Донской государственный технический университет
Кафедра «Кибербезопасность информационных систем»

Учебная дисциплина:

Модели безопасности компьютерных систем

Группы ВКБ 51 и ВКБ 52
Лектор: Черкесова Л.В.

Содержание

Содержание

Квалификационная характеристика выпускника специалитета:

Область науки и техники, охватывающая совокупность проблем, связанных с построением и доказательным анализом качества защищенных компьютерных систем

Объекты проф. деятельнрости – защищенные компьютерные системы и средства обработки, хранения и передачи информации; службы защиты информации; математические модели процессов, возникающих при защите информации

Виды профессиональной деятельности:

производственно-технологическая;

организационно-управленческая;

экспериментально-исследовательская:

разработка и исследование специальных технических и программно-аппаратных средств защиты информации в КС;

разработка математических моделей безопасности КС;

подбор, изучение и обобщение н/т литературы, нормативных и методических документов по программно-аппаратным средствам и способам обеспечения ИБ КС

составление информационных обзоров по вопросам компьютерной безопасности

изучение и анализ информационной безопасности современных информационных технологий

Связь с другими дисциплинами

ОПД.Ф.01 «Аппаратные средства вычислительной техники»
ОПД.Ф.02 «Методы программирования»
ОПД.Ф.03 «Языки программирования»
ОПД.Ф.04 «Операционные системы»
ОПД.Ф.05 «Вычислительные сети»
ОПД.Ф.06 «Системы управления базами данных»
ОПД.Ф.07 «Электроника и системотехника»
ОПД.Ф.08 «Системы и сети передачи информации»
ОПД.Ф.09 «Основы информационной безопасности»
ОПД.Ф.10 «Теоретические основы компьютерной безопасности»
ОПД.Ф.11 «Организационно-правовое обеспечение информационной безопасности»
ОПД.Ф.12 «Технические средства и методы защиты информации»
ОПД.Ф.13 «Криптографические методы защиты информации»
ОПД.Ф.14 «Программно-аппаратные средства обеспечения информационной безопасности»
- Защита программ и данных
- Защита в операционных системах
- Защита в сетях
- Защита в СУБД

ОПД.Ф.15 «Основы управленческой деятельности»
ОПД.Ф.16 «Безопасность жизнедеятельности»

1. Исходные положения теории компьютерной безопасности

1.1. **Содержание и основные понятия компьютерной безопасности** (*история ТКБ, основные направления обеспечения КБ, информация как объект защиты, конфиденциальность, целостность и доступность информации*)

1.2. **Угрозы безопасности в КС** (*классификация и аксонометрия угроз безопасности информации в КС, оценивание угроз*)

1.3. **Политика и модели безопасности в КС** (*монитор безопасности и основные типы политик безопасности в КС, изолированная программная среда*)

2. Модели безопасности компьютерных систем

2.1. **Модели разграничения доступа** (*дискреционные модели - модели на основе матрицы доступа; модели распространения прав доступа - модель Харрисона-Руззо-Ульмана, теоретико-графовая модель TAKE-GRANT; мандатные модели – модель Белла-ЛаПадуллы и ее расширения, модель тематического разграничения доступа на основе иерархических рубрикаторов; теоретико-информационные модели – модель информационного невмешательства, модель информационной невыводимости, модели ролевого доступа*)

2.2. **Модели и технологии обеспечения целостности компьютерной информации** (*субъектно-объектные модели – дискреционная модель Биба, мандатная модель Кларка-Вильсона; технологии ЭЦП, технологии обеспечения целостности мониторами транзакций в клиент-серверных СУБД*)

2.3. **Модели и механизмы обеспечения правомерной доступности (сохранности) компьютерной информации** (*резервирование и журнализация данных, модели и технологии репликации данных*)

2.4. **Модели безопасности распределенных КС** (*модель Варахараджана, зональная модель безопасности*)

3. Методы, анализа и оценки защищенности компьютерных систем

3.1. **Методы, критерии и шкалы оценки защищенности *КС*** (*порядковые, ранговые, интервальные шкалы измерений; содержание объекта оценки и способы оценки*)

3.3. **Теоретико-графовые модели комплексной оценки защищенности КС** (*модель системы с полным перекрытием, модель Клементса, гиперграфовая модель*)

3.3. **Теоретико-графовая модель анализа системы индивидуально-группового доступа к иерархически организованным информационным ресурсам**

Источники

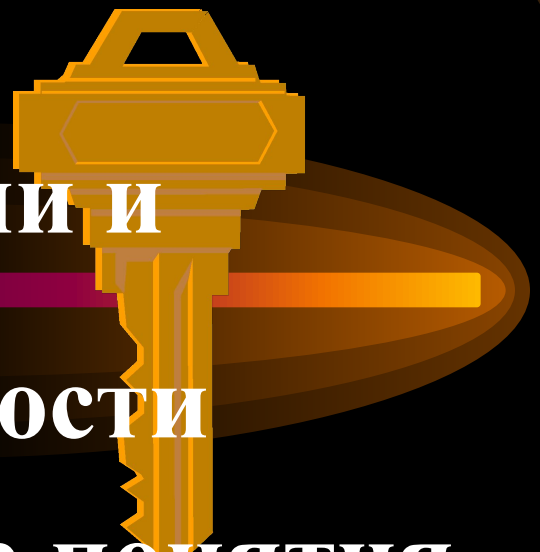
1. **Хоффман Л.** Современные методы защиты информации. М.:Сов.радио, 1980. – 264с.
2. **Грушо А.А.,Тимонина Е.Е.** Теоретические основы защиты информации. М.: Яхтсмен, 1996. - 192с.
3. **Теория и практика обеспечения информационной безопасности** / Под ред. П.Д. **Зегжды**. М.:Яхтсмен, 1996. - 302с
4. **Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю.** Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998.- 184с.
5. **Зегжда Д.П.,Ивашко А.М.** Основы безопасности информационных систем. - М.:Горячая линия - Телеком, 2000. - 452с.
6. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / **П.Н. Девянин, О.О.Михальский, Д.И.Правиков** и др.- М.: Радио и Связь, 2000. - 192с.
8. **Щербаков А.Ю.** Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачев С.В.- 2001- 352 с.
9. **Гайдамакин Н.А.** Разграничение доступа к информации в компью-терных системах. - Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.
10. **Корт С.С.** Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.
11. **Девянин П.Н.** Модели безопасности компьютерных систем: Учеб. пособие. – М.: Изд.центр «Академия», 2005. – 144 с.

Тема **1.** **Основы теории компьютерной безопасности**

Лекция 1.1Лекция 1.1.

Содержание и основные понятия компьютерной безопасности

Учебные вопросы:



1. История развития теории и практики обеспечения компьютерной безопасности
2. Содержание и структура понятия компьютерной безопасности
3. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности

1. История развития теории и практики обеспечения компьютерной безопасности

Защита информации – проблема с древнейших времен

Специфика компьютерной формы информации:

- возможность получения доступа к большим объемам информации в локальном физическом сосредоточении
- возможность быстрого или мгновенного копирование огромны объемов информации и, как правило, без следов
- возможность быстрого или мгновенного разрушения или искажения огромных объемов информации

провоцирует на посягательство

в результате – КС и ИБ – неотделимые понятия

Защита (обеспечение) безопасности информации – не просто вспомогательная, но одна из главных (основных) функций КС при их создании

Основные этапы развития теории и практики КБ:

Этап	Год	Основные факторы	Содержание
Начальный	60-е - 70-е г.г.	•Появление ЭВМ 3-го поколения •Начало примен-я ЭВМ для инф. обеспеч-я крупн. предпр-й и орг-й	•Начало теоретич. иссл. проблем защиты КИ (АДЕПТ-50, 1967г.) •Исследование и первые реализации технолог. аспектов защиты инф-и (парольные системы аутентификации) •"Открытие" криптографии во внегосударственной сфере (однако 1-е работы К.Шеннона в 1949г.)
2-й этап	70-е - нач. 80-х г.г.	•Широкое внедр. ЭВМ в инф.обесп. не только крупн., но средн. предпр. •Персонализация СВТ •Внедр. ПЭВМ в офисн., фин/хоз/ экон. деят-ть •Появл. на базе ПЭВМ систем лок. инф. коммун.	•Интенсивные теоретич. исследования по формальным моделям безопасности: -Хоффман(1970-1974 г.г.) -Хартсон (1975г.) -Харрисон, Рузо, Ульман (1975г.) -Белл, ЛаПадула (1975г.-1976г.) •Опубл-е в США стандарта DES (1977г.) •Интенс-е теор. иссл-я в сфере нессиметр. криптографии: -У.Диффи, М.Хеллман (1976г.) -стандарт RSA - Р.Райвест, А.Шамир А.Адлеман (1978г.) •"Оранжевая книга" (1983г.) •MMS-модель (1984г.) •ГОСТ 28147-89

Основные этапы развития теории и практики КБ:

Эт ап	Год ы	Основные факторы	Содержание
3-й этап	ко-нец 80-х - 90-е г.г.	•Полная компьюте-ризация всех сфер деятельности •Повсеместн. исп. ПК, в т.ч. и как ср. инф. коммун. •Возникн. и стрем. разв. глоб. инф.-компь. инфраструктуры (сети Интернет) •Возникновения и развитие "Инфор-мационного" зако-нодательства	•Дальн. разв. формальных моделей и техноло-гий защиты информации •Переход на "защищенность" при разработке коммерческих КС: -ОС -СУБД •Появление спец. проблемы КБ – **компьютер-ных вирусов** (термин ввел Ф.Коэн, 1984) •Развитие национальных и международных стандартов защищенности КС •Широкое внедрение криптографических средств защиты информации: -для хранения и передачи КИ -в архитектуру КС -в процедуры аутентификации (появл. криптограф. протоколов) •Теорет. иссл. и реализация практ. систем обеспечения целостности КИ (появления стандартов и систем ЭЦП) •Появление "компьютерной" преступности

Основные этапы развития теории и практики КБ:

Отечественная школа КБ

В.А.Герасименко - ***1991г.***, модель системно-концептуального подхода к безопасности

Грушо А.А., Тимонина Е.Е. – ***1996г.,*** гарантированность защищенности АС как математическое доказательство гарантированного выполнения априорно заданной политики без-ти

Расторгуев С.П., ***начало 90-х г.г. -*** теория разрушающих программных воздействий, ***середина 90-х г.г. -*** теория информационного противоборства

Щербаков А.Ю. – ***90-е г.г.,*** субъектно-объектная модель изолированной программной среды

СПб школа **Зегжды П.Д.** – ***середина 90-х г.г.,*** таксонометрия изъянов безопасности КС

Школа **ИКСИ** (**Б.А.Погорелов, А.П.Коваленко**) – ***конец 90-х г.г.,*** государственные образовательные стандарты подготов-ки специалистов в сфере компьютерной безопасности

2. Содержание и структура понятия компьютерной безопасности

Иерархия понятий:

Безопасность

Информационная *Безопасность*

Компьютерная *Безопасность*

Безопасность компьютерной информации

Методологическая база - понятие ***безопасности***
(з-н "О безопасности", 1993г.)

- состояние ***защищенности*** жизненно важных интересов личности, общества и государства от внутренних и внешних ***угроз***

Информационная безопасность РФ - состояние защищенности ее (РФ) национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства (Доктрина ИБ РФ)

Компьютерная безопасность – состояние защищенности (безопасность) информации в компьютерных системах и безотказность (надежность) функционирования компьютерных систем

2. Содержание и структура понятия компьютерной безопасности

Компьютерная безопасность

Безопасность информации в КС

- Обеспечение конфиденциальности информации
- Обеспечение целостности информации
- Обеспечение доступности информации

- неискаженность, достоверность, полнота, адекватность и т.д., т.е. такое свойство информации, при котором ее содержание и структура (данных) определены уполномоченными лицами и процессами

- свойство информации, субъективно устанавливаемое ее собственником, когда ему может быть причинен ущерб от ознакомления с информацией неуполномоченных на то лиц, при условии того, что собственник принимает меры по организации доступа к информации только уполномоченных лиц

Безотказность (надежность) функционирования КС

- Обеспечение аутентичности реализации функций
- Обеспечение безотказности реализации функций
- Обеспечение целостности параметров ПО
- Обеспечение целостности ПО
- Обеспечение безотказности ПО
- Обеспечение безотказности оборудования

- такое свойство информации, при котором отсутствуют препятствия доступа к информации и закономерному ее использованию собственником или уполномоченными лицами

2. Содержание и структура понятия компьютерной безопасности

Безопасность информации

- состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Общие принципы обеспечения компьютерной безопасности

Разумной достаточности

-внедрение в архитектуру, в алгоритмы и технологии функционирования КС защитных механизмов, функций и процедур объективно вызывает дополнительные затраты, издержки при создании и эксплуатации КС, ограничивает, снижает функциональные возможности КС и параметры ее эффективности (быстродействие, задействуемые ресурсы), вызывает неудобства в работе пользователям КС, налагает на них дополнительные нагрузки и требования — поэтому защита должна быть разумно достаточной (на минимально необходимом уровне)

Целенаправленности

-устранение, нейтрализация (либо обеспечение снижения потенциального ущерба) конкретного перечня угроз (опасностей), характерных для конкретной КС в конкретных условиях ее создания и эксплуатации

Системности

-выбор защитных механизмов с учетом системной сути КС, как организационно-технологической человеко-машинной системы, состоящей из взаимосвязанных, составляющих единое целое функциональных, программных, технических, организационно-технологических подсистем

Комплексности

-выбор защитных механизмов различной и наиболее целесообразной в конкретных условиях природы – программно-алгоритмических, процедурно-технологических, нормативно-организационных, и на всех стадиях жизненного цикла – на этапах создания, эксплуатации и вывода из строя

Общие принципы обеспечения компьютерной безопасности

Непрерывности

-защитные механизмы должны функционировать в любых ситуациях в т. ч. и внештатных, обеспечивая как конфиденциальность, целостность, так и сохранность (правомерную доступность)

