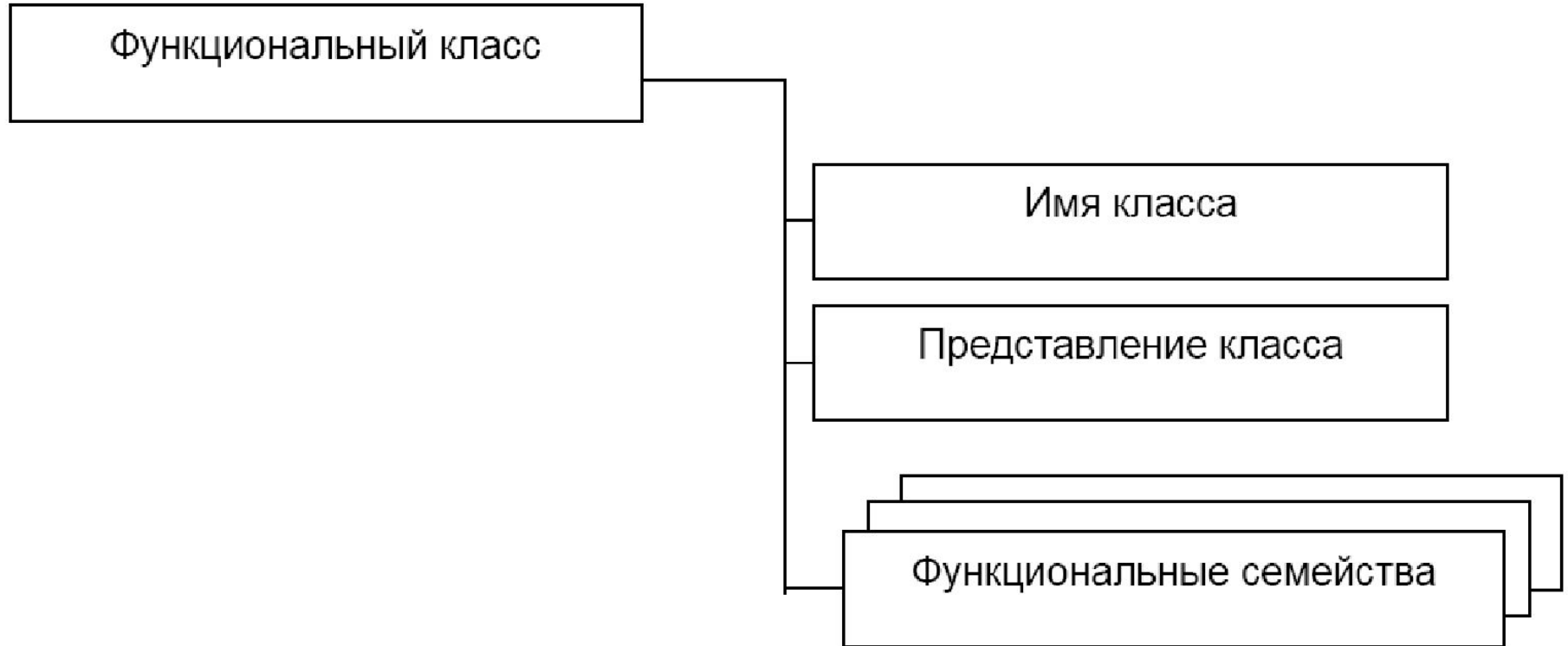
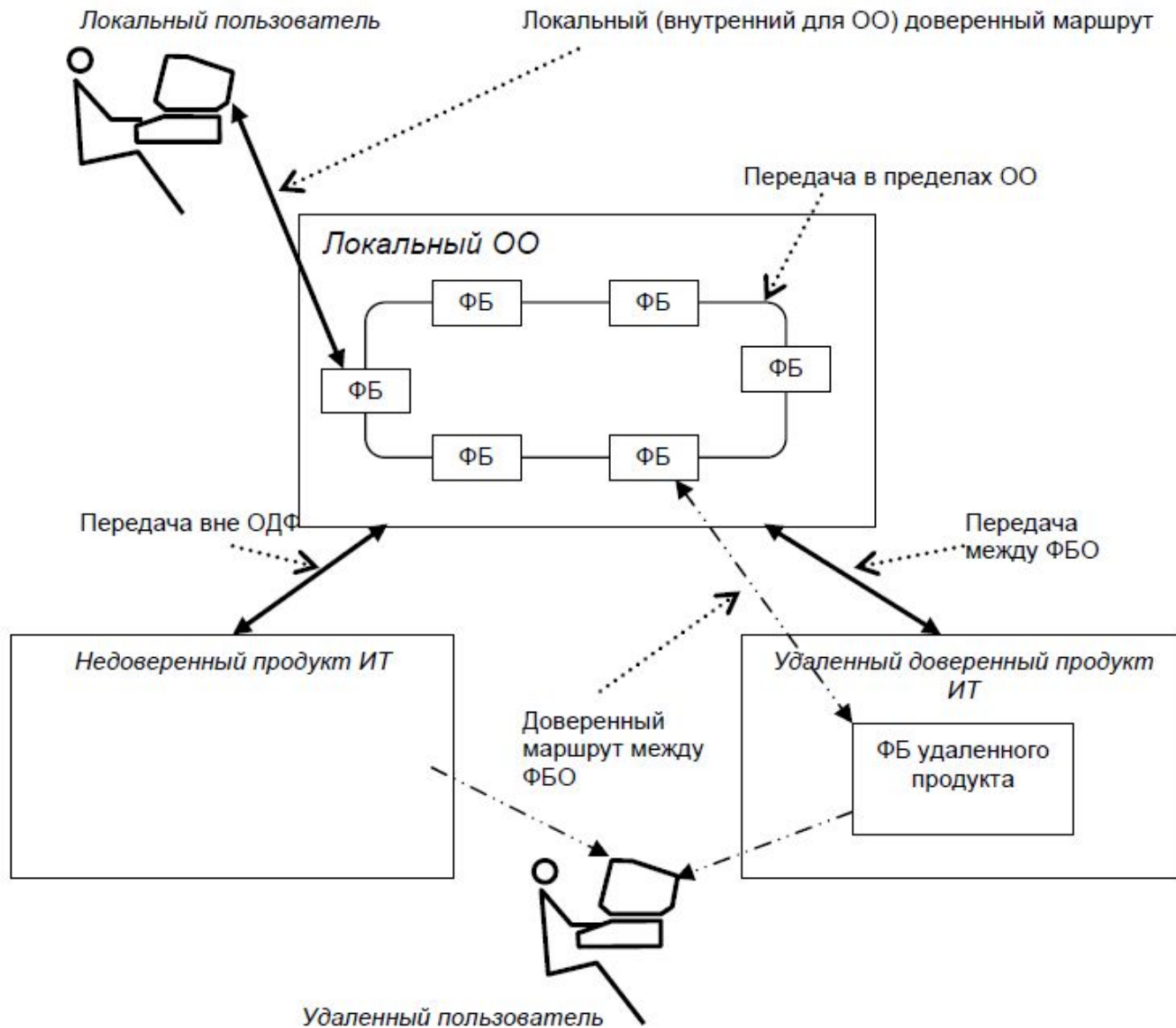


