО, реализованных в ОО, для возможного использования и интерпретации этих данных между ФБО и другими доверенными продуктами. Поддерживает цели безопасности O.ACCESS и O.AUDIT.

FPT_TST.1 ***Тестирование ФБО***. Данный компонент выбран для того, чтобы обеспечить проверку правильности функционирования ФБО, включая верификацию целостности данных ФБО и выполняемого кода ФБО ОО. Поддерживает цели безопасности O.PROTECT и O.AUDIT.

FMT_MSA.1 ***Управление атрибутами безопасности***. Данный компонент включен для того, чтобы допустить ролевое участие пользователей для управления идентифицированными атрибутами безопасности. Принятие роли осуществляется в компоненте FMT_SMR.1. Поддерживает цели безопасности O.ACCESS и O.ADMIN.

FMT_MSA.3 ***Инициализация статических атрибутов***. Данный компонент содержит требования, чтобы ОО предоставлял возможность присвоения атрибутам безопасности значений по умолчанию, а также их замены начальными значениями. Поддерживает цели безопасности O.ACCESS и O.ADMIN.

FMT_MTD.1 ***Управление данными ФБО***. Данный компонент допускает уполномоченных пользователей в соответствии с их ролями к управлению данными ОО. Поддерживает цели безопасности O.ACCESS, O.ADMIN и O.AUDIT.

FMT_SMR.1 ***Роли безопасности***. Данный компонент предназначен для управления назначением различных ролей пользователям. Поддерживает цели безопасности O.ACCESS и O.ADMIN.

FAU_ARP.1 ***Сигналы нарушения безопасности***. Данный компонент включен для того, чтобы определить действия, предпринимаемые ФБО при обнаружении нарушения безопасности. Поддерживает цель безопасности O.ACCESS.

FAU_GEN.1 ***Генерация данных аудита***. Данный компонент выбран для обеспечения конкретных типов регистрируемых событий, а также минимального содержания контрольных записей для ОО. Он непосредственно поддерживает цель безопасности O.AUDIT – аудит.

FAU_SAA.1 ***Анализ потенциального нарушения***. Данный компонент требует наличия в ОО возможности обнаружения проникновения на основе установленного набора правил управления доступом ОО. Он непосредственно поддерживает цель безопасности O.AUDIT – аудит.

FAU_SAR.1 ***Просмотр аудита***. Данный компонент требует наличия средств просмотра журнала аудита и указывает на использование данных аудита только уполномоченным администратором. Он непосредственно поддерживает цель безопасности O.AUDIT – аудит, а также O.ADMIN – доступ администратора.

FAU_SAR.3 ***Выборочный просмотр аудита***. Данный компонент указывает на необходимость наличия ограниченного поиска и сортировки контрольных записей. Это

требование имеет большое значение из-за большого объема контрольных данных. Компонент непосредственно поддерживает цель безопасности O.AUDIT – аудит.

FAU_SEL.1 ***Избирательный аудит***. Данный компонент указывает на необходимость наличия в ОО необходимой избирательности событий аудита безопасности. Данное требование предотвращает разрастание журнала аудита до таких размеров, когда он становится бесполезен. Он непосредственно поддерживает цель безопасности O.AUDIT – аудит.

FAU_STG.1 ***Защищенное хранение журнала аудита***. Данный компонент включен для того, чтобы ОО обеспечивал защиту записей журнала аудита от несанкционированного удаления. Поддерживает цель безопасности O.AUDIT – аудит.

FAU_STG.4 ***Предотвращение потери данных аудита***. Данный компонент определяет действия, обеспечиваемые ОО, в случае переполнения журнала аудита, с целью предотвращения потери данных аудита. Он важен для поддержки цели безопасности O.AUDIT – аудит, в отношении обеспечения относительной полноты контрольных записей.

FPR_ANO.1 ***Анонимность***. Данный компонент необходим для обеспечения того, что пользователь может использовать внешние информационные ресурсы или услуги без раскрытия своих идентификаторов. Поддерживает цель безопасности O.ACCOUNT.