Управляемость

-система защиты КС строится как система управления – объект управления (угрозы безопасности и процедуры функционирования КС), субъект управления (средства и механизмы защиты), среда функционирования, обратная связь в цикле управления, целевая функция управления (снижение риска от угроз безопасности до требуемого (приемлемого) уровня), контроль эффективности (результативности) функционирования

Сочетания унификации и оригинальности

-с одной стороны с учетом опыта создания и применения КС, опыта обеспечения безопасности КС должны применяться максимально проверенные, стандартизированные и унифицированные архитектурные, программно-алгоритмические, организационно-технологические решения,

-с другой стороны, с учетом динамики развития ИТ, диалектики средств нападения и защиты должны разрабатываться и внедряться новые оригинальные архитектурные, программно-алгоритмические, организационно-технологические решения, обеспечивающие безопасность КС в новых условиях угроз, с минимизацией затрат и издержек, повышением эффективности и параметров функционирования КС, снижением требований к пользователям

3. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности

Систематика методов и механизмов обеспечения КБ

Основного характера (прямого действия)

Общесистемного характера

Инфраструктурного характера

- Управление (контроль) конфигурацией
- Управление сеансами
- Управление удаленным доступом с раб. станций
- Управление сетевым соединениями

Общеархитектурного характера

- Идентификация аутентификация пользователей, устройств, данных
- Управление памятью, потоками, изоляция процессов
- Управление транзакциями

- Управление инфраструктурой сертификатов криптоключей

Непосредственного действия

- Разграничение доступа к данным
- Контроль, управление информационной структурой данных
- Контроль ограничений целостности данных
- Шифрование данных
- ЭЦП данных
- Защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти

конфиденциальность

целостность

доступность

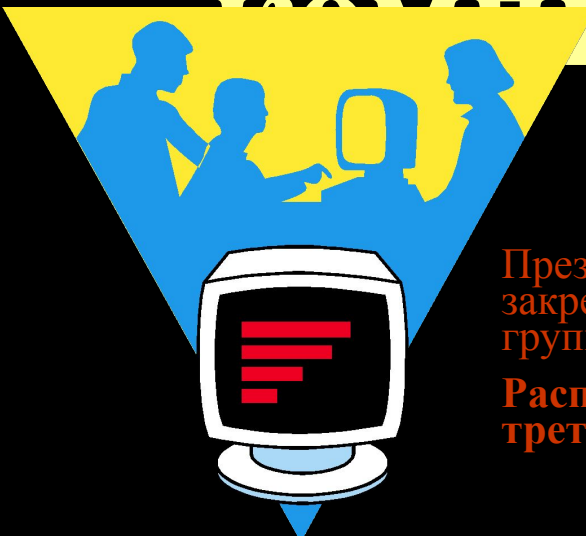
Обеспечивающего (профилактирующего) характера

- Протоколирование, аудит событий
- Резервирование данных, журнализация процессов изменения данных
- Профилактика носителей данных
- Учет/контроль носителей данных
- Нормативно-организационная регламентация использования КС
- Обучение. нормативно-административное побуждение и принуждение пользователей по вопросам ИБ

Тема 1. Исходные положения теории компьютерной безопасности

Лекция 1.2.

Угрозы безопасности в компьютерных системах



Презентация предназначена для отработки и закрепления лекционного материала студентами группы КБ МатМех УрГУ.

Учебные вопросы:

1. **Понятие и классификация угроз**
2. **Идентификация и таксонометрия (каталогизация) угроз**
3. **Оценивание угроз**
4. **Человеческий фактор в угрозах безопасности и модель нарушителя**

Литература:

1. **ГОСТ Р 51275-99.** Защита информации. Объект информатизации. Факторы, воздействующие на информацию
2. Bundesamt für Sicherheit der Informationstechnik (Германский стандарт безопасности IT), http://www.bsi.de
3. **РД ГосТехКомиссии России.** Безопасность ИТ. Руководство по формированию семейств профилей защиты
4. **ГОСТ Р ИСО 7498-2-99**. Взаимосвязь открытых систем. Базовая эталонная модель. **Ч.2.** Архитектура защиты информации

1. Понятие и классификация угроз

ГОСТ Р 51624-2000

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее

РД ГосТехКомиссии «Безопасность ИТ. Положение о разработке ПЗ и ЗБ»

Угроза (*threat*) – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его собственнику

Угроза безопасности КС – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, [правомерной] доступности КИ и/или снижения надежности [безотказности и аутентичности] реализации функций КС

1. Понятие и классификация угроз

Систематизация – приведение в систему, т.е. в нечто целое, представляющее собой единство закономерно расположенных и находящихся во взаимной связи частей; выстраивание в определенный порядок.

Частным случаем *систематизации* является **классификация**

Классификация –

последовательное деление понятий, проводимое по характеристикам и параметрам, существенным с точки зрения исследовательской задачи

Существенные параметры и характеристики называются основаниями, критериями классификации

Выделяется

таксономическая классификация (род-вид)

мереологическая классификация (часть-целое)

фасетная классификация (аналитико-синтетическая)

1. Понятие и классификация угроз

1. Понятие и классификация угроз

А Угрозы по природе происхождения

Случайные (объективные) - *возникают без преднамеренного умысла*

- **Отказы и сбои аппаратуры**
  - *определяются качеством и надежностью аппаратуры*
  - *техническими решениями и др. факторами*
- **Помехи на линиях связи от внешних воздействий**
  - *правильность выбора места (маршрута) прокладки*
  - *технических решений по помехозащищенности*
  - *э/м обстановки*
- **Ошибки человека как звена информационной системы**

По месту в системе
- *как источника информации*
- *как оператора (ввод-вывод данных)*
- *как обслуживающего персонала*
- *как звена принятия решений*

Интенсивность - $2 \cdot 10^{-2} \ldots 4 \cdot 10^{-3}$

По типу:
- логические (неправильные решения)
- сенсорные (неправильное восприятие)
- оперативные и моторные (неправильная реализация или реакция)

- **Схемные и системотехнические ошибки разработчиков**
- **Структурные, алгоритмические и программные ошибки**
  - *специальные методы проектирования и разработки*
  - *специальные процедуры тестирования и отладки*
- **Аварийные ситуации**
  - *по выходу из строя электропитания*
  - *по стихийным бедствиям*
  - *по выходу из строя систем жизнеобеспечения*

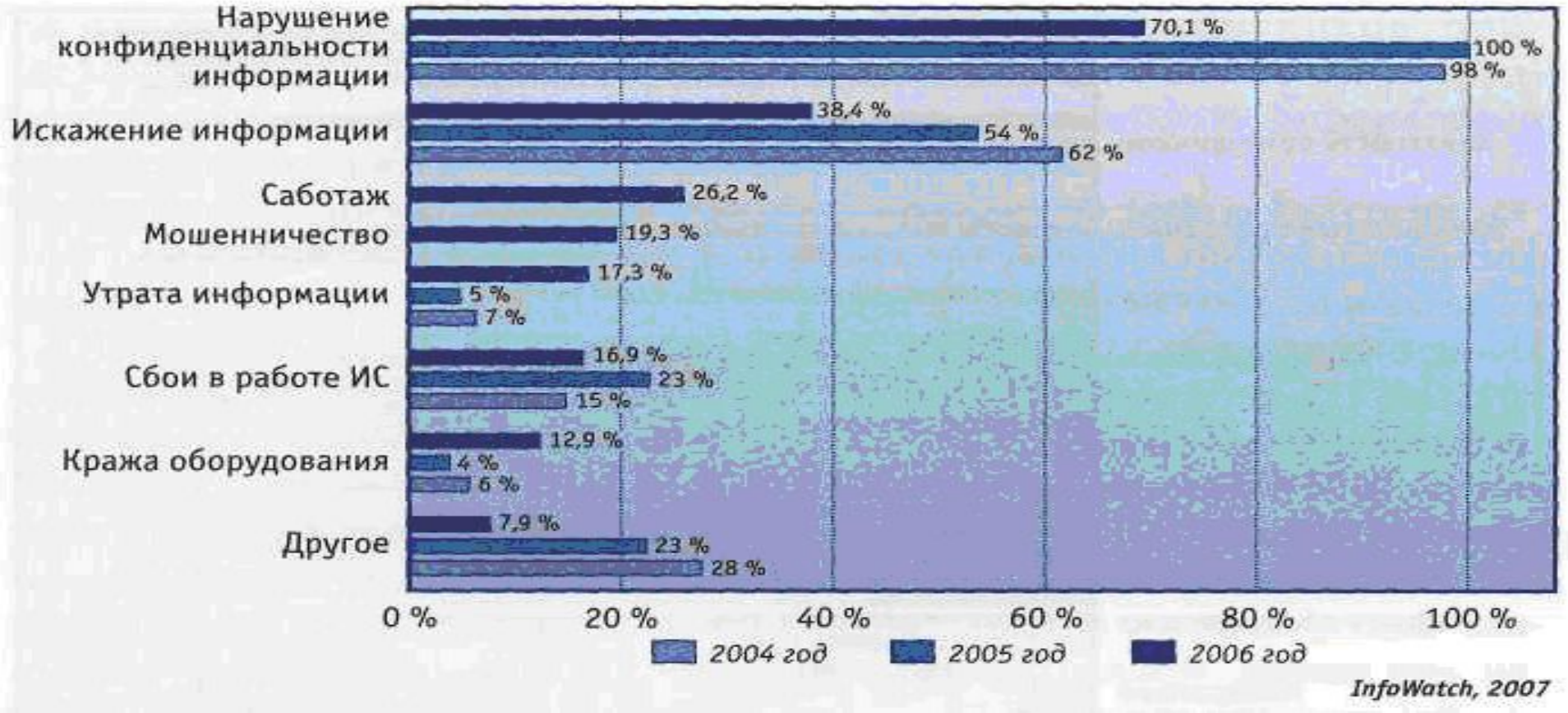
1. Понятие и классификация угроз

A Угрозы по природе происхождения

Преднамеренные
(субъективные)

- вызванные человеком или связанные с действиями человека, определяются т.н. человеческим фактором (мотивы, категории, возможности)

Общий ландшафт инцидентов в **IT**-сфере РФ



1. Понятие и классификация угроз

Угрозы по направлению осуществления

Внешние

- исходящие извне по отношению к персоналу, к организации (предприятию), к государству, к территории (зданиям, помещениям) компьют. системы