# **ISO/IEC 15408 ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ**

# СТРУКТУРА ФУНКЦИОНАЛЬНОГО КЛАССА



# ФБ В РАСПРЕДЕЛЕННОМ ОО

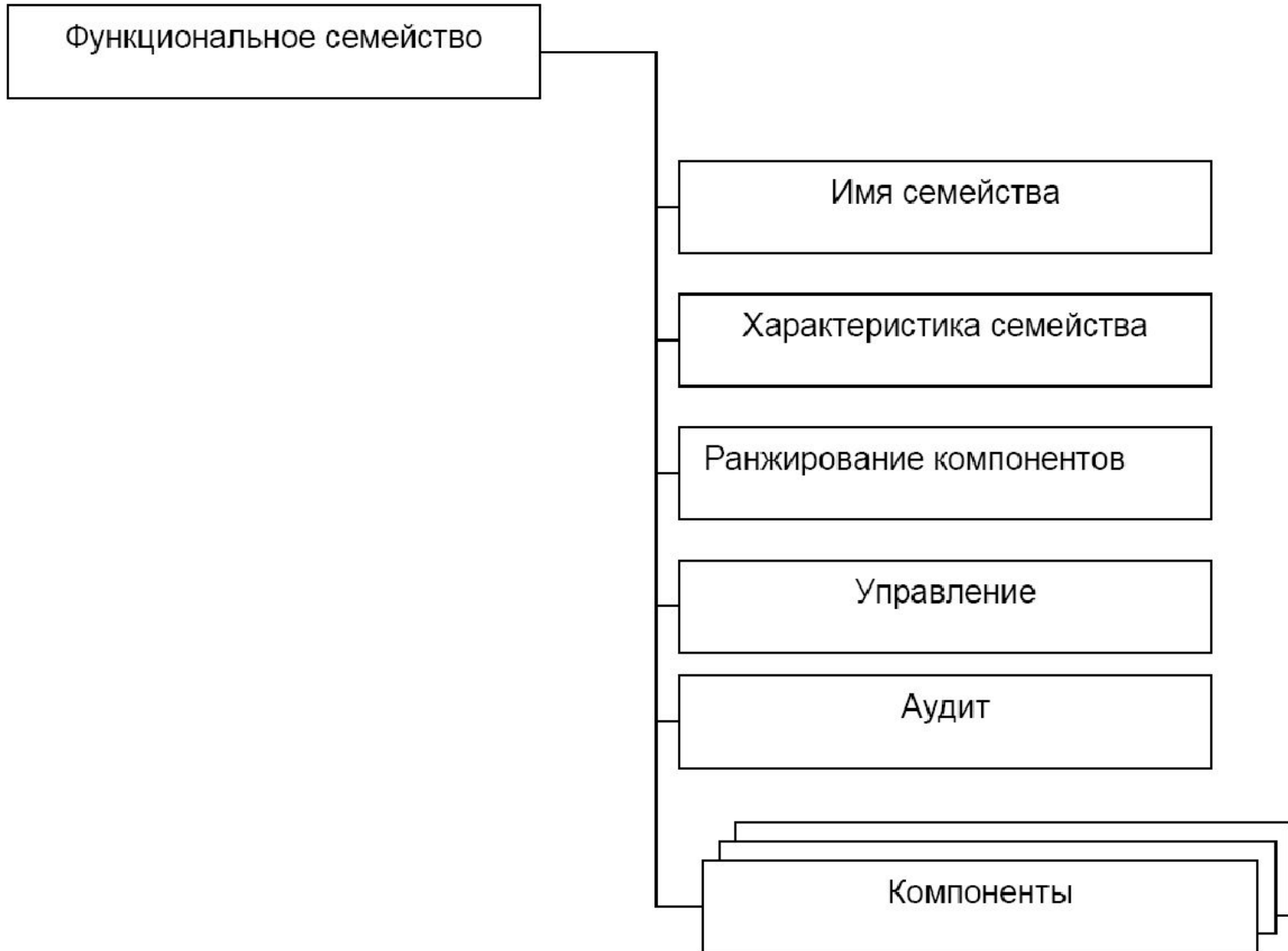


# СТРУКТУРА ФУНКЦИОНАЛЬНОГО КЛАССА

- **Имя класса** - содержит информацию, необходимую для идентификации функционального класса и отнесения его к определенной категории.
- **Представление класса** - представление класса обобщает участие семейств класса в достижении целей безопасности.
- **Структура семейства.**