FPR_PSE.1 ***Псевдонимность***. Данный компонент необходим для обеспечения того, что внутренний пользователь может использовать внешние ресурсы без раскрытия своего идентификатора, оставаясь, однако, ответственным за свои действия. Поддерживает цель безопасности O.ACCOUNT, O.ACCESS.

FPR_UNL.1 ***Невозможность ассоциации***. Данный компонент необходим для обеспечения невозможности ассоциации запросов к ресурсам внешнего информационного пространства с тем или иным пользователем внутреннего информационного пространства. Поддерживает цель безопасности O.ACCOUNT.

FTP_ITC.1 ***Доверенный канал передачи между ФБО.*** Данный компонент определяет правила создания доверенного канала между ОО и другими доверенными продуктами ИТ для выполнения операций, критичных по безопасности. Примером такой операции может служить процесс информационного обмена между удаленной консолью администратора и ОО. Поддерживает цель безопасности O.ACCESS, O.ADMIN и O.AUDIT.

8.2.2. Логическое обоснование требований доверия

Требования доверия настоящего ЗБ соответствуют ОУД3, который выбран в целях реализации независимо подтверждаемого умеренного уровня доверия на основе всестороннего исследования ОО и процесса его разработки без существенных затрат на изменение технологии проектирования.

8.2.3. Логическое обоснование зависимостей требований

В таблице 6 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворены в настоящем ЗБ либо включением компонентов, определённых в Части 2 ОК под рубрикой

«Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определённым в Части 2 ОК под рубрикой «Зависимости».

Таким образом, столбец «Зависимости по ОК» таблицы 6 является справочным и содержит компоненты, определённые в Части 2 ОК в описании компонентов требований, приведённых в столбце «Функциональные требования безопасности» таблицы 6, под рубрикой «Зависимости».

Столбец «Удовлетворение зависимостей» таблицы 6 показывает, какие компоненты требований были реально включены в ЗБ для удовлетворения зависимостей компонентов, приведённых в столбце «Функциональные требования безопасности» таблицы 6. Компоненты требований либо совпадают с указанными в столбце «Зависимости по ОК», либо иерархичны по отношению к ним.

Таблица 6. ***Зависимости функциональных требований***

Функциональные требования безопасности	**Зависимости по ОК**	**Удовлетворение зависимостей**
FDP_ACC.2(1)	FDP_ACF.1	FDP_ACF.1
FDP_ACC.2(2)	FDP_ACF.1	FDP_ACF.1
FDP_ACC.2(3)	FDP_ACF.1	FDP_ACF.1
FDP_ACC.2(4)	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2(1) FMT_MSA.3
FDP_IFC.2(1)	FDP_IFF.1	FDP_IFF.1
FDP_IFC.2(2)	FDP_IFF.1	FDP_IFF.1
FDP_IFC.2(3)	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2(1) FMT_MSA.3
FDP_ITC.2	[FDP_ACC.1или FDP_IFC.1] [FTP_ITC.1 или FTP_TRP.1] FPT_TDC.1	FDP_ACC.2(1) FTP_ITC.1 FPT_TDC.1
FDP_RIP.2	Отсутствуют	-
FDP_SDI.2	Отсутствуют	-
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	Отсутствуют	-
FIA_SOS.1	Отсутствуют	-
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.3	Отсутствуют	-
FIA_UAU.5	Отсутствуют	-
FIA_UID.2	Отсутствуют	-
FPT_AMT.1	Отсутствуют	-
FPT_FLS.1	ADV_SPM.1	ADV_SPM.1
FPT_RCV.1	FPT_TST.1 AGD_ADM.1	FPT_TST.1 AGD_ADM.1

Функциональные требования безопасности	**Зависимости по ОК**	**Удовлетворение зависимостей**
	ADV_SPM.1	ADV_SPM.1
FPT_RVM.1	Отсутствуют	-
FPT_SEP.1	Отсутствуют	-
FPT_STM.1	Отсутствуют	-
FPT_TDC.1	Отсутствуют	-
FPT_TST.1	FPT_AMT.1	FPT_AMT.1
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1] FMT_SMR.1	FDP_ACC.2 (1) FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAA.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	FAU_GEN.1 FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FPR_ANO.1	Отсутствуют	-
FPR_PSE.1	Отсутствуют	-
FPR_UNL.1	Отсутствуют	-
FTP_ITC.1	Отсутствуют	-

Зависимость FPT_FLS.1 и FPT_RCV.1 от ADV_SPM.1 не учитывается, поскольку в ЗБ приведено четкое определение безопасного состояния ОО (согласно п. Л.2 и Л.8 Части 3 ОК).