Внутренние

- происходящие внутри КС, среди персонала, в зоне расположения объектов КС

Внешняя (неконтролируемая) зона

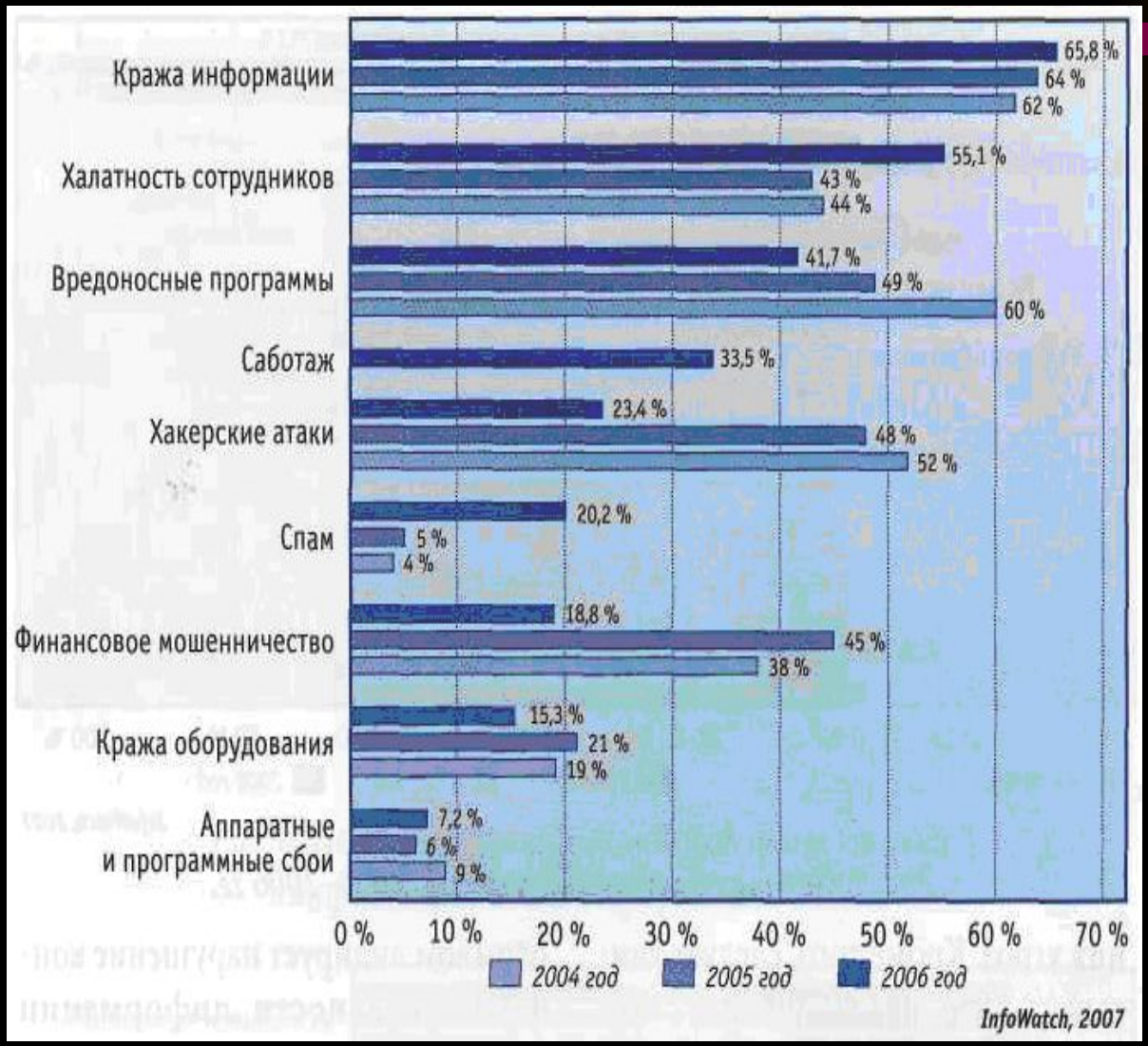
Внутренняя зона КС

Зона контролируемой территории

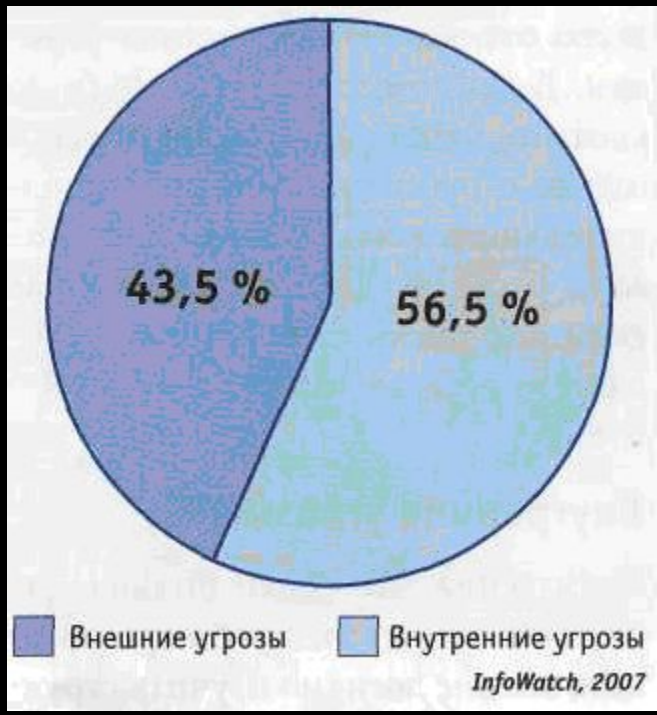
Зона помещений КС

Зона ресурсов КС

Соотношение некоторых видов угроз



Соотношение внешних и внутренних (т.н. инсайдерских) угроз



2. Идентификация и таксонометрия (каталогизация) угроз

ГОСТ Р ИСО/МЭК 15408-2002, ч.1

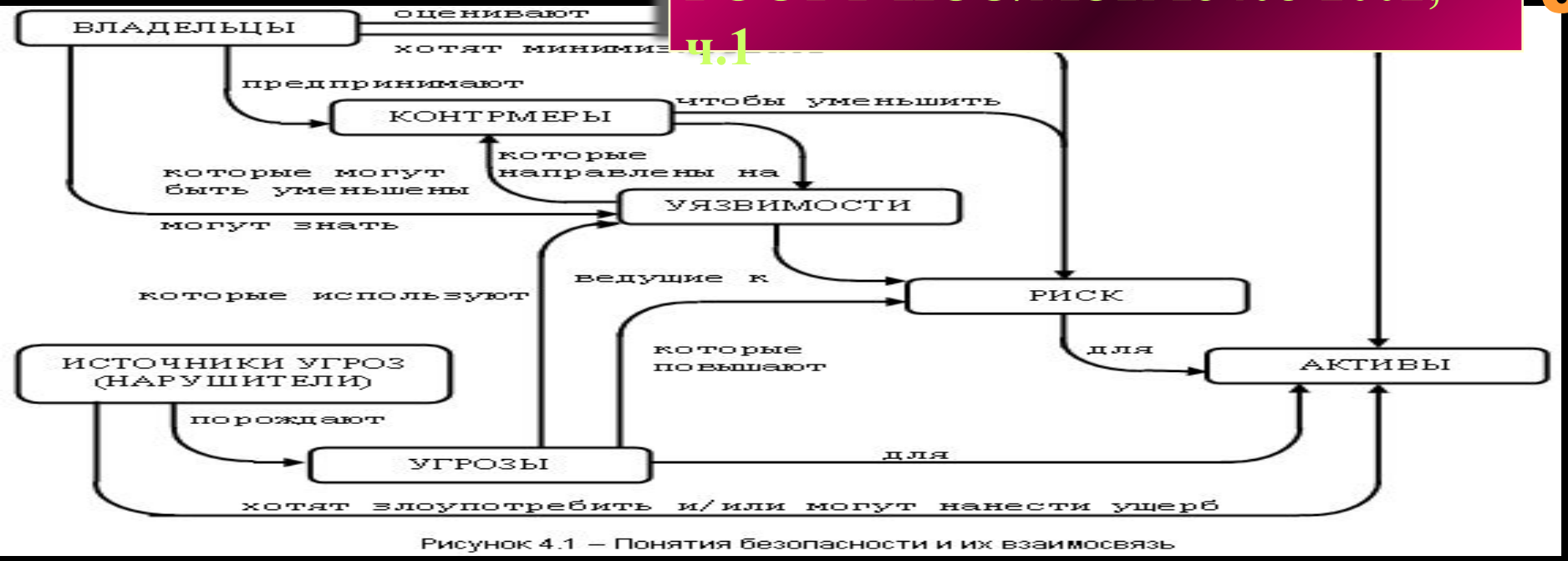


Рисунок 4.1 — Понятия безопасности и их взаимосвязь

Процесс создания КС в аспекте обеспечения безопасности:

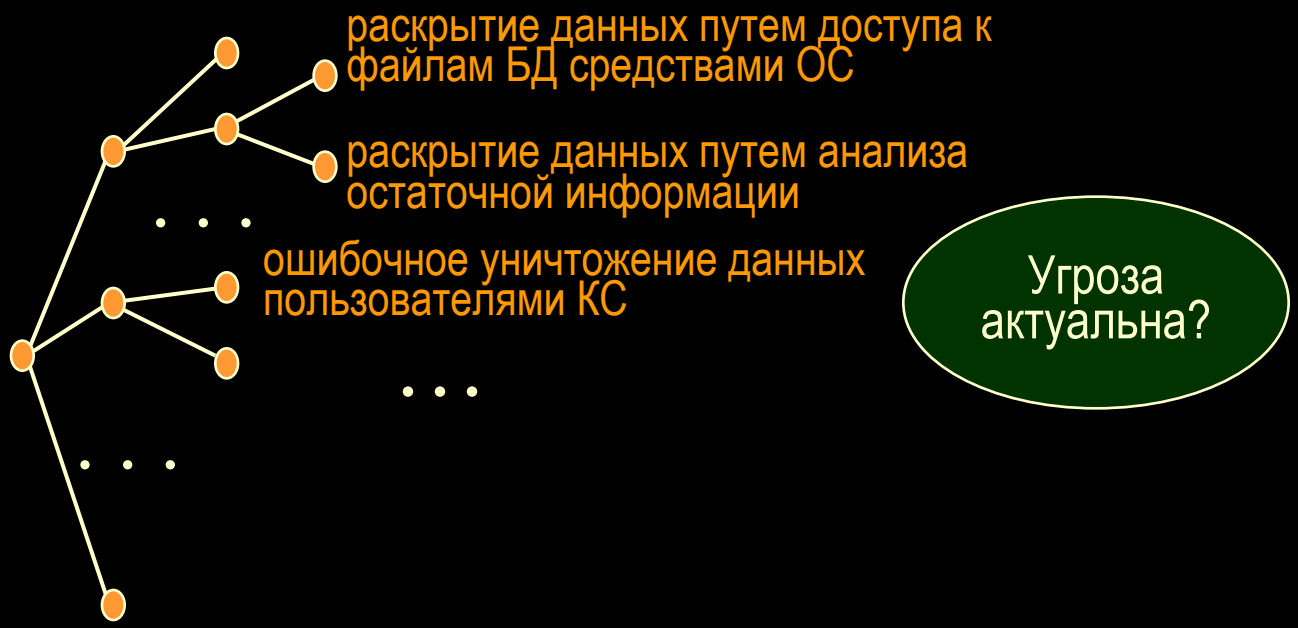
1. Идентификация и оценка защищаемых активов (*конфиденциальность*, *целостность*, *доступность*) и функций КС
2. Идентификация угроз безопасности (выявление и спецификация - источники/природа; активы/функции, подвергаемые воздействию; методы/способы/особенности реализации; используемые уязвимости) и их оценка
3. Выбор и обоснование функциональных требований к КС (архитектура и лежащие в ее основе модели обеспечения конфиденциальности/целостности/доступности; функции обеспечения безопасности)
4. Реализация функциональных требований в процессе проектирования/создания
5. Оценка степени реализации функциональных требований (сертификация по требованиям безопасности), в т.ч. возможных уязвимостей, брешей безопасн-ти

2. Идентификация и таксонометрия (каталогизация) угроз

Идентификация угроз

-установление из всех возможных - тех угроз, которые имеют место быть (существуют, актуальны, воздействуют) для данной КС в процессах ее создания и эксплуатации;

-основывается на использовании таксономических классификационных перечней угроз (каталогов угроз), закрепляемых в стандартах и др. нормативно-методических документах и анализе актуальности тех или иных угроз в отношении активов (ресурсов КС) и их ценности



Перечень угроз для КС

Угр.1. Раскрытие данных путем доступа к файлам БД средствами ОС

Угр.2. Раскрытие данных путем анализа остаточной информации

. . .

2. Идентификация и таксонометрия (каталогизация) угроз

Каталоги (таксономические схемы классификации) угроз безопасности

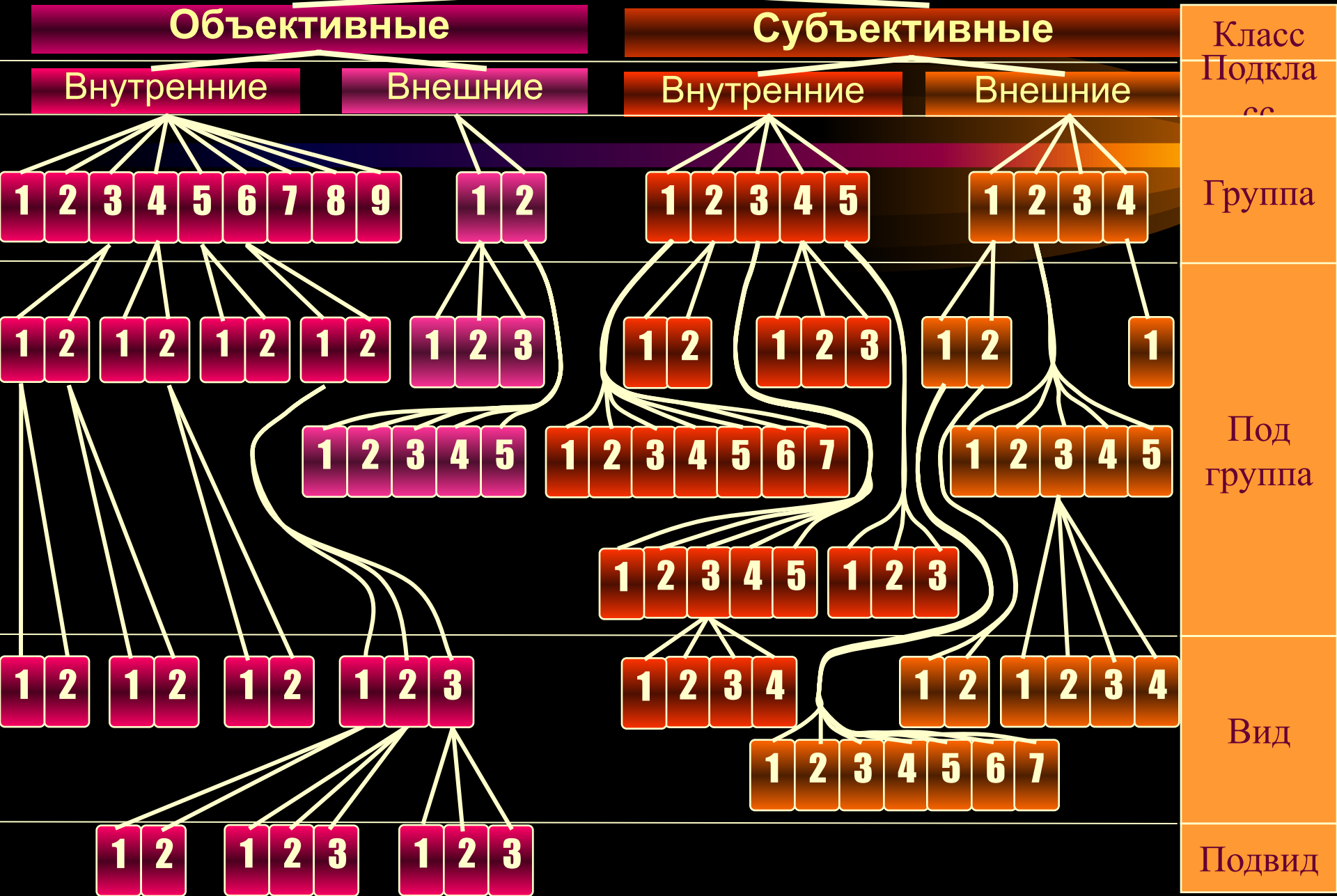
ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. http://linux.nist.fss.ru

Bundesamt für Sicherheit der Informationstechnik (Германский стандарт безопасности IT), http://www.bsi.de

РД ГосТехКомиссии России. Безопасность ИТ. Руководство по формированию семейств профилей защиты. http://www.fstec.ru

2. Идентификация и таксонометрия (каталогизация) угроз

Факторы, воздействующие на информацию (ГОСТ Р 51275-99)



2. Идентификация и таксонометрия (каталогизация) угроз

Классы, подклассы и группы факторов (ГОСТ Р 51275-99)