# СТРУКТУРА ФУНКЦИОНАЛЬНОГО СЕМЕЙСТВА

---

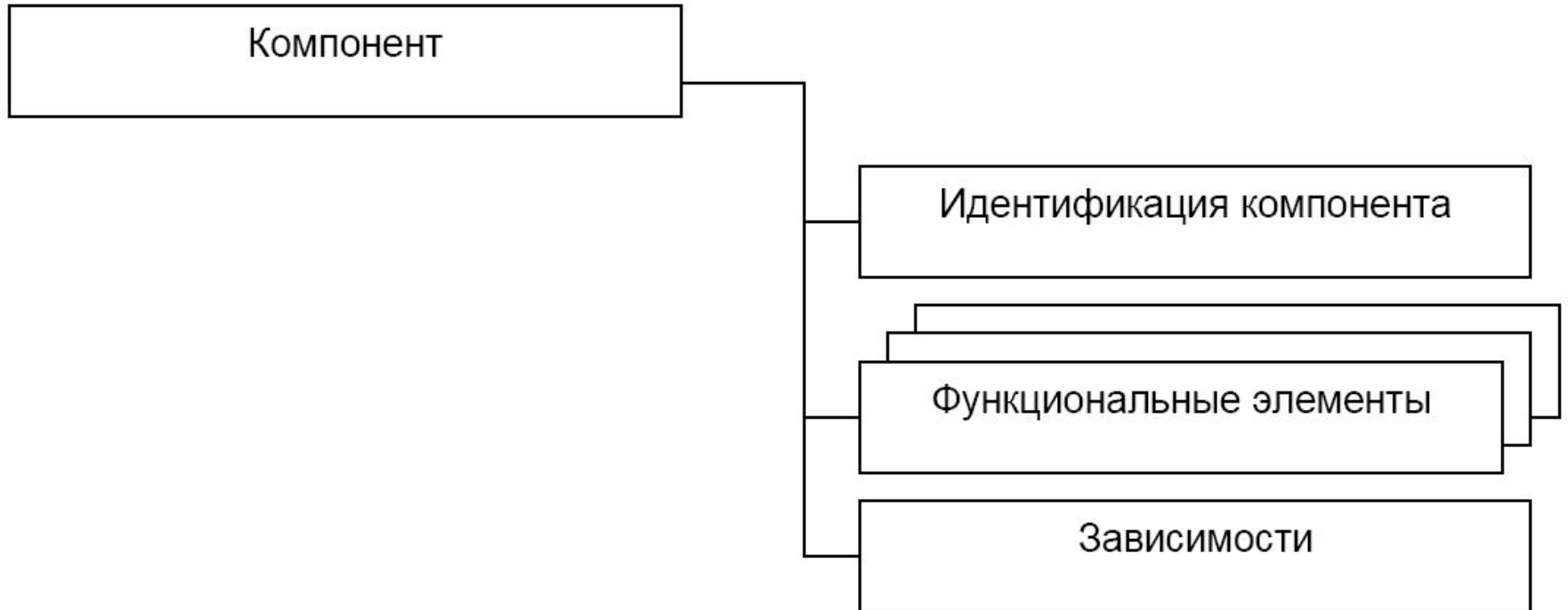


# СТРУКТУРА ФУНКЦИОНАЛЬНОГО СЕМЕЙСТВА

---

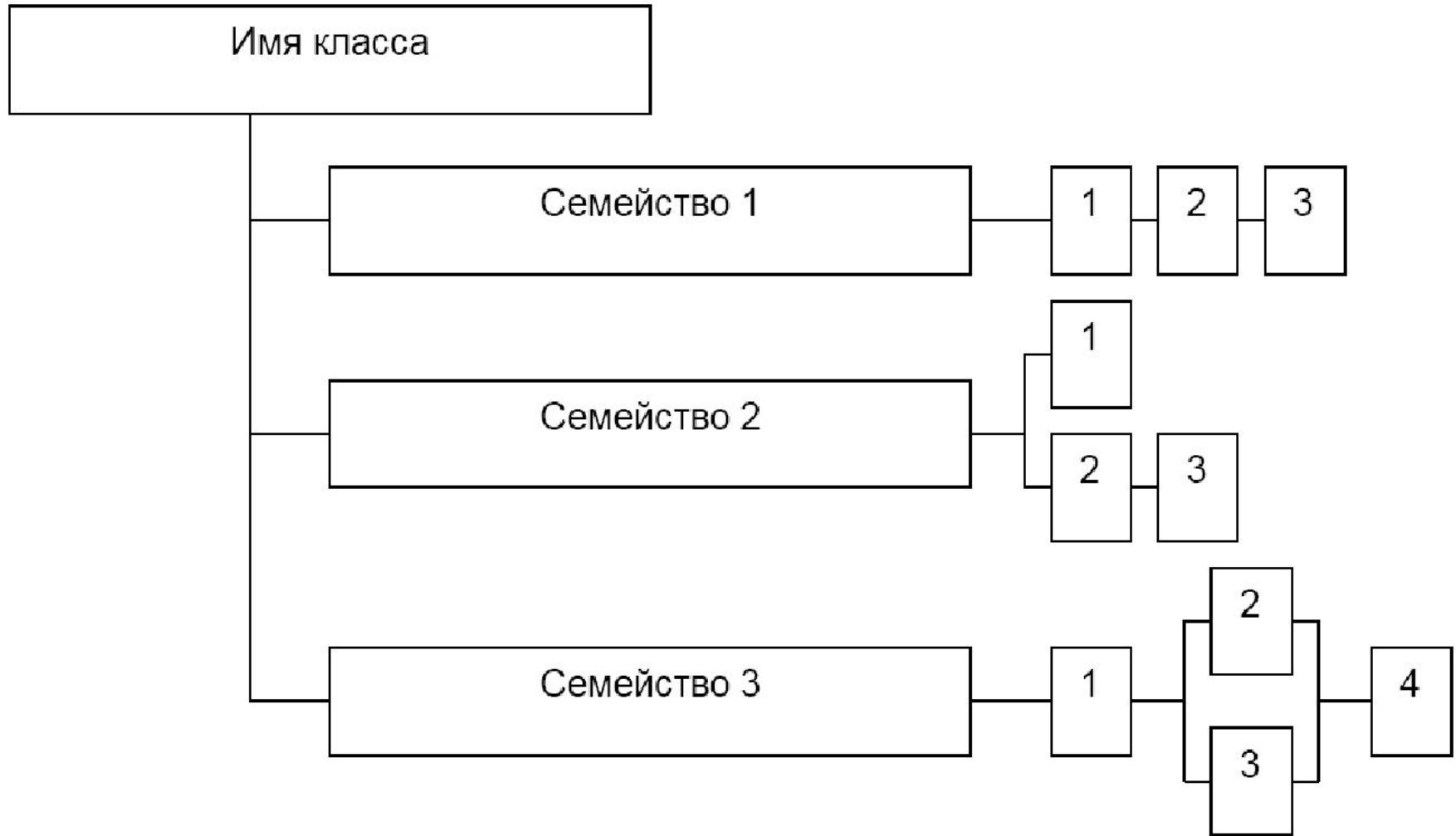
- **Имя семейства** содержит описательную информацию, необходимую, чтобы идентифицировать и категорировать функциональное семейство.
- **Характеристика семейства** – это описание ФС, в котором излагаются его цели безопасности и общее описание функциональных требований.
- **Ранжирование компонентов.** ФС содержат один или несколько компонентов, каждый из которых может быть выбран для включения в ПЗ, ЗБ и функциональные пакеты, а также имеющиеся компоненты и приводится их обоснование.
- **Управление** - содержат информацию для разработчиков ПЗ/ЗБ, учитываемую при определении действий по управлению для данного компонента.
- **Аудит** - содержит события, потенциально подвергаемые аудиту, для их отбора разработчиками ПЗ/ЗБ при условии включения в ПЗ/ЗБ требований из класса FAU «Аудит безопасности».