Таким образом, все зависимости включенных в ЗБ требований удовлетворены.

8.3. Логическое обоснование краткой спецификации ОО

8.3.1. Логическое обоснование функций безопасности

Отображение функциональных требований безопасности на функции безопасности приведено в таблице 7.

Таблица 7. ***Отображение функциональных требований безопасности на функции безопасности***

	SF.Administer	SF.Trafcontr	SF.Antispoof	SF.Defrag	SF.NAT	SF.Auth	SF.Filter	SF.Audit	SF.Alert
FDP_ACC.2(1)		X	X	X					
FDP_ACC.2(2)		X	X	X					
FDP_ACC.2(3)		X	X	X					
FDP_ACC.2(4)		X	X	X					
FDP_ACF.1		X	X	X					
FDP_IFC.2(1)		X	X	X			X		
FDP_IFC.2(2)		X	X	X					
FDP_IFC.2(3)		X	X	X					
FDP_IFF.1		X	X	X					
FDP_ITC.2						X			
FDP_RIP.2		X							
FDP_SDI.2								X	X
FIA_AFL.1	X					X			X
FIA_ATD.1		X				X			
FIA_SOS.1	X	X				X			
FIA_UAU.1		X				X			
FIA_UAU.3		X				X			
FIA_UAU.5	X	X				X			
FIA_UID.2	X	X				X			
FPT_AMT.1								X	
FPT_FLS.1		X							
FPT_RCV.1	X	X							
FPT_RVM.1		X							
FPT_SEP.1	X								
FPT_STM.1		X						X	
FPT_TDC.1		X						X	
FPT_TST.1								X	
FMT_MSA.1	X	X							
FMT_MSA.3	X	X							
FMT_MTD.1	X	X						X	
FMT_SMR.1	X	X							
FAU_ARP.1		X							X
FAU_GEN.1								X	
FAU_SAA.1								X	
FAU_SAR.1	X							X	
FAU_SAR.3								X	
FAU_SEL.1								X	
FAU_STG.1								X	
FAU_STG.4								X	
FPR_ANO.1						X			
FPR_PSE.1					X	X			

	SF.Administer	SF.Trafcontr	SF.Antispoof	SF.Defrag	SF.NAT	SF.Auth	SF.Filter	SF.Audit	SF.Alert
FPR_UNL.1					X	X			
FTP_ITC.1	X	X							

Тем самым, сочетание специфицированных для ОО функций безопасности при совместном использовании удовлетворяет функциональным требованиям безопасности ОО.

8.3.2. Логическое обоснование мер доверия

Отображение мер доверия на требования доверия приведено в таблице 8.

Таблица 8. ***Отображение требований доверия на меры доверия***

	IF.CONF	IF.DEL	IF.DOC	IF.MAN	IF.TST	IF.VUL
ACM_CAP.3	X					
ACM_SCP.1	X					
ADO_DEL.1		X				
ADO_IGS.1		X				
ADV_FSP.1			X			
ADV_HLD.2			X			
ADV_RCR.1			X			
AGD_ADM.1				X		
AGD_USR.1				X		
ALC_DVS.1			X			
ATE_COV.2					X	
ATE_DPT.1					X	
ATE_FUN.1					X	
ATE_IND.2					X	
AVA_MSU.1						X
AVA_SOF.1						X
AVA_VLA.1						X

Тем самым, изложенные меры доверия полностью соответствуют требованиям доверия.

8.3.3. Логическое обоснование утверждений о соответствии функций безопасности

Функции безопасности, реализованные с помощью вероятностных или перестановочных механизмов, в ОО отсутствуют.

8.4. Обоснование утверждений о соответствии профилю защиты

Для данного Задания по безопасности соответствие какому-либо Профилю защиты не декларируется.