4.3.1. Объективные

4.3.1.1. Внутренние

- 4.3.1.1.1. Передача сигналов по проводным линиям связи
- 4.3.1.1.2. Передача сигналов по оптико-волоконным линиям связи
- 4.3.1.1.3. Излучение сигналов, функционально-присущих ОИ
- 4.3.1.1.4. ПЭМИ
- 4.3.1.1.5. Паразитные электромагнитные излучения
- 4.3.1.1.6. Наводки
- 4.3.1.1.7. Акустоэлектрические преобразования в элементах ТС ОИ
- 4.3.1.1.8. Дефекты, сбои, аварии ТС и систем ОИ
- 4.3.1.1.9. Дефекты, сбои и отказы программного обеспечения ОИ

4.3.1.2. Внешние

- 4.3.1.2.1. Явления техногенного характера
- 4.3.1.2.2. Природные явления, стихийные бедствия

4.3.2. Субъективные

4.3.2.1. Внутренние

- 4.3.2.1.1. Разглашение ЗИ лицами, имеющими к ней право доступа
- 4.3.2.1.2. Неправомерные дейст-я со стороны лиц,имею-х право доступа к ЗИ
- 4.3.2.1.3. НСД к ЗИ (внутренний)
- 4.3.2.1.4. Неправильное организационное обеспечение ЗИ
- 4.3.2.1.5. Неправильное организационное обеспечение ЗИ
- 4.3.2.1.6. Ошибки обслуживающего персонала ОИ

4.3.2.2. Внешние

- 4.3.2.2.1. Доступ к ЗИ с применением технических средств
- 4.3.2.2.2. НСД к ЗИ (внешний)
- 4.3.2.2.3. Блокирование доступа к ЗИ путем перегрузки технических средств обработки информации ложными заявками на ее обработку
- 4.3.2.2.4. Действия криминальных групп и отдельных преступных элементов

2. Идентификация и таксонометрия (каталогизация) угроз

Каталог угроз (BSI)

Каталог угроз по Германскому стандарту

Т.1 Форс-мажор	Т.1.1. Опасности персоналу (болезни, несчастные случаи, забастовки,...)
	Т.1.2. Недостатки ИС
	Т.1.3. Молниеопасность
	Т.1.4. Пожары
	Т. 1.5. Затопления
	Т.1.6. Возгорание, замыкание кабелей
	Т.1.7. Недопустимые температуры и влажность
	Т.1.8. Запыления, загрязнения
	Т.1.9. Утрата данных из-за сильных магнитных полей
	Т.1.10. Недостатки во внешних сетях
Т.2. Организа-ционные дефекты и недостатки	Т.2.1. Отсутствие или неэффективное управление, руководство
	.... (60 факторов)
Т.3 Челове-ческие недостат-ки	Т.3.1. Потеря конфиденциальности/целостности данных в результате ошибок ИТ-персонала
	Т.3.2. Разрушение оборудования или данных в результате небрежности
	Т.3.3. Несоблюдение (несогласие) мер ИТ-безопасности
	....(45 факторов)
Т.4. Техн. недостат-ки	Т.4.1. Разрушение вследствие аварий энергоснабжения
	...(42 фактора)
Т.5. Предна-мерен-ные действия	Т.5.1. Подделка, искажение, разрушение оборудования или принадлежностей
	Т.5.2. Искажение данных или программ
	Т.5.3. Безконтрольный (неавторизованный) вход в здания
	Т.5.4. Кражи, хищения
	Т.5.5. Вандализм
	Т.5.6. Атаки
	Т.5.7. Перехват с линий связи
	... (99 факторов)

2. Идентификация и таксонометрия (каталогизация) угроз

Методология объектов и угроз в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2015г., пример)

- Угрозы данным на носителях
- Угрозы данным в телекоммуникационных линиях
- Угрозы прикладным программам (приложениям)
- Угрозы прикладным процессам и данным
- Угрозы отображаемым данным
- Угрозы вводимым данным
- Угрозы данным, выводимым на печать
- Угрозы данным пользователей
- Угрозы системным службам и данным
- Угрозы информационному оборудованию

Аспекты угрозы

- источник угрозы (люди либо иные факторы)
- предполагаемый метод (способ, особенности) нападения/реализации
- уязвимости, которые м.б. использованы для нападения/реализации
- активы, подверженные нападению/реализации

Угрозы защищаемым активам в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2015г., пример)

данные на носителях

- данные раскрыты путем незаконного перемещения носителя
- обращение к данным, изменение, удаление, добавление в приложение или извлечение из приложения данных неуполномоченным лицом
- данные раскрыты путем их выгрузки с носителя данных неуполномоченным лицом
- использование остаточной информации на носителе
- незаконное копирование данных
- данные незаконно используются, или их использование затруднено из-за изменения атрибутов доступа к данным неуполномоченным лицом
- данные получены незаконно путем фальсификации файла
- данные повреждены из-за разрушения носителя
- данные уничтожены или их использование затруднено из-за неисправности устройства ввода-вывода
- обращение к данным, изменение, удаление, добавление в приложение или извлечение из приложения данных неуполномоченным лицом путем использования соответствующей команды
- зашифрованные данные не могут быть дешифрованы из-за потери секретного ключа
- данные ошибочно удалены уполномоченным лицом

2. Идентификация и таксонометрия (каталогизация) угроз

Угрозы защищаемым активам в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2015г., пример)

данные в телекоммуникационных линиях	данные перехвачены или разрушены в телекоммуникационной линии
	данные прослушиваются, незаконно умышленно изменены, искажены, похищены, удалены или дополнены в системе коммутации
	данные незаконно используются в результате подмены их адресата, отправителя или изменения атрибутов доступа в системе коммутации
	связь заблокирована из-за повреждения линии
	связь заблокирована из-за аномалий в канале связи
	несанкционированная повторная передача данных в неразрешенный адрес
прикладные программы (приложения)	выполнение приложения неуполномоченным лицом
	обращение к данным в библиотеке программ, модификация или удаление данных в библиотеке программ неуполномоченным лицом
	незаконное использование программы или затруднение ее использования путем изменения ее атрибутов доступа неуполномоченным лицом
	аномалии в ходе выполнения программы из-за аппаратного отказа компьютера

2. Идентификация и таксонометрия (каталогизация) угроз

Угрозы защищаемым активам в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2015г., пример)

прикладные проце… и данные

- несанкционированное использование прикладных процессов (например, запросов по Telnet и FTP)
- блокировка прикладных процессов (атаки, направленные на переполнение трафика, например, запросы на обработку потока ненужных данных)
- отрицание факта обмена данными или отрицание их содержания
- отказ от авторства данных
- несанкционированная передача данных
- несанкционированное использование данных или программ путем использования оставшихся в программах отладочных функций
- необоснованный отказ от предоставления услуги
- незаконное умышленное изменение, искажение, похищение, удаление или разрушение данных
- несанкционированное выполнение операций
- нарушение конфиденциальности

отображаемые дан…

- просмотр данных неуполномоченным лицом
- несанкционированное копирование или печать

вводимые данные

- данные раскрыты во время ввода
- введенные данные несанкционированно изъяты (или удалены)

2. Идентификация и таксонометрия (каталогизация) угроз

Угрозы защищаемым активам в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2015г., пример)

данные, выводимые на печать

- ознакомление или изъятие данных неуполномоченным лицом
- несанкционированное копирование

данные пользовательской

- пользователь (человек, система, терминал) не может быть идентифицирован
- маскировка путем использования раскрытой идентификационной информации пользователя (человека, системы, терминала)
- пользователь не идентифицирован
- маскировка путем использования незаконно раскрытой информации аутентификации
- маскировка путем незаконного (логического) вывода аутентификационной информации
- маскировка путем использования недействительной аутентификационной информации
- использование недействительного права из-за сбоя журнала регистрации прав пользователей
- действия пользователя несанкционированно раскрыты (нарушение конфиденциальности)
- отрицание факта передачи данных
- отрицание владения данными
- отрицание факта приема данных
- данные посланы несоответствующему получателю вследствие его маскировки под авторизованного пользователя или ошибки спецификации
- маскировка путем подделки информации аутентификации

2. Идентификация и таксонометрия (каталогизация) угроз

Угрозы защищаемым активам в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2015г., пример)

системные службы данные

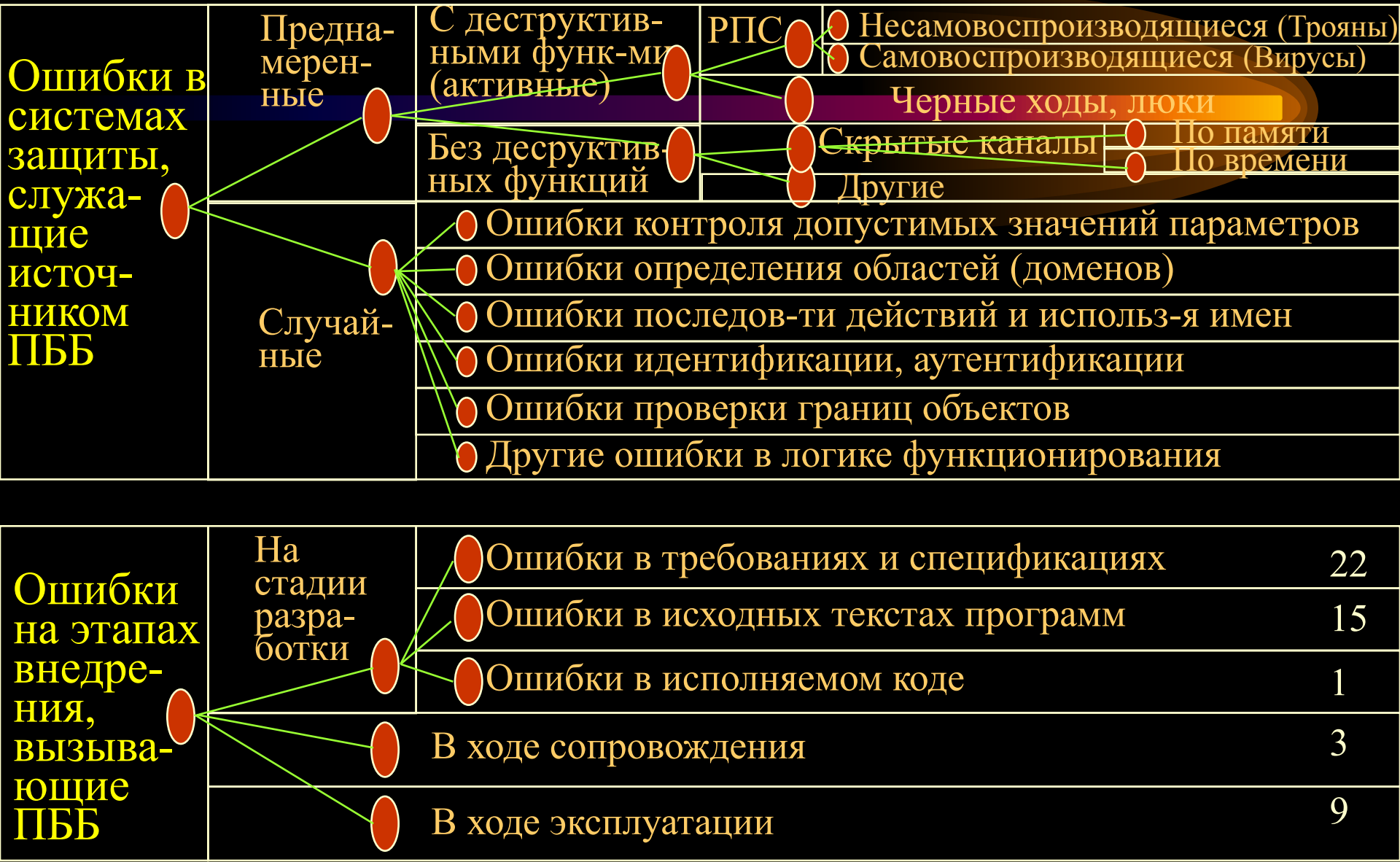
- нарушение безопасности системы путем раскрытия секретного ключа шифрования
- система незаконно используется пользователем, который выдает себя за оператора во время отсутствия оператора
- нарушение безопасности системы вследствие несанкционированного действия или ошибки уполномоченного пользователя
- внедрение вирусов
- несанкционированное проникновение в систему
- проникновение в систему, используя известные дефекты протоколов (например, протокола IP)
- нарушение безопасности системы вследствие несанкционированной замены системной программы
- обслуживание прекращено из-за разрушения системной программы
- несанкционированная системная операция