# СТРУКТУРА ФУНКЦИОНАЛЬНОГО КОМПОНЕНТА



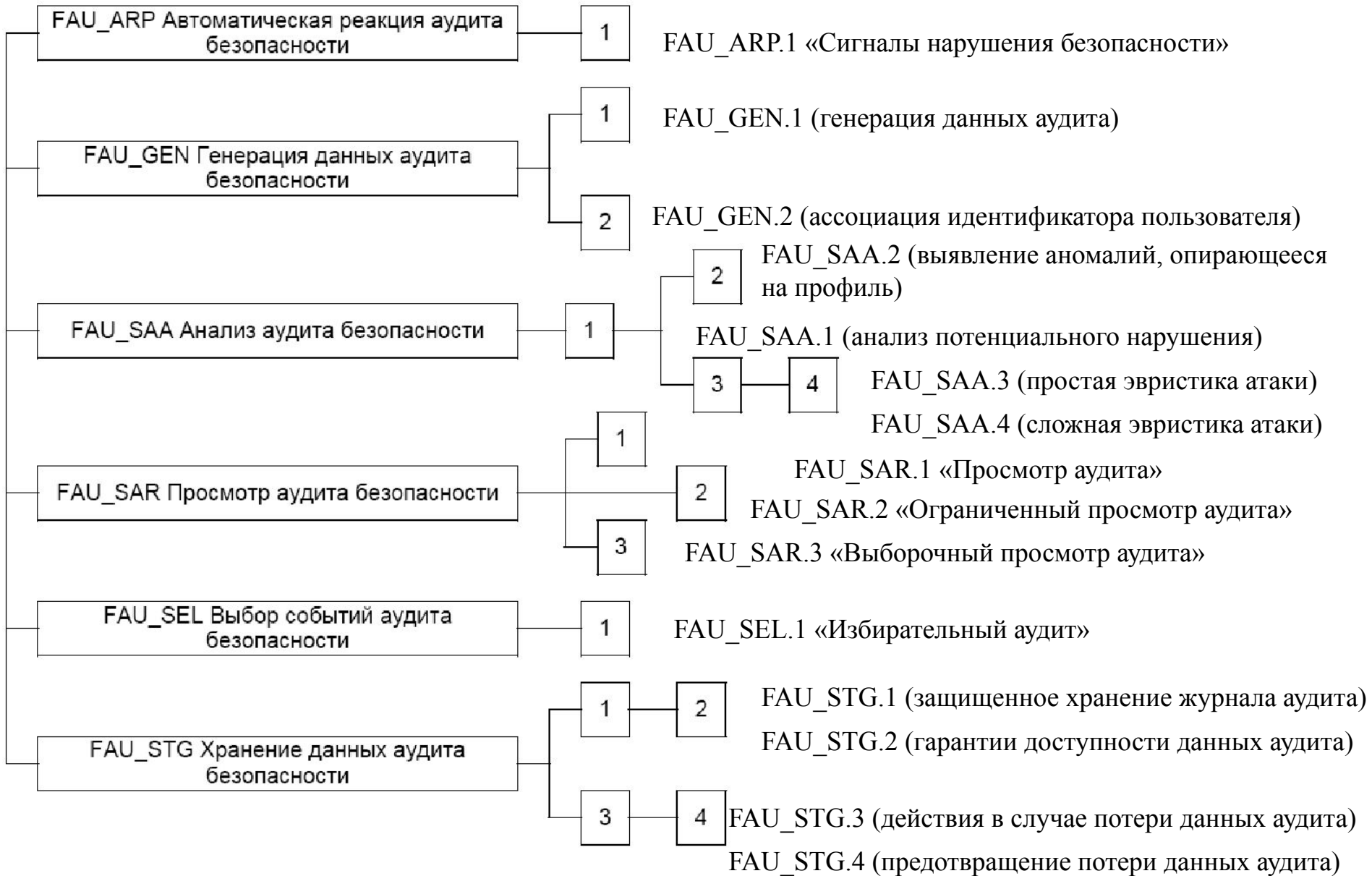
# ПРИМЕР ДЕКОМПОЗИЦИИ КЛАССА

---





# Декомпозиция класса FAU «Аудит безопасности»

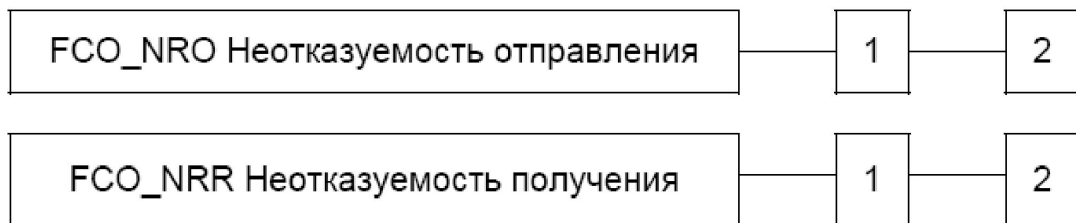


# Декомпозиция класса FCO «Связь»

---

FCO\_NRO.1 «Избирательное доказательство отправления»

FCO\_NRO.2 «Принудительное доказательство отправления»



FCO\_NRR.1 «Избирательное доказательство получения»

FCO\_NRR.2 «Принудительное доказательство получения»

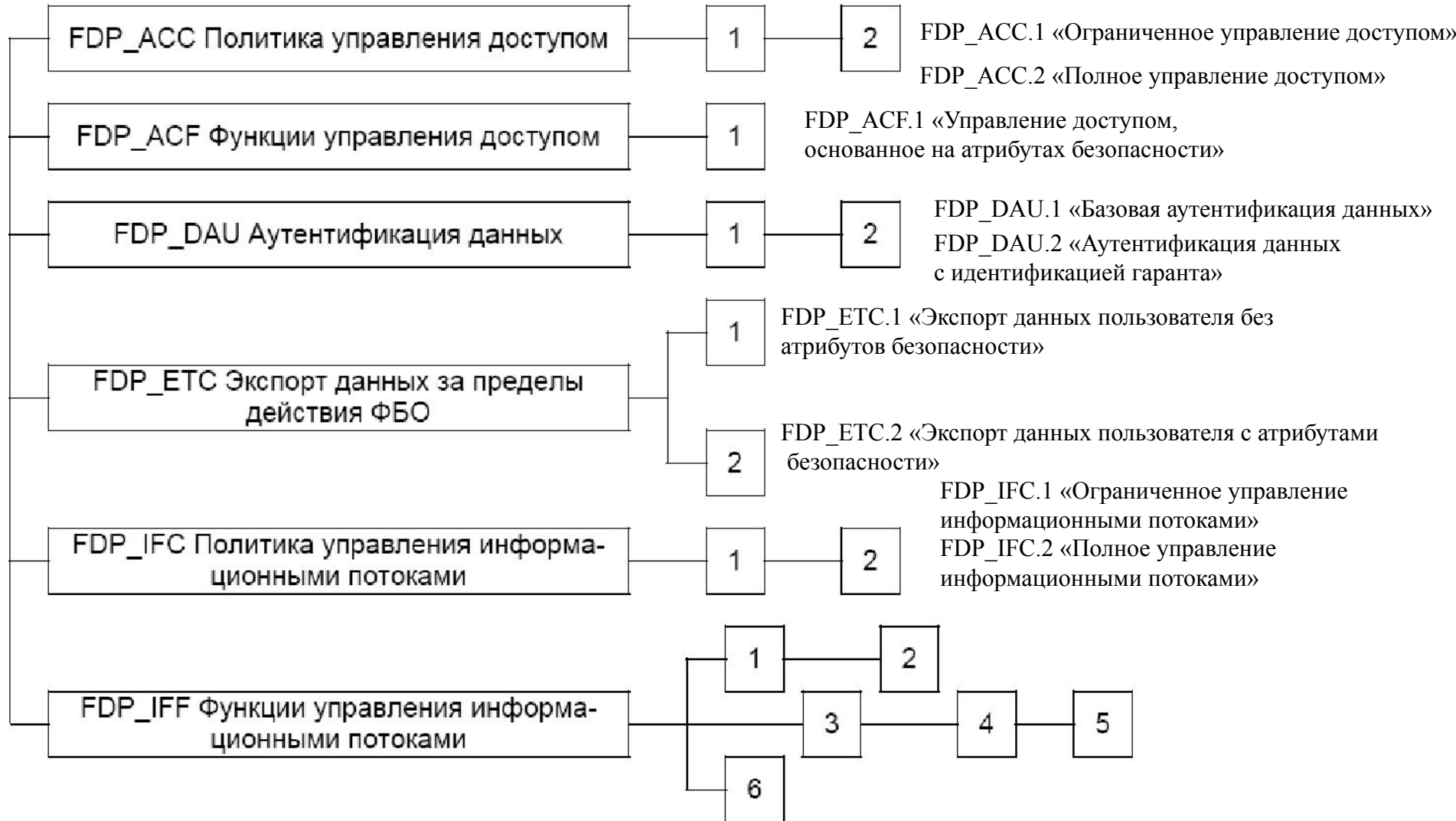
# Декомпозиция класса FCS «Криптографическая поддержка»