информационное оборудование

- повреждение или изъятие
- отключение питания

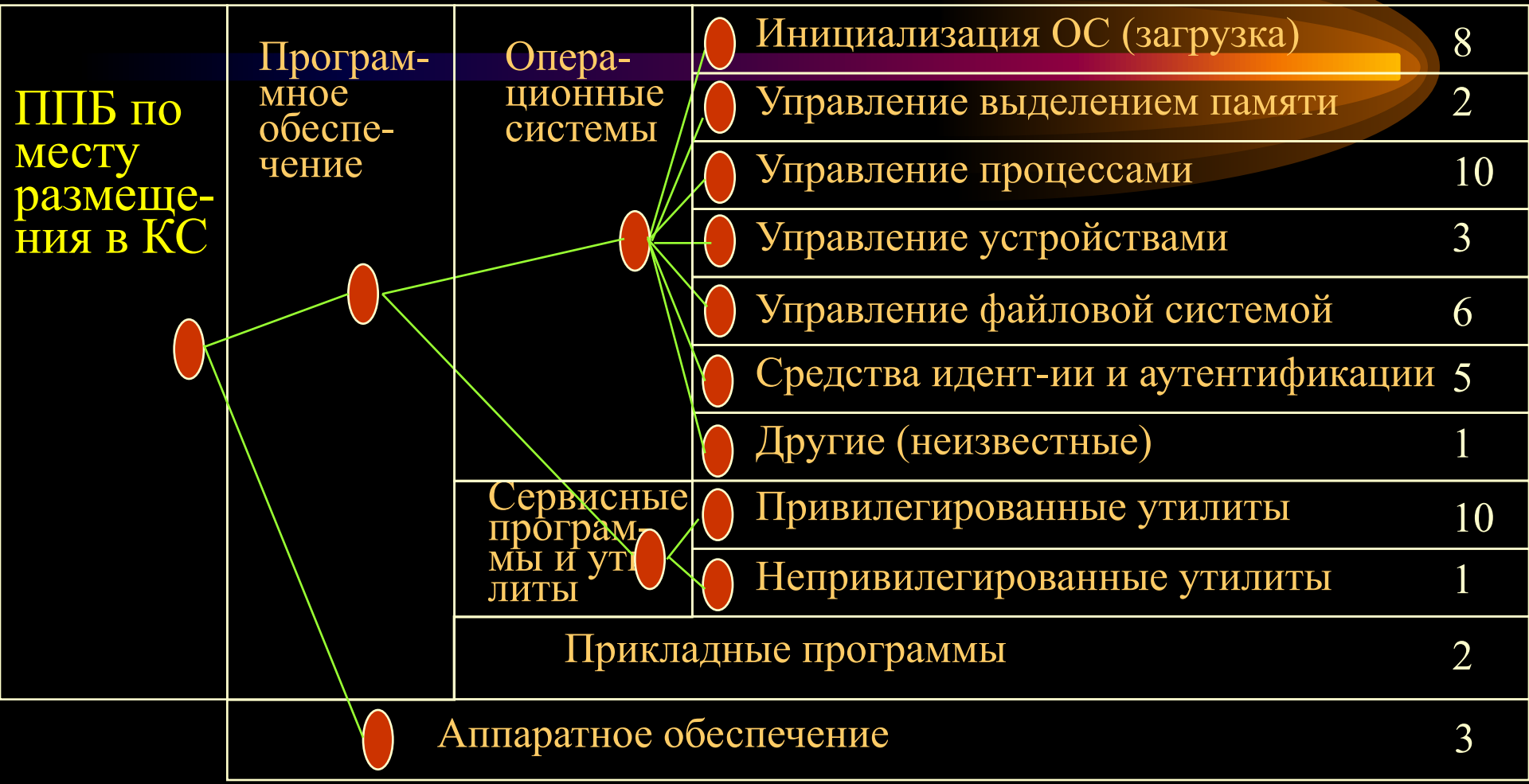
2. Идентификация и таксонометрия (каталогизация) угроз

Потенциальные бреши безопасности (по Зегжде)

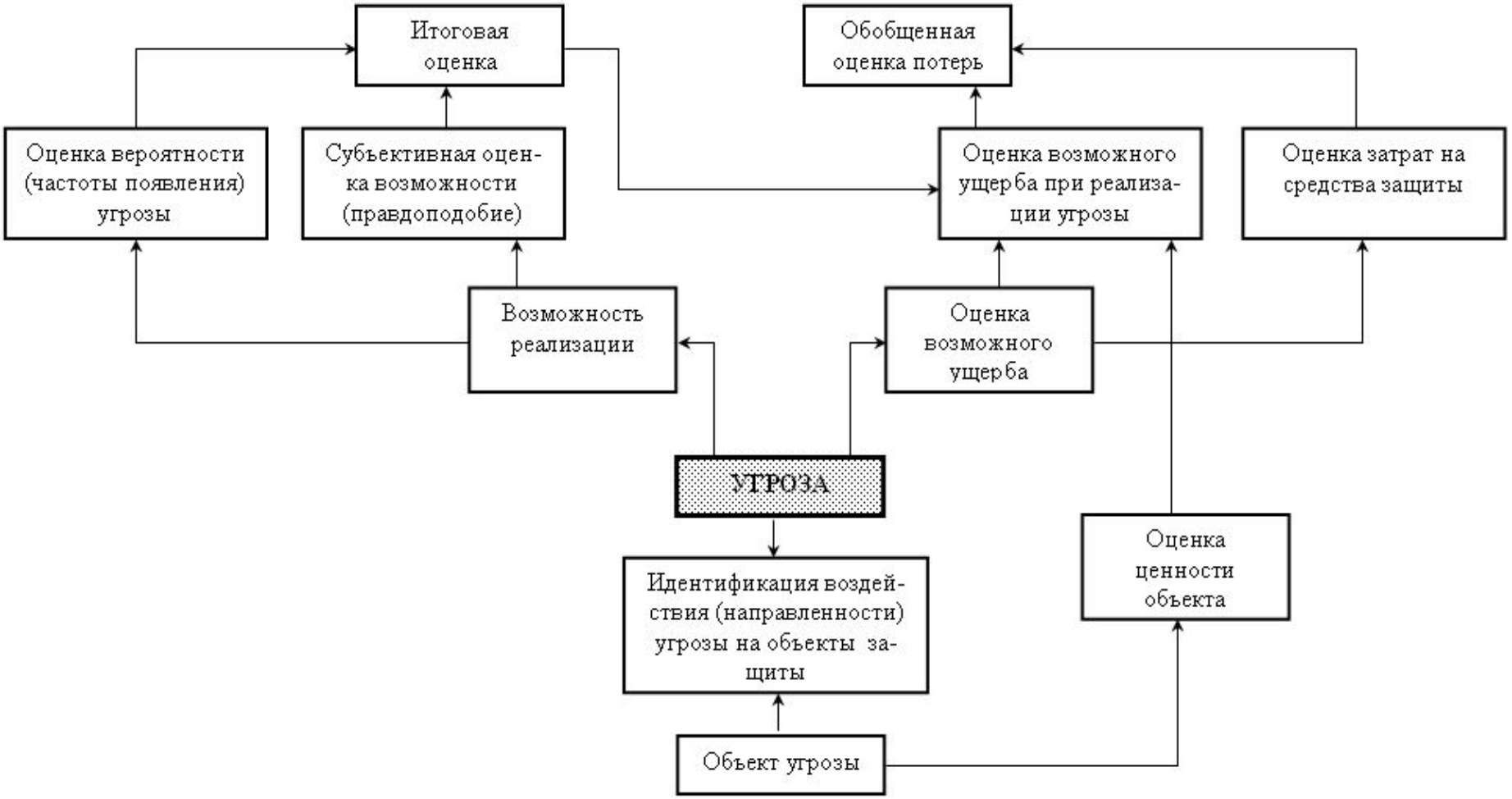


2. Идентификация и таксонометрия (каталогизация) угроз

Потенциальные бреши безопасности (Зегжда)



Общая схема оценивания угроз



Общая схема оценки угроз

$$Ущ = Р_{уг} * Ст_{о}$$

3. Оценивание угроз

Методы оценивания вероятности угроз

Априорные, на основе моделей и статистических характеристик физических процессов, реализующих соотв. угрозы (*z.b.* на основе Пуассоновского распределения вероятности моторных ошибок человека-оператора при вводе информации с клавиатуры с $\alpha = -2 \cdot 10^{-2} \ldots 4 \cdot 10^{-3}$)

Апостериорные, на основе гистограмм распределения событий проявления соотв. угроз по результатам эксплуатации КС

Экспертные, на основе экспертных оценок специалистов

Методики экспертных оценок

1. Отбор экспертов (формальные и неформальные требования, метод «снежного кома», 10-12 экспертов)
2. Выбор параметров, по которым оцениваются объекты (стоимость, важность, веса параметров)
3. Выбор шкал оценивания (методов экспертного шкалирования)

Методы оценивания вероятности угроз

Методы экспертного шкалирования

Непосредственной оценкой

	Эксп. 1	Эксп. 2		Эксп. *M*
Угр. 1				
Угр. 2				
…			p_{ij}	
Угр. *N*				

$$p_i = \sum_{j=1}^{M} \frac{1}{M} p_{ij}$$

Парным сравнением

$$p_i = \sum_{j=1}^{N} \sum_{m=1}^{M} \frac{1}{MN} p^{m}{}_{ij}$$

Эксп. *M*	Угр. 1	Угр. 2		Угр. *N*
Угр. 1				
Угр. 2				
…			p^{M}_{ij}	
Угр. *N*				

Эксп. 2	Угр. 1	Угр. 2		Угр. *N*
Угр. 1				
Угр. 2				
…			p^{2}_{ij}	
Угр. *N*				

Эксп. 1	Угр. 1	Угр. 2		Угр. *N*
Угр. 1				
Угр. 2				
…			p^{1}_{ij}	
Угр. *N*				

Ранжированием

	Эксп. 1	Эксп. 2		Эксп. *M*
Угр. 1	2	1		5
Угр. 2	1	3		1
…				
Угр. *N*	5	2		2

4. Процедуры опроса экспертов (метод «Дельфи»)
5. Агрегирование оценок, анализ их устойчивости и согласованности

Человеческий фактор в угрозах

Роль человека в угрозах безопасности информации:

- носитель/источник угроз (*как внутренних, так и внешних, как случайных, так и преднамеренных*)

- средство, орудие осуществления угроз (*всех преднамеренных и определенной части случайных угроз*)

- предмет, объект, среда осуществления угроз (*как элемента человеко-машинной КС*)

4. Человеческий фактор в угрозах безопасности и модель нарушителя

Структура потенциальных нарушителей (злоумышленников)

Внешняя сторона

Компьютерная (информационная) система

Внутренняя сторона

Сфера сотрудничества

Производственно-технологический аспект

Общественно-политический аспект

Сфера противоборства

Конкуренция

Преступность

Иные сферы

Сторонние эксперты, конс.

Родственники, друзья

Бывшие работники

- **Персонал, непосредственно связанный с КС**
  - ***обслуживающий персонал***
    - администраторы
      - системные
      - безопасности
    - инженеры-программисты
      - системные
      - прикладные
    - руководители служб ИТ
  - ***обслуживаемый персонал***
    - пользователи
      - индивидуальные
      - члены раб. групп
      - руководители подр-й
- **Персонал, не связанный непосредственно с КС**
  - ***руководители***
  - ***прочие работники***

Мотивы
действий, поступков по осуществлению угроз

- ***Осознанные***
  - *Корысть, нажива*
  - *Политика, власть, шпионаж*
  - *Исследовательский интерес*

- ***Неосознанные*** (не вполне, не до конца осознаваемые)
  - *Хулиганство*
  - *Месть*
  - *Зависть*
  - *Недовольство*
  - *Небрежность, недобросовестность*

4. Человеческий фактор в угрозах безопасности и модель нарушителя

Модель нарушителя

-совокупность представлений по человечес-кому фактору осуществления угроз безопасности

- категории лиц, в числе которых может оказаться нарушитель

- его мотивационные основания и преследуемые цели

- его возможности по осуществлению тех или иных угроз (квалификация, техническая и иная инструментальная оснащенность)

- наиболее вероятные способы его действий

Исходное основание для разработки и синтеза системы защиты информации!!!

4. Человеческий фактор в угрозах безопасности и модель нарушителя

Модель внутреннего нарушителя по РД ГосТехКомисии

!!! Концепция ориентируется на физически защищенную среду -

- нарушитель безопасности как "субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС"

4-й (высший) уровень возможностей нарушителя

Весь объем 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

3-й уровень

Возможность управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию оборудования

2-й уровень

Возможность создания и запуска собственных программ с новыми функциями по обработке информации

1-й уровень

Запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации

Основные способы НСД

- непосредственное обращение к объектам доступа
- создание прогр. и техн. средств, выполняющих обращение к объектам доступа в обход средств защиты
- модификация средств защиты, позволяющая осуществить НСД
- внедрение в техн.ср. СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД

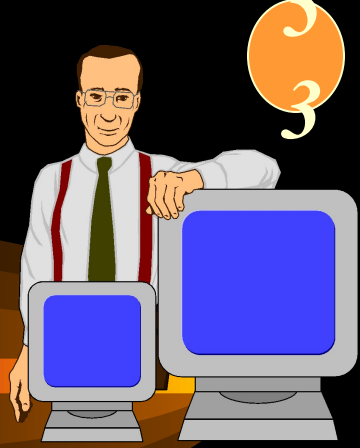
Тема 1. Исходные положения теории компьютерной безопасности

Лекция Лекция 1Лекция 1.Лекция 1.3Лекция

1.3. Политика и модели безопасности в компьютерных системах

Учебные вопросы:

1. **Понятие политики и моделей безопасности информации в компьютерных системах**
2. **Монитор (ядро) безопасности КС**
3. **Гарантирование выполнения политики безопасности. Изолированная программная среда**



Литература:

1. **Теория и практика обеспечения информационной безопасности** / Под ред. П.Д. Зегжды. М.:Яхтсмен, 1996. - 302с
2. **Грушо А.А.,Тимонина** Е.Е.Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с
3. **Баранов А.П., Борисенко Н.П., Зегжда П.Д, Корт С.С., Ростовце** А.Г. Математические основы информационной безопасности. - Орел, ВИПС, 1997.- 354с.
4. **Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю.** Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998.- 184с.
5. **Щербаков А.Ю.** Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачев С.В.- 2001- 352 с.

1.Понятие политики и моделей безопасности информации в КС

Политика безопасности организации

-совокупность руководящих принципов, правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности (ГОСТ Р ИСО/МЭК 15408)

Политика безопасности КС

-интегральная (качественная) характеристика, описывающая свойства, принципы и правила защищенности информации в КС в заданном пространстве угроз

Модель безопасности

-формальное (*математическое*, *алгоритмическое*, *схемотехническое* и т.п.) выражение политики безопасности

Модель безопасности служит для:

-выбора и обоснования базовых принципов архитектуры, определяющих механизмы реализации средств защиты информации

-подтверждения свойств (защищенности) разрабатываемой системы путем формального доказательства соблюдения политики (требований, условий, критериев) безопасности

-составления формальной спецификации политики безопасности разрабатываемой системы

1.Понятие политики и моделей безопасности информации в КС

Модель безопасности включает:

-модель компьютерной системы

-критерии, принципы или целевые функции защищенности и угроз

-формализованные правила, алгоритмы, механизмы безопасного функционирования КС

Большинство моделей КС относится к классу **моделей конечных состояний**

1. Компьютерная система – система, функционирующая в дискретном времени: $t_0, t_1, t_2, \ldots, t_k, \ldots$

В каждый следующий момент времени t_k КС переходит в новое состояние.

В результате функционирование КС представляет собой *детерминированный* или *случайный* **процесс**

- стационарность (временно́е поведение [количественных] параметров системы)
- эргодичность (поведение параметров системы по совокупность реализаций)
- марковость (память по параметрам системы)

2. Модели конечных состояний позволяют описать (спрогнозировать) состояние КС в момент времени t_n,($n \geq 1$), если известно состояние в момент t_0 и установлены некоторые правила (алгоритмы, ограничения) на переходы системы из состояния t_k в t_{k+1}

1.Понятие политики и моделей безопасности информации в КС

Большинство моделей конечных состояний представляет КС системой взаимодействующих сущностей двух типов субъектов и субъектов

(т.н. *субъектно-объектные модели КС*)

3. В каждый момент времени t_k КС представляется конечным множеством элементов, разделяемых на два подмножества:

-множество **субъектов - *S***

-множество **объектов – *O***

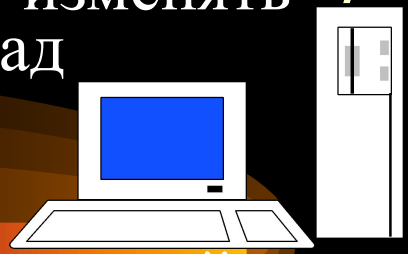
4. В каждый момент времени t_k субъекты могут порождать *процессы над объектами*, называемыми ***доступами***

Доступы субъектов к объектам порождают *информационные потоки*, переводящие КС в новое состояние t_{k+1}, в котором в т.ч. м. измениться декомпозиция КС на множество субъектов и множество объектов

Т.о. процесс функ-я КС нестационарный

1.Понятие политики и моделей безопасности информации в КС

Субъект -активная сущность КС, которая может изменять состояние системы через порождение процессов над объектами и, в т.ч., порождать новые объекты и инициализировать порождение новых субъектов

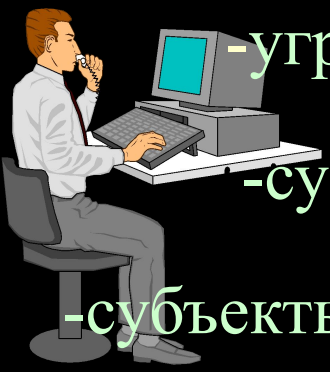


Объект -пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов

Отличия пользователя от субъекта

Пользователь - лицо, внешний фактор, управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии КС через субъекты, которыми он управляет

Свойства субъектов:



-угрозы информации исходят от субъектов, изменяющих состояние объектов в КС

-субъекты-инициаторы могут порождать через объекты-источники новые объекты

-субъекты могут порождать потоки (передачу) информации от одних объектов к другим

1.Понятие политики и моделей безопасности информации в КС

Субъектно-объектная модель Щербакова

Множество объектов можно разделить на два непересекающихся подмножества

- объекты-источники;
- объекты-данные

Определение 1.Объект O_i называется ***источником*** для субъекта S_m если существует субъект S_j, в результате воздействия которого на объект O_i возникает субъект S_m

S_j – *активизирующий* субъект для субъекта S_m

S_m – *порожденный* субъект

$Create(S_j, O_i) \rightarrow S_m$

Функционирование КС – ***нестационарный*** процесс, но в субъектно-объектной модели КС действует ***дискретное время*** t_i. В любой момент времени t_i множество субъектов, объектов-источников, объектов-данных ***фиксировано!!!***

Определение 2.Объект в момент времени t_k ***ассоциирован*** с субъектом , если состояние объекта O_i повлияло на состояние субъекта S_m в след. момент времени t_{k+1}. (т.е. субъект S_m использует информацию, содержащуюся в объекте O_i).

Можно выделить: - множество ***функционально-ассоциированных объектов***

- множество ***ассоциированных объектов-данных*** с субъектом S_m в момент времени t_k

Следствие 2.1. В момент порождения объект-источник является ассоциированным с порожденным субъектом

1.Понятие политики и моделей безопасности информации в КС

Определение 3.***Потоком*** информации между объектом O_i и объектом O_j называется произвольная операция над объектом O_j, осуществляемая субъектом S_m, и зависящая от объекта O_i

$$Stream(S_m, O_i) \rightarrow O_j$$

– потоки информации м.б. только между объектами (а не между субъектом и объектом)

– объекты м.б. как ассоциированы, так и не ассоциированы с субъектом S_m

– операция порождения потока локализована в субъекте и сопровождается изменением состояния ассоциированных (отображающих субъект) объектов

– операция ***Stream*** может осуществляться в виде "*чтения*", "*записи*", "*уничтожения*", "*создания*" объекта

Определение 4.***Доступом*** субъекта к объекту O_j называется порождение субъектом S_m потока информации между объектом O_j и некоторым(и) объектом O_i (в т.ч., но не обязательно, объект O_i ассоциирован с субъектом S_m)

Будем считать, что все множество потоков информации P (объединение всех потоков во все t_k) разбито на два подмножества

- множество потоков P_L, характеризующих ***легальный доступ***
- множество потоков P_N, характеризующих ***несанкционированный доступ***

Определение 5.***Правила разграничения доступа***, задаваемые политикой безопасности, есть формально описанные потоки, принадлежащие множеству P_L.

1.Понятие политики и моделей безопасности информации в КС

Аксиомы защищенности компьютерных систем

Аксиома 1. В любой момент времени любой субъект, объект (процесс, файл, устройство) д.б. ***идентифициро- ваны*** и ***аутентифицированы***

Аксиома 2. В защищенной системе должна присутствовать активная компонента (субъект, процесс и объект-источник), осуществляющая *контроль процессов субъектов над объектами*

Аксиома 3. Для осуществления процессов субъектов над объектами необходима (должна существовать) *дополнительная информация* (и наличие содержащего ее объекта), помимо информации идентифицирующей субъекты и объекты

Аксиома 4. Все вопросы безопасности информации в КС описываются *доступами субъектов к объектам*

Аксиома 5. Субъекты в КС могут быть порождены только активной компонентой (субъектами же) из объектов

Аксиома 6. Система безопасна, если субъекты не имеют возможности нарушать (обходить) правила и ограничения ПБ

!!!Оси критерий безопасности

Политики безопасности компьютерных систем

Политика *избирательного* (*дискреционного*) доступа

- множество P_L задается явным образом внешним по отношению к системе фактором в виде указания дискретного набора троек "субъект-поток(операция)-объект"

Политика *полномочного* (*мандатного*) доступа

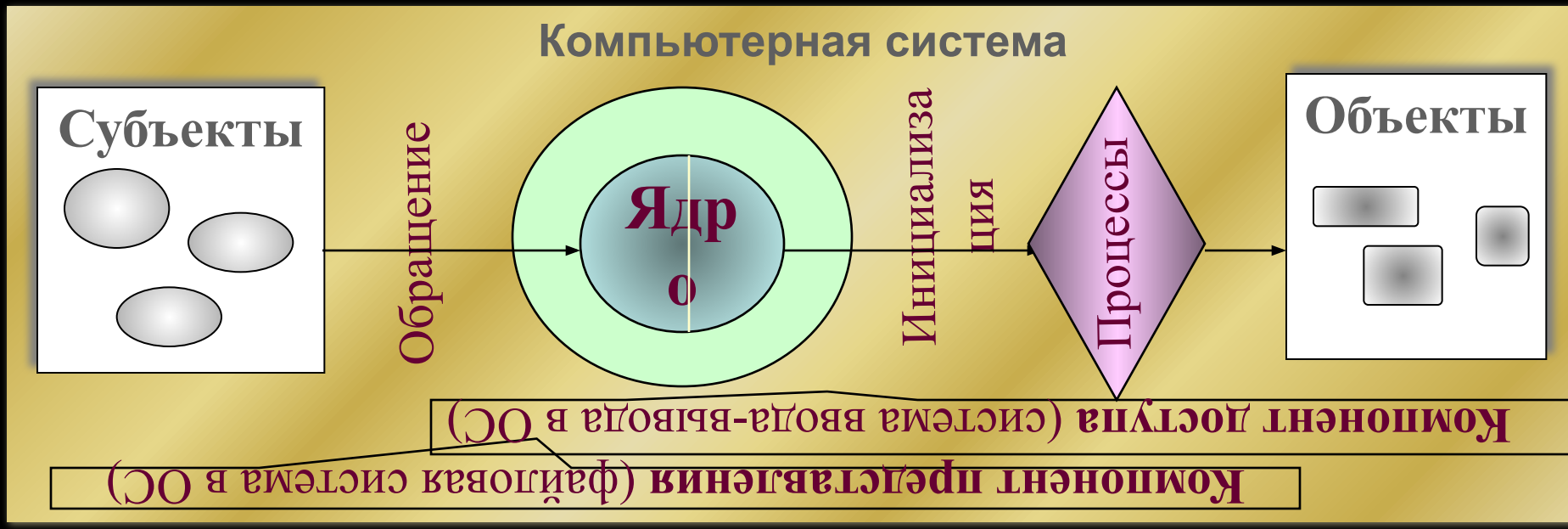
- множество P_L задается неявным образом через предоставление субъектам неких полномочий (допуска, мандата) порождать определенные потоки над объектами с определенными характеристиками конфиденциальности (метками, грифами секретности)

Политика *ролевого* (*типизованного*) доступа

- множество P_L задается через введение в системе дополнительных абстрактных сущностей – ролей, с которыми ассоциируются конкретные пользователи, и наделение ролевых субъектов доступа на основе дискреционного или мандатного принципа правами доступа к объектам системы

2. Монитор (ядро) безопасности КС

Структура КС в программно-техническом аспекте

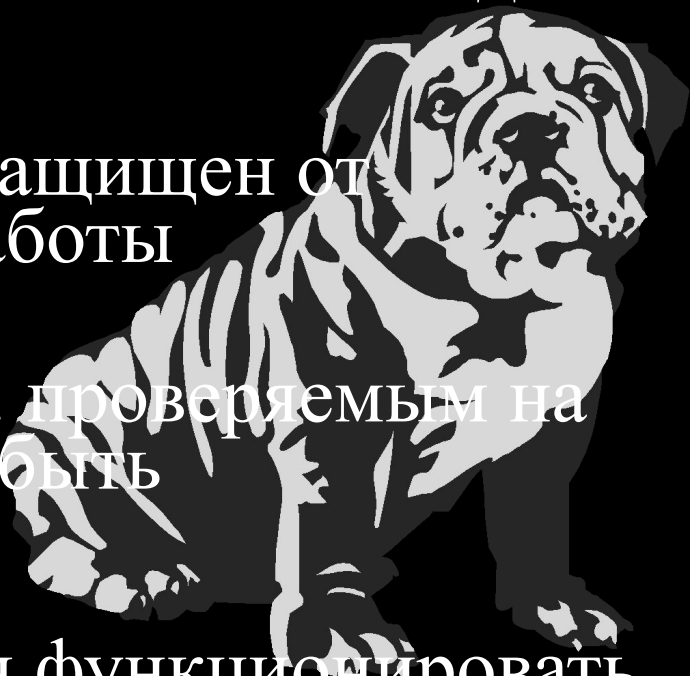


2. Монитор (ядро) безопасности КС

Монитор безопасности реализует политику безопасности на основе той или иной модели безопасности

Требования к монитору безопасности

Полнота - монитор должен вызываться при каждом обращении субъектов за сервисом к ядру системы и не д.б. никаких способов его обхода



Изолированность - монитор д.б. защищен от отслеживания и перехвата своей работы

Верифицируемость - монитор д.б. проверяемым на выполнение своих функций, т.е. быть тестируемым (самотестируемым)

Непрерывность - монитор должен функционировать при любых штатных и нештатных (в т.ч. и в аварийных) ситуациях

2. Монитор (ядро) безопасности КС

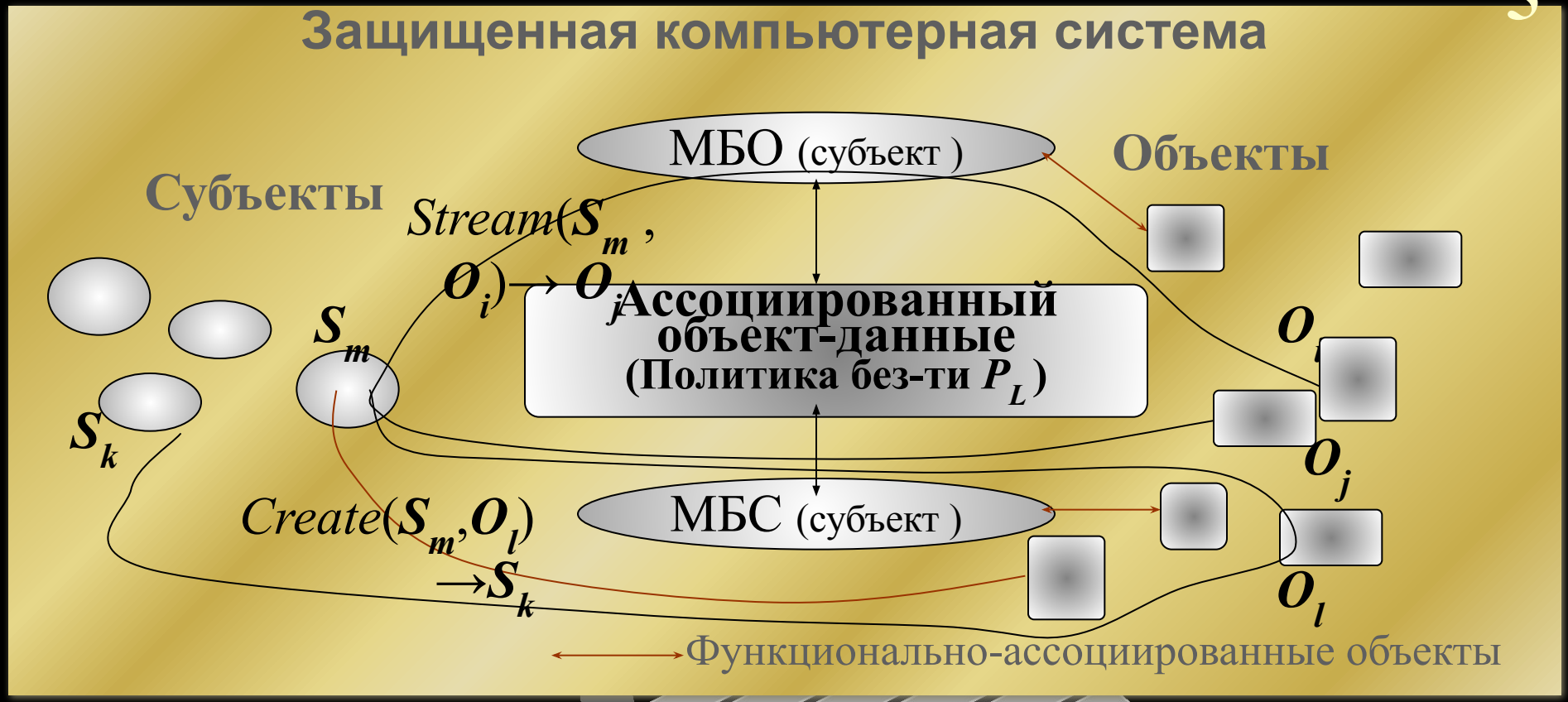
Особенности субъектно-объектной модели КС (определения 1, 2, 3 и 4) требуют структуризации монитора безопасности на две компоненты:

- **монитор безопасности объектов (*МБО*)**
- **монитор безопасности субъектов (*МБС*)**

Определение 6.***Монитором безопасности объектов*** **(*МБО*)** называется субъект, активизирующийся при возникновении потока между любыми объектами, порождаемым любым субъектом, и разрешающий только те потоки, которые принадлежат множеству P_L

Определение 7.***Монитором безопасности субъектов*** **(*МБС*)** называется субъект, активизирующийся при любом порождении субъектов, и разрешающий порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и объектов-источников

2. Монитор (ядро) безопасности КС



Гарантии выполнения политики безопасности обеспечиваются определенными требованиями к МБО и МБС, реализующими т.н. *изолированную программную среду* (*ИПС*)

3. Гарантирование выполнения политики безопасности. ИПС.

Исх. тезис -

при изменении объектов, функционально ассоциированных с субъектом монитора безопасности могут измениться свойства самого МБО и МБС, что м. привести к нарушению ПБ

Определение 8. Объекты O_i и O_j ***тождественны*** в момент времени t_k, если они совпадают как слова, записанные на одном языке

Определение 9. Субъекты S_i и S_j ***тождественны*** в момент времени t_k, если попарно тождественны все соответствующие ассоциированные с ними объекты

Следствие 9.1. Порожденные субъекты тождественны, если тождественны порождающие их субъекты и объекты-источники

Определение 10. Субъекты S_i и S_j называются ***невлияющими*** друг на друга (или ***корректными*** относительно друг друга), если в любой момент времени отсутствует поток (изменяющий состояние объекта) между любыми объектами O_i и O_j, ассоциированными соответственно с субъектами S_i и S_j, причем O_i не ассоциирован с S_j, а O_j не ассоциирован с S_i

(Изменение состояние объекта – не тождественность в соотв. моменты времени)

3. Гарантирование выполнения политики безопасности. ИПС.

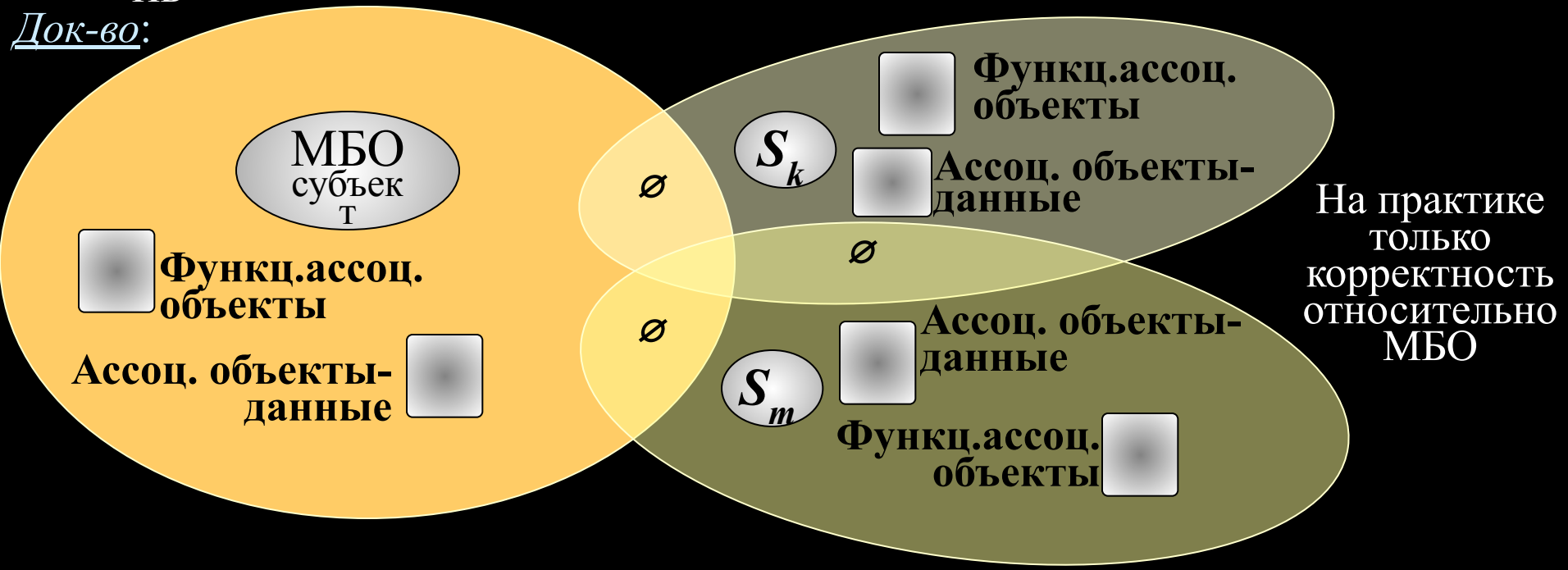
Определение 11. Субъекты S_i и S_j называются ***абсолютно невлияющими*** друг на друга (или ***абсолютно корректными*** относительно друг друга), если дополнительно к условию определения 10 множества ассоциированных объектов указанных субъектов не имеют пересечений

Утверждение 1. ПБ гарантированно выполняется в КС, если:

- МБО разрешает порождение потоков только из P_L;
- все существующие в КС субъекты абсолютно корректны относительно МБО и друг друга

Достаточное условие гарантированного выполнения ПБ

Док-во:



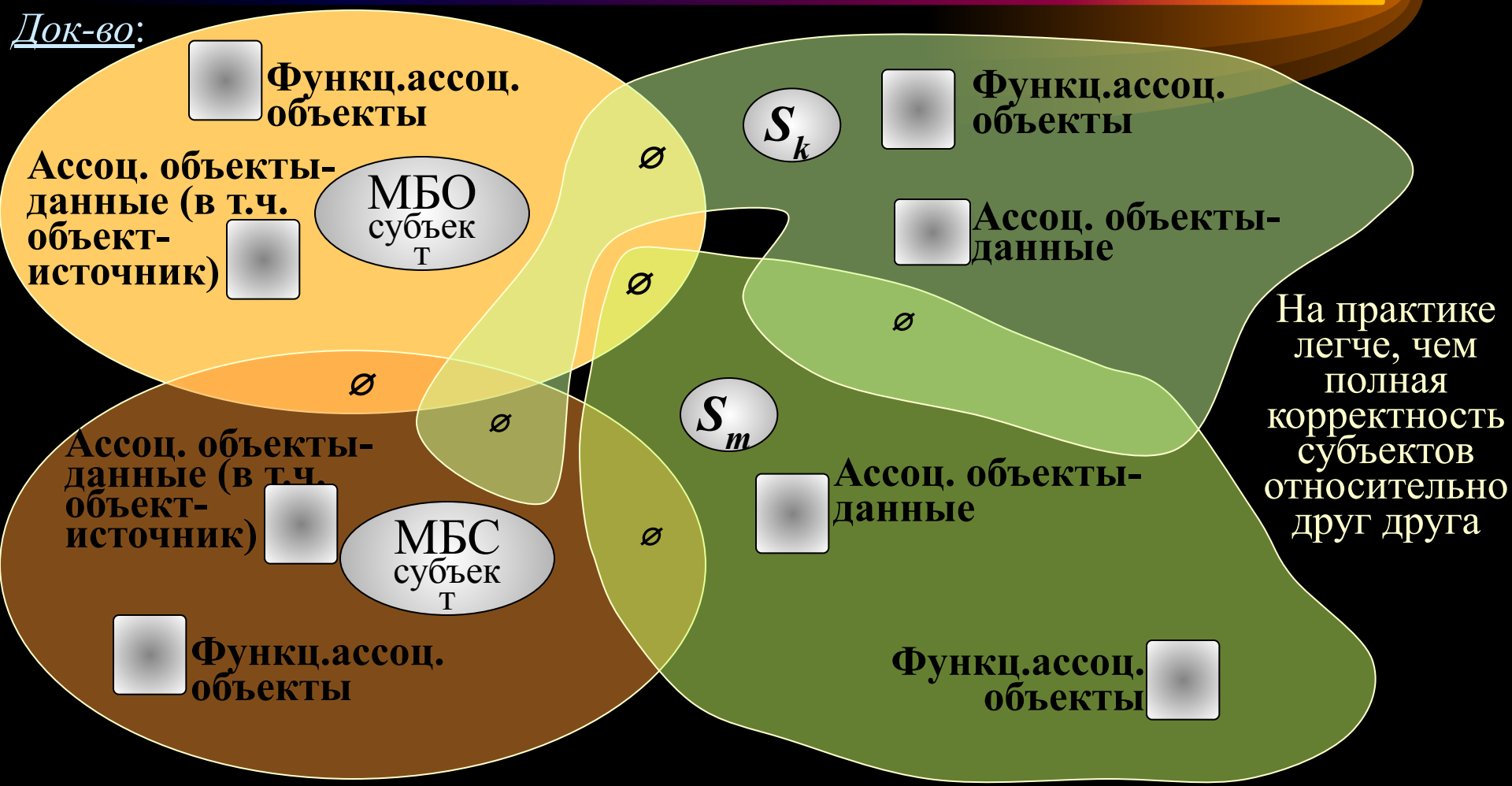
На практике только корректность относительно МБО

3. Гарантирование выполнения политики безопасности. ИПС.

Утверждение 2. Если в абсолютно изолированной КС существует МБО и порождаемые субъекты абсолютно корректны относительно МБО, а также МБС абсолютно корректен относительно МБО, то в КС реализуется доступ, описанный правилами разграничения доступа (ПБ)

Достаточное условие гарантированного выполнения ПБ

Док-во:



3. Гарантирование выполнения политики безопасности. ИПС.

Определение 12. КС называется ***замкнутой по порождению субъектов***, если в ней действует МБС, разрешающий порождение только фиксированного конечного подмножества субъектов для любых объектов-источников при фиксированной декомпозиции КС на субъекты и объекты

Определение 13. Множество субъектов КС называется ***изолированным (абсолютно изолированным)***, если в ней действует МБС и субъекты из порождаемого множества корректны (абсолютно корректны) относительно друг друга и МБС

Называют "изолированной программной средой (ИПС)

Следствие 13.1. Любое подмножество субъектов изолированной (абсолютно изолированной) КС, включающее МБО и МБС, также составляет изолированную (абсолютно изолированную) программную среду

Следствие 13.2. Дополнение изолированной (абсолютно изолированной) КС субъектом, корректным (абсолютно корректным) относительно любого из числа входящих в ИПС субъектов, оставляет КС изолированной (абсолютно изолированной)

3. Гарантирование выполнения политики безопасности. ИПС.

Определение 16. Операция порождения субъекта $Create(S_i, O_j) \rightarrow S_m^0$ называется ***порождением с контролем неизменности объекта***, если для любого момента времени $t_k > t_0$, в который активизирована операция ***Create***, порождение субъекта S_m возможно только при тождественности объектов в соответствующие моменты времени – $O_j[t_k] = O_j[t_0]$

Следствие 16.1. При порождении с контролем неизменности объектов субъекты, порожденные в различные моменты времени, тождественны $S_m[t_1] = S_m[t_2]$. При $t_1 = t_2$ порождается один и тот же субъект.

Утверждение 3. Если в момент времени t_0 в изолированной КС действует только порождение субъектов с контролем неизменности объекта и существуют потоки между объектами через субъекты, не противоречащие условию корректности (абсолютной корректности) субъектов, то в любой момент времени КС также остается изолированной (абсолютно изолированной).

Базовая Теорема ИПС

Док-во: ***1.*** Из условия абс. корр. м.б. только такие потоки, которые изменяют состояние объектов, не ассоциированных в соотв. моменты времени с каким-либо субъектом. Отсюда не м.б. изменены объекты-источники.