---



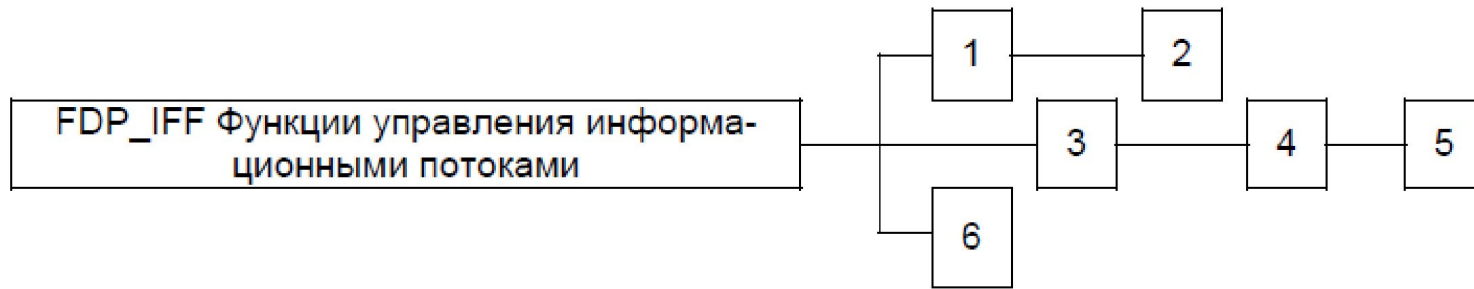
**ПРИМЕР FCS\_COP.1.1 : ФБО должны выполнять [назначение: *список криптографических операций*] в соответствии с определенными алгоритмами [назначение: *криптографические алгоритмы*] и длиной [назначение: *длины криптографических ключей*], которые отвечают следующему: [назначение: *список стандартов*].**

# FDP «Защита данных пользователя»



# FDP «Защита данных пользователя»

---



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

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

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

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

**FDP\_IFF.5 «Полное устранение неразрешенных информационных потоков»** содержит требование, чтобы ПФБ обеспечила устранение всех неразрешенных информационных потоков.

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

# Декомпозиция класса FDP «Защита данных пользователя» (продолжение)



# Декомпозиция класса FIA «Идентификация и аутентификация»



# ПРИМЕР. ОПИСАНИЕ FIA\_UAU.1

---

**FIA\_UAU.1** Выбор момента аутентификации

**Иерархический для:** Нет подчиненных компонентов.

**Зависимости:** FIA\_UID.1 Выбор момента идентификации

## **FIA\_UAU.1.1**

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

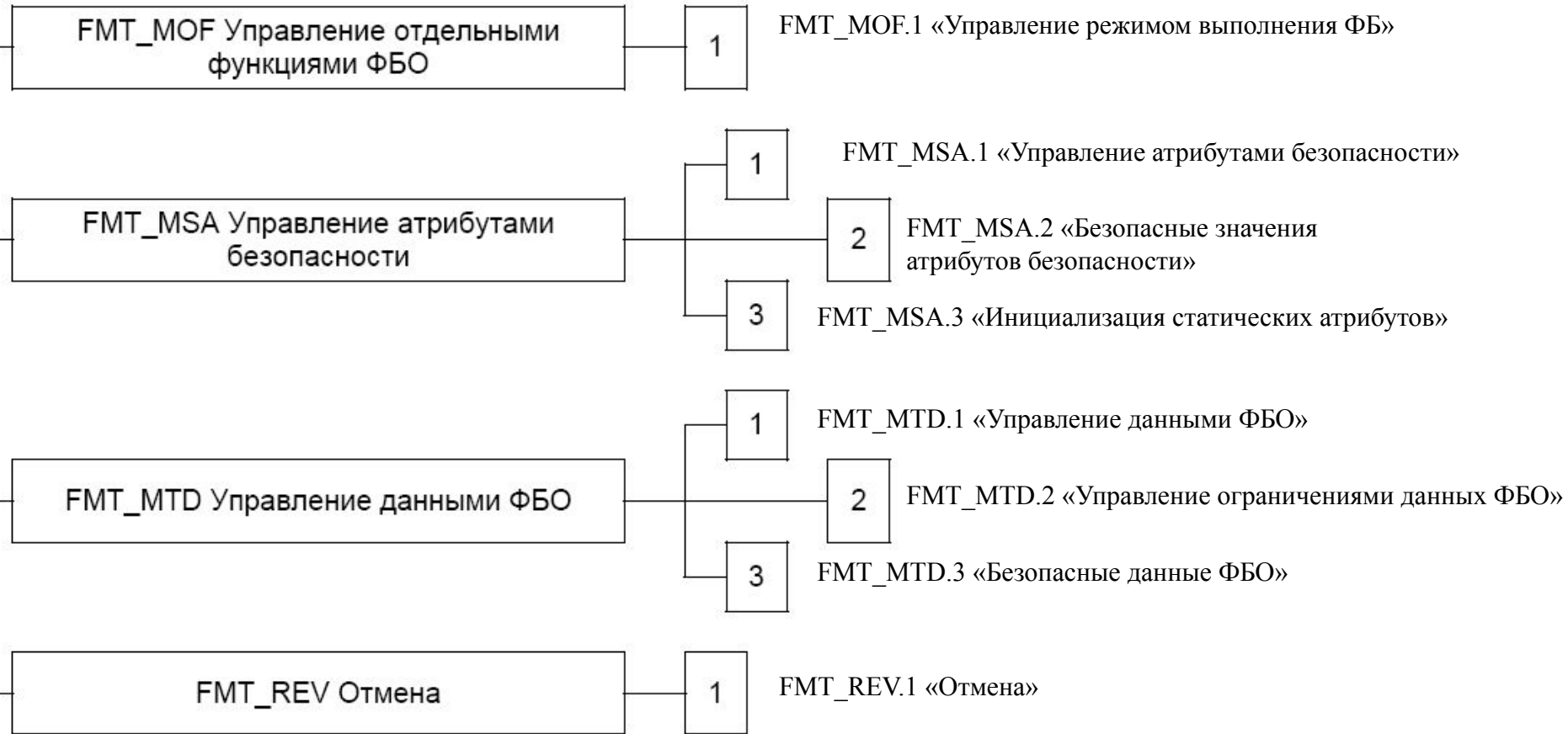
## **FIA\_UAU.1.2**

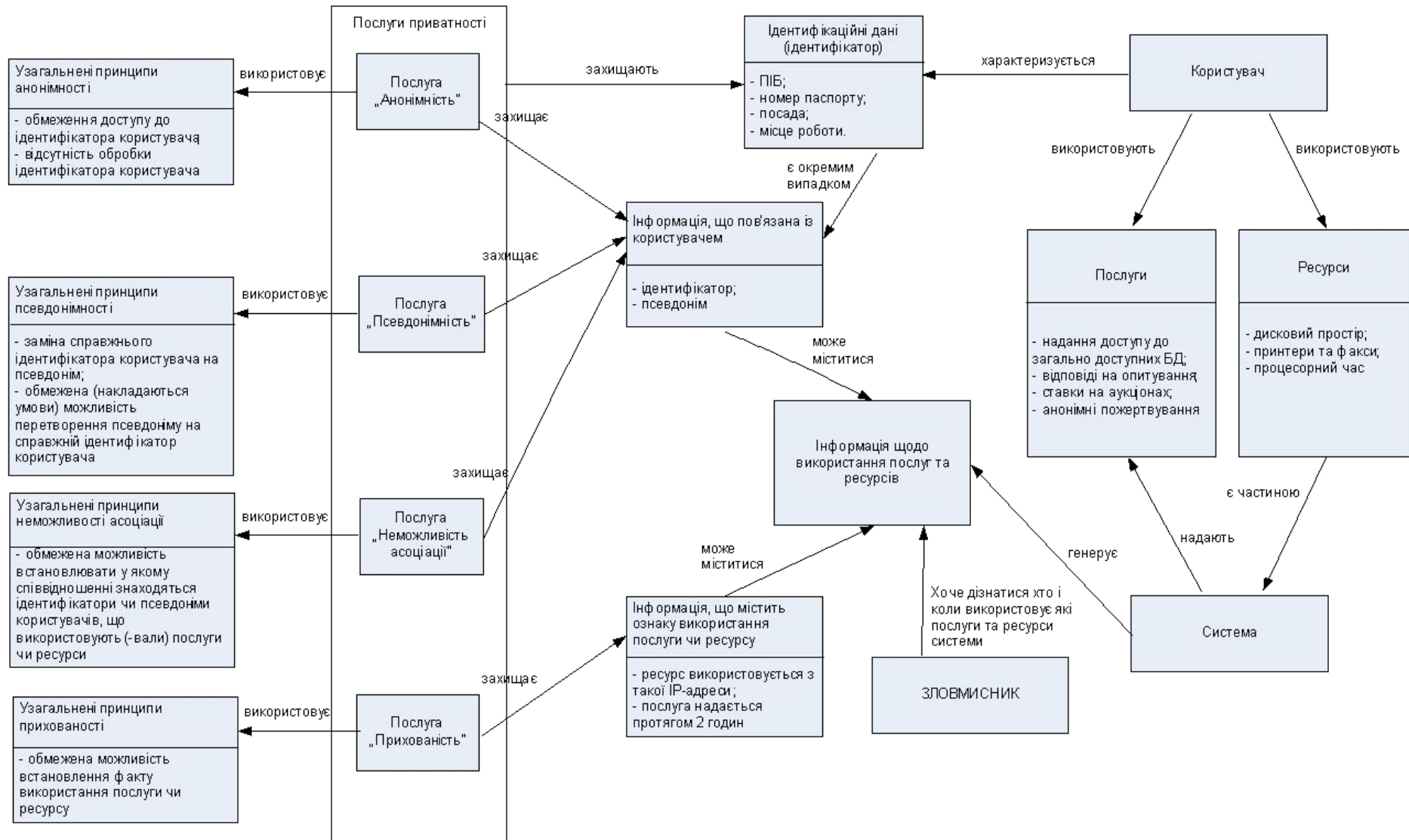
ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого другого действия, выполняемого при посредничестве ФБО от имени этого пользователя.



# Декомпозиция класса FMT «Управление безопасностью»

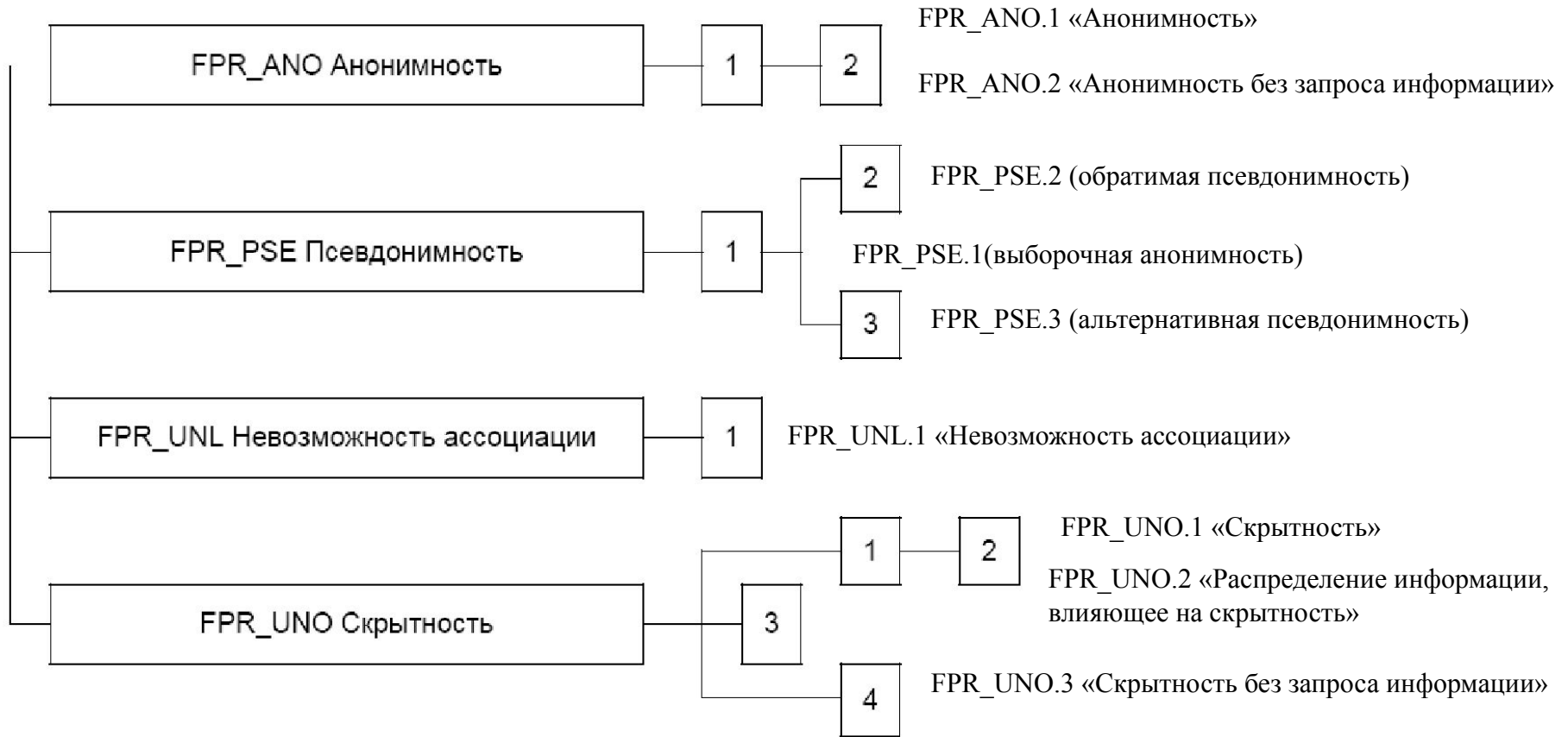
---





# Декомпозиция класса FPR «Приватность»

---



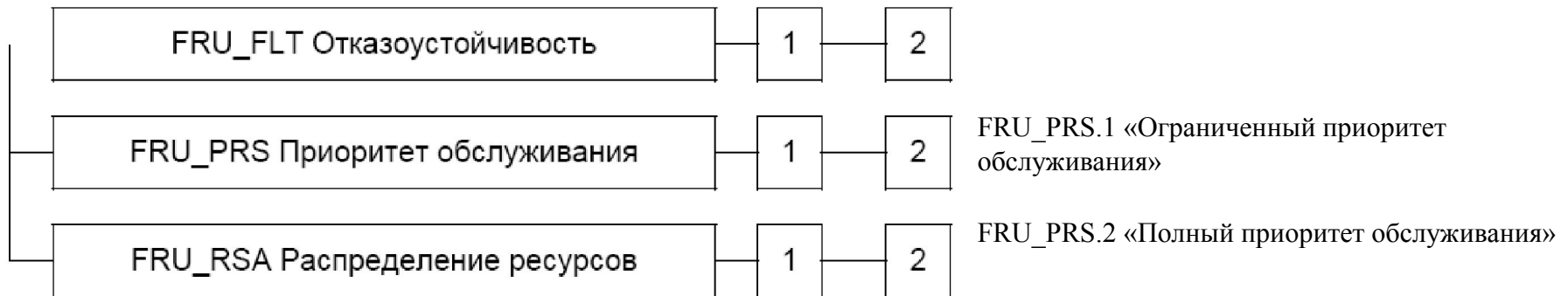
FPR\_UNO.4 (открытость для уполномоченного пользователя)

# Декомпозиция класса FRU «Использование ресурсов»

---

FRU\_FLT.1 «Пониженная отказоустойчивость»

FRU\_FLT.2 «Ограниченная отказоустойчивость»



FRU\_RSA.1 «Максимальные квоты»

FRU\_RSA.2 «Минимальные и максимальные квоты»

# Декомпозиция класса FPT «Защита ФБО»



# ПРИКЛАДИ ДЖЕРЕЛ ЗАГРОЗ

Ідентифікатор джерела загрози	Повна назва джерела загрози
Admin	Системний адміністратор
Hacker	Хакер
Physical_Environment	Фізичне середовище
System_Developer	Розробник системи
User	Авторизований користувач

# ПРИКЛАД ВІДОБРАЖЕННЯ КАТЕГОРІЙ ЗАГРОЗ/ЗАГАЛЬНИХ ЗАГРОЗ БЕЗПЕКИ

<b>Ідентифікатор категорії загрози</b>	<b>Ідентифікатор загальної загрози</b>	<b>Повна назва загальної загрози</b>
<b>Hacker</b>	<b>Hack_Comm_Eavesdrop</b>	<b>Хакер прослуховує дані, що передаються каналами зв'язку</b>
<b>Hacker</b>	<b>Hack_Crypto</b>	<b>Здійснення криптоаналізу або крадіжки інформації</b>
<b>Hacker</b>	<b>Hack_Masq</b>	<b>Хакер маскується під легітимного користувача або системний процес</b>
<b>Hacker</b>	<b>Hack_Msg_Data</b>	<b>Модифікації змісту повідомлення</b>
<b>Hacker</b>	<b>Hack_Phys</b>	<b>Використання вразливостей у фізичному середовищі системи</b>
<b>Hacker</b>	<b>Hack_Social_Engineer</b>	<b>Соціальний інжиніринг</b>
<b>Hacker</b>	<b>Malicious_Code</b>	<b>Виконання шкідливого програмного коду</b>

# Приклад відображення загальних загроз безпеки/деталізована атака

Ідентифікатор загальної загрози	Ідентифікатор деталізованої атаки	Повна назва деталізованої атаки
Hack_Comm_Eavesdror	Hack_CommEaves_Intrc	Аутсайдер перехоплює дані користувача
Hack_Crypto	Hack_Crypto_ChsnCy	Криптоаналіз за обраним закритим текстом
Hack_Crypto	Hack_Crypto_ChsnPln	Криптоаналіз за обраним відкритим текстом
Hack_Crypto	Hack_Crypto_ChsnTxt	Криптоаналіз за обраним текстом
Hack_Masq	Hack_Masq_Hijack	Хакер отримує ідентифікатор авторизованого користувача
Hack_Masq	Hack_Masq_Uwkstn	Користувач отримує ідентифікатор авторизованого користувача
Hack_Masq	Hack_Masq_Wauth	Атака типу «маскарад» як наслідок слабкості механізмів автентифікації
Hack_Msg_Data	Hack_MsgData_RcvTSF	Модифікації критичних з точки зору безпеки даних під час передачі від віддаленого довіреного вузла
Hack_Msg_Data	Hack_MsgData_RcvUsr	Модифікація даних користувача при передачі віддаленого довіреного вузла
Hack_Social_Engineer	Hack_SocEng_Password	Соціальний інжиніринг з метою крадіжки паролів
Hack_Social_Engineer	Hack_SocEng_SysInfo	Хакер використовує методи соціального інжинірингу для отримання інформацію про систему – предмет атаки



Ідентифікатор деталізованої атаки	Ідентифікатор цілі безпеки	Повна назва цілі безпеки
Hack Crypto ChsnCy (Криптоаналіз за обраним закритим текстом)	Encryption_Access	Захист шифрованого тексту
	Encryption_Prohibit	Захист пар відкритий/шифрований текст
	Robust_Encryption	Сильна криптографія
.....		
Hack_Masq_Hijack (Хакер отримує ідентифікатор авторизованого користувача)	Audit_Gen_User	Індивідуальна відповідальність
	Trusted_Path	Надання достовірного шляху
Hack_Masq_Uwkstn (Користувач отримує ідентифікатор авторизованого користувача)	Audit_Gen_User	Індивідуальна відповідальність
	Screen_Lock	Блокування екрану користувача
	Session_Termination	Розривання сесії у випадку неактивності користувача
	Trusted_Path	Надання достовірного шляху
	User_Guidance	Документація користувача
Hack_SocEng_Password (Соціальний інжиніринг з метою крадіжки паролів)	Limit_Mult_Sessions	Обмеження кількості користувальницьких сесій
	User_Auth_Enhanced	Надійна автентифікація користувачів
Hack_SocEng_SysInfo (Хакер використовує методи соціального інжинірингу для отримання інформацію про систему – предмет атаки)	Admin_Guidance	Документація адміністратора
	Audit_Unusual_User	Запис до журналів аудиту незвичайних дій користувачів
	Identify_Unusual_Act	Викриття незвичайних дій користувачів
	User_Guidance	Документація користувача

# Приклад відображення ціль безпеки/ вимога з ISO/IEC 15408

Ідентифікатор ціль безпеки	Ідентифікатор вимоги	Повна назва вимоги
Admin_Guidance (Документація адміністратора)	AGD_ADM.1	Руководство пользователя
Audit_Gen_User (Індивідуальна відповідальність)	FAU_GEN.2	Ассоциация идентификатора пользователя
	FIA_UID.1	Выбор момента идентификации
Audit_Unusual_User (Запис до журналів аудиту незвичайних дій користувачів)	FAU_GEN.1	Генерация данных аудита
	FAU_SAA.2	Выявление аномалии, основанное на профиле
Encryption_Access (Захист шифрованого тексту)	FDP_ACC.1	Ограниченное управление доступом
	FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
	FDP_ETC.2	Экспорт данных пользователя с атрибутами безопасности
Encryption_Prohibit (Захист пар відкритий/шифрований текст)	FCS_COP.1	Криптографические операции
	FDP_IFC.1	Ограниченное управление информационными потоками
	FDP_IFF.1	Простые атрибуты безопасности
Identify_Unusual_Act (Викриття незвичайних дій користувачів)	FTA_TSE.1	Открытие сеанса с ОО

Ідентифікатор цілі безпеки	Ідентифікатор вимоги	Повна назва вимоги
Limit_Mult_Sessions (Обмеження кількості користувальницьких сесій)	FTA_MCS.1	Базовое ограничение на параллельные сеансы
	FTA_MCS.2	Ограничение на параллельные сеансы по атрибутам пользователя
Robust_Encryption (Сильна криптографія)	FCS_CKM.1	Генерация криптографических ключей
	FCS_CKM.2	Распределение криптографических ключей
	FCS_CKM.3	Доступ к криптографическим ключам
	FCS_COP.1	Криптографические операции
Screen_Lock (Блокування екрану користувача)	FTA_SSL.1	Блокирование сеанса, инициированное ФБО
	FTA_SSL.2	Блокирование, инициированное пользователем
Session_Termination (Розривання сесії у випадку неактивності користувача)	FTA_SSL.3	Завершение, инициированное ФБО
Trusted_Path (Надання достовірного шляху)	FTP_TRP.1	Доверенный маршрут
User_Auth_Enhanced (Надійна автентифікація користувачів)	FIA_UAU.3	Аутентификация, защищенная от подделок
	FIA_UAU.4	Механизмы одноразовой аутентификации
User_Guidance (Документація користувача)	AGD_USR.1	Руководство пользователя

# КОМПОНЕНТ FAU\_GEN.1

## FAU\_GEN.1 Генерация данных аудита

### FAU\_GEN.1.1

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

- a) запуск и завершение выполнения функций аудита;
- b) все события, потенциально подвергаемые аудиту, на [выбор (выбрать одно из): *минимальный, базовый, детализированный, неопределенный*] уровне аудита;
- c) [назначение: *другие специально определенные события, потенциально подвергаемые аудиту*].

### FAU\_GEN.1.2

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

- a) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);
- b) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ПЗ/ЗБ, [назначение: *другая относящаяся к аудиту информация*].

# Пример определения услуги из ЗБ на MICROSOFT SQL SERVER 2005

## **FAU\_GEN.1 Генерация данных аудита**

### **FAU\_GEN.1.1**

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

- а) запуск и завершение выполнения функций аудита;
- б) все события, потенциально подвергаемые аудиту, на *неопределенном* уровне аудита;
- в) **(события, приведенные во втором столбце таблицы 5.2).**

### **FAU\_GEN.1.2**

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

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

# СОБЫТИЯ, ПОДЛЕЖАЩИЕ АУДИТУ

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во время сбора данных аудита	
FAU_STG.3	Предпринимаемые действия после превышения порога заполнения журнала аудита	
FAU_STG.4	Факт останова ОО при отсутствии свободного дискового пространства для создания журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на именованном объекте, на который распространяется политика дискреционного управления доступом	Идентификатор объекта
FIA_AFL.1 (1)	Достижение ограничения неуспешных попыток аутентификации и предпринятые действия	
FIA_UAU.2 (1)	Все случаи использования механизма аутентификации субъектов доступа	

# КОМПОНЕНТ FIA\_ATD.1

## **FIA\_ATD.1 Определение атрибутов пользователя**

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

### **Пример определения услуги из Задания по безопасности на MICROSOFT SQL SERVER 2005**

## **FIA\_ATD.1 Определение атрибутов пользователя**

FIA\_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

- [
- а) идентификатор регистрационной записи пользователя;
  - б) идентификатор роли, участником которой является пользователь;
  - в) идентификатор учетной записи пользователя
- ].

# КОМПОНЕНТ FMT\_SMR.1

## FMT\_SMR.1.1

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

## FMT\_SMR.1.2

ФБО должны быть способны ассоциировать пользователей с ролями.

### Пример определения услуги из

### Задания по безопасности на MICROSOFT SQL SERVER 2005

#### FMT\_SMR.1 Роли безопасности

FMT\_SMR.1.1 ФБО должны поддерживать следующие роли:

[

а) администратор ОО;

б) пользователь ОО

].

FMT\_SMR.1.2 ФБО должны быть способны ассоциировать **субъектов доступа** с ролями.



# КОМПОНЕНТ FRU\_FLT.2

## FRU\_FLT.2 Ограниченная отказоустойчивость

### FRU\_FLT.2.1

ФБО должны обеспечить выполнение **всех возможностей ОО**, когда происходят следующие сбои: [назначение: *список типов сбоев*].

## Пример определения услуги из

### Задания по безопасности на MICROSOFT SERVER 2008

## FRU\_FLT.2 Ограниченная отказоустойчивость

FRU\_FLT.2.1 ФБО должны обеспечить выполнение **всех возможностей ОО**, когда происходят следующие сбои:

[

- а) отключение электропитания на активном узле ОО;
- б) потеря взаимодействия между узлами ОО;
- в) возникновение аппаратного сбоя на узле ОО

].

# КОМПОНЕНТ FDP\_ACF.1 (ЧАСТЬ)

## FDP\_ACF.1 Управление доступом, основанное на атрибутах безопасности

### FDP\_ACF.1.1

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

### FDP\_ACF.1.2

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

# Пример определения услуги из ЗБ на MICROSOFT SERVER 2008

FDP\_ACF.1 Управление доступом, основанное на атрибутах безопасности

FDP\_ACF.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] к объектам, основываясь на

[

а) ассоциированных с субъектом идентификаторе пользователя, принадлежности к группе (группам) и привилегиях субъекта;

б) следующих, ассоциированных с объектом, атрибутах управления доступом:

[

– владелец объекта;

– список дискреционного управления доступом (DACL), который может отсутствовать, быть пустым либо содержать одну или более записей; каждая запись в DACL содержит:

– тип (разрешение или запрет);

– идентификатор пользователя или группы;

– право доступа к объекту;

]

].

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

[

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

а) запись, содержащаяся в DACL, явно разрешает доступ пользователю, и доступ не был запрещен предыдущей записью, содержащейся в DACL;

б) запись, содержащаяся в DACL, явно разрешает доступ группе, членом которой является субъект, и доступ не был запрещен предыдущей записью, содержащейся в DACL;

в) список DACL отсутствует;

г) субъект является владельцем объекта и может просматривать или модифицировать список DACL, или субъект является владельцем и может создавать объект

].