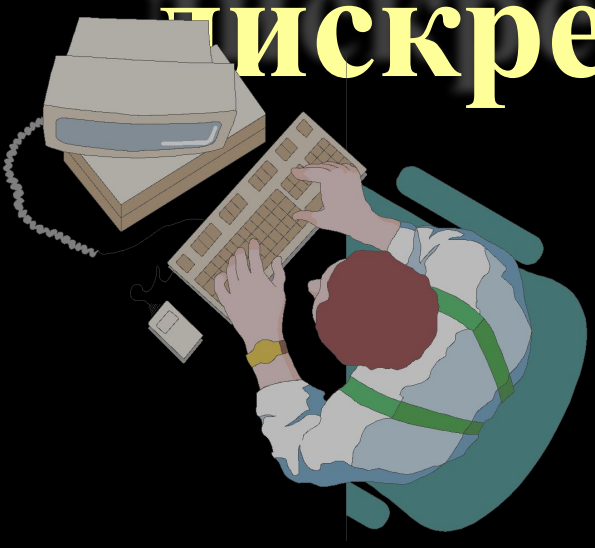
2. Т.к. объекты-источники остаются неизменными, то мощность множества порождаемых субъектов нерасширяемо, и тем самым множество субъектов КС остается изолированным

Проблемы реализации *Изолированной программной среды*

- повышенные требования к вычислительным ресурсам – ***проблема производительности***
- нестационарность функционирования КС (особенно в нач. момент времени) из-за изменения уровня представления объектов (сектора-файлы) – ***проблема загрузки (начального инициирования) ИПС***
- сложность технической реализацией контроля неизменности объектов - ***проблема целостности объектов*** и ***проблема чтения реальных данных***

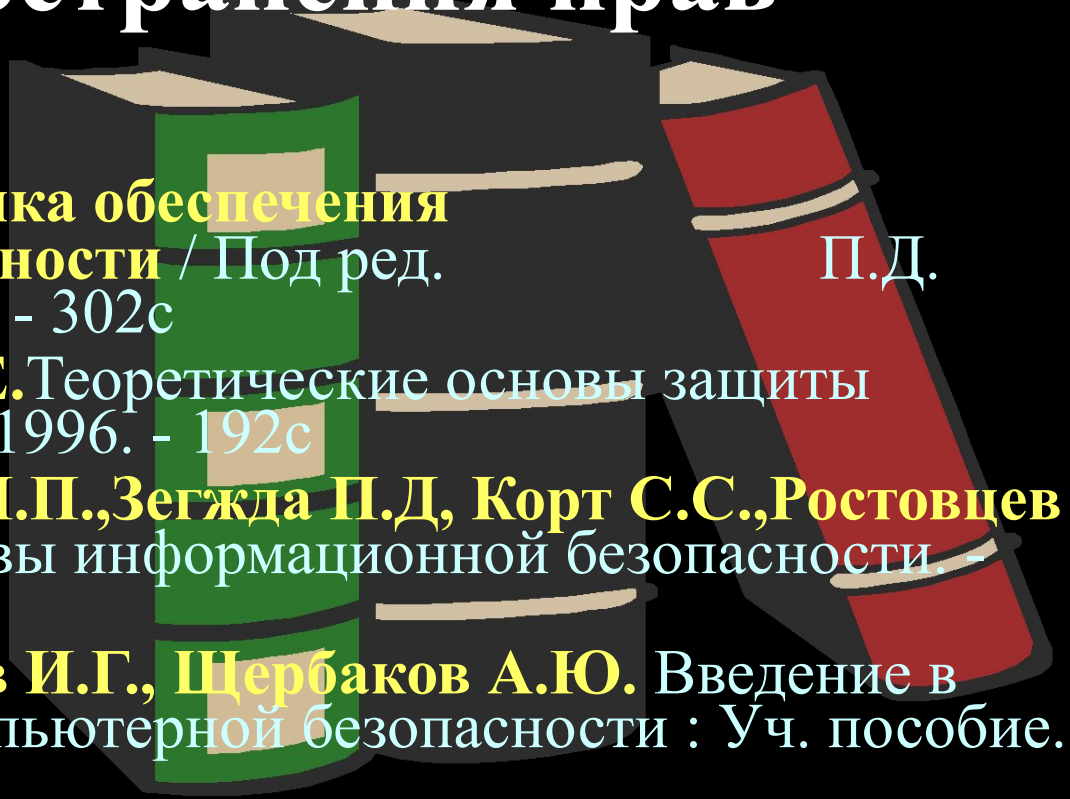
Лекция 2.1.

Модели безопасности на основе дискреционной политики



Учебные вопросы:

1. Общая характеристика политики дискреционного доступа
2. Пятимерное пространство Хартсона
3. Модели на основе матрицы доступа
4. Модели распространения прав доступа



Литература:

1. **Теория и практика обеспечения информационной безопасности** / Под ред. П.Д. Зегжды. М.:Яхтсмен, 1996. - 302с

2. **Грушо А.А.,Тимонина Е.Е.** Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с

3. **Баранов А.П.,Борисенко Н.П.,Зегжда П.Д, Корт С.С.,Ростовцев А.Г.** Математические основы информационной безопасности. - Орел, ВИПС, 1997.- 354с.

4. **Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю.** Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998.- 184с.

1. Общая характеристика политики дискреционного доступа

Исходные понятия

Разграничение доступа к информации (данным) КС

-разделение информации АИС на объекты (части, элементы, компоненты и т. д.), и организация такой системы работы с информацией, при которой пользователи имеют доступ только и только к той части информации (к тем данным), которая им необходима для выполнения своих функциональных обязанностей или необходима исходя из иных соображений

-создание такой системы организации данных, а также правил и механизмов обработки, хранения, циркуляции данных, которые обеспечивают функциональность КС и безопасность информации (ее конфиденциальность, целостность и доступность)

Доступ к информации (данным)

-действия субъектов на объектами КС, вызывающие одно- двунаправленные информационные потоки

Методы доступы

-виды действий (операций) субъектов над объектами КС (чтение/просмотр, запись/модификация/добавление, удаление, создание, запуск и т.п.)

Права доступа

-методы доступа (действия, операции), которыми обладают (наделяются, способны выполнять) субъекты над объектами КС

Политика (правила) разграничения доступа

-совокупность руководящих принципов и правил наделения субъектов КС правами доступа к объектам, а также правил и механизмов осуществления самих доступов и реализации информационных потоков

1. Общая характеристика политики дискреционного доступа

Виды политик (правил, механизмов) разграничения доступа

Политика дискреционного разграничения доступа

-разграничение доступа на основе *непосредственного* и *явного предоставления* субъектам *прав* доступа к объектам в виде троек «субъект-операция-объект»

Политика мандатного разграничения доступа

-предоставление прав доступа субъектов к объектам *неявным образом* посредством присвоения уровней (меток) безопасности объектам (*гриф конфиденциальности, уровень целостности*), субъектам (*уровень допуска/полномочий*) и организация доступа на основе соотношения «уровень безопасности субъекта-операция-уровень безопасности объекта»

Политика тематического разграничения доступа

-предоставление прав доступа субъектам к объектам *неявным образом* посредством присвоения тематических категорий объектам (*тематические индексы*) и субъектам (*тематические полномочия*) и организация доступа на основе соотношения «тематическая категория субъекта-операция-тематическая категория объекта»

Политика ролевого разграничения доступа

-агрегирование прав доступа к объектам в именованные совокупности (роли), имеющие определенный функционально-технологический смысл в предметной области КС, и наделение пользователей правом работы в КС в соответствующих ролях

Политика временно́го разграничения доступа

-предоставление пользователям прав работы в КС по определенному временному регламенту (по времени и длительность доступа)

Политика маршрутного доступа

-предоставление пользователям прав работы в КС при доступе по определенному маршруту (*с определенных рабочих станций*)

Общая характеристика политики дискреционного доступа

-множество легальных (неопасных) доступов P_L задается явным образом внешним по отношению к системе фактором в виде указания дискретного набора троек "субъект-поток(операция)-объект";

-права доступа предоставляются (*«прописываются» в специальных информационных объектах-стуктурах, ассоциированных с монитором безопасности*), отдельно каждому пользователю к тем объектам, которые ему необходимы для работы в КС;

-при запросе субъекта на доступ к объекту монитор безопасности, обращаясь к ассоциированным с ним информационным объектам, в которых «прописана» политика разграничения доступа, определяет «легальность» запрашиваемого доступа и разрешает/отвергает доступ

Модели и механизмы реализации дискреционного разграничения доступа

Различаются:

-в зависимости от принципов и механизмов программно-информационной структуры объекта(объектов), ассоциированных с монитором безопасности, в которых хранятся «прописанные» права доступа (тройки доступа)

-в зависимости от принципа управления правами доступа, т.е. в зависимости от того – кто и как заполняет/изменяет ячейки матрицы доступа (принудительный и добровольный принцип управления доступом)

Выделяют:

-теоретико-множественные (реляционные) модели разграничения доступа (пятимерное пространство Хартсона, модели на основе матрицы доступа)

-модели распространения прав доступа (модель Харисона-Рузо-Ульмана, модел типизованной матрицы доступа, теоретико-графовая модель TAKE-GRANT)

2. Пятимерное пространство Хартсона

Система защиты -пятимерное пространство на основе следующих множеств:

U - множество пользователей;
R - множество ресурсов;
E - множество операций над ресурсами;
S - множество состояний системы;
A - множество установленных полномочий.

Элементы множества A - a_{ijkl} специфицируют:
- ресурсы
- вхождение пользователей в группы;
- разрешенные операции для групп по отношению к ресурсам;

Декартово произведение $A \times U \times E \times R \times S$ - область безопасного доступа

Запрос пользователя на доступ представляет собой *4-х мерный кортеж*: $q = (u,e,R',s)$, где R' - требуемый набор ресурсов

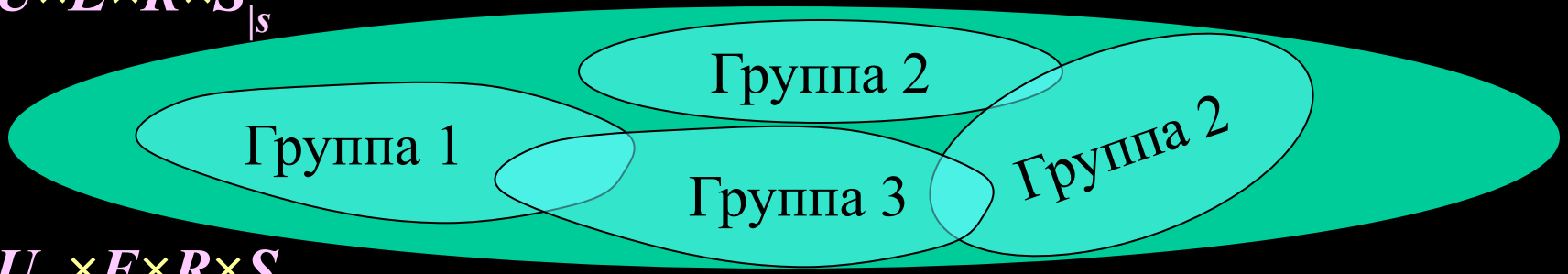
Процесс организации доступа по запросу осуществляется по следующему алгоритму:

1. Вызвать все вспомогательные программы для предварительного принятия решения

2. Определить те группы пользователей, в которые входит u, и выбрать из A те спецификации полномочий $P=F(u)$, которым соответствуют выделенные группы пользователей. Набор полномочий $P=F(u)$ определяет т.н. **привилегию пользователя**

2. Пятимерное пространство Хартсона

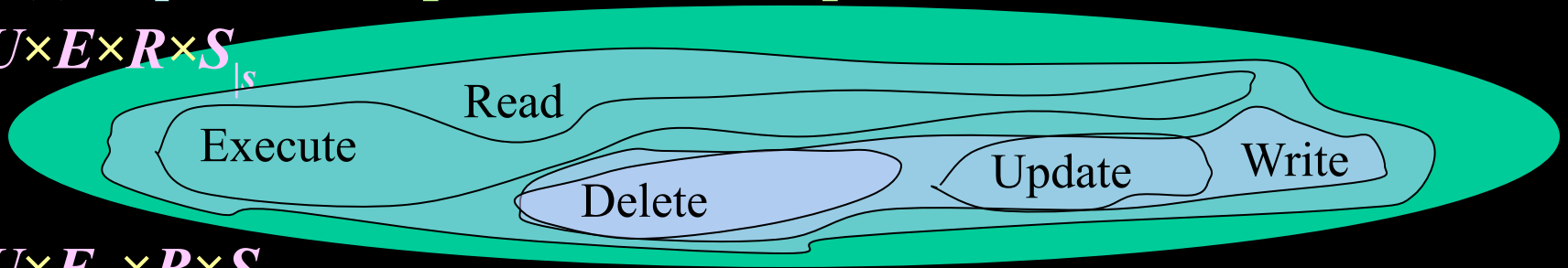
$A \times U \times E \times R \times S_{|s}$



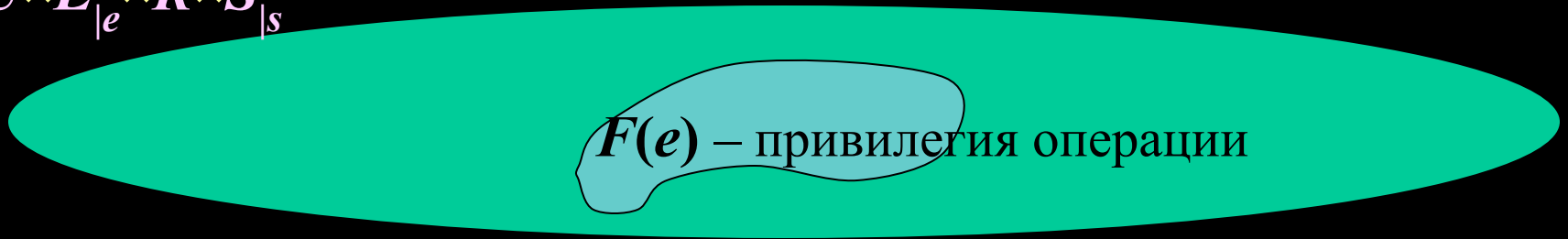
$A \times U_{|u} \times E \times R \times S_{|s}$

3. Определить из множества *A* набор полномочий ***P=F(e)***, которые устанавливают ***e***, как основную операцию. Набор полномочий ***P=F(e)*** определяет **привилегию операции**.

$A \times U \times E \times R \times S_{|s}$



$A \times U \times E_{|e} \times R \times S_{|s}$



2. Пятимерное пространство Хартсона

4. Определить из множества A набор полномочий $P=F(R')$, разрешающих доступ к набору ресурсов R'. Набор полномочий $P=F(R')$ определяет **привилегию ресурсов**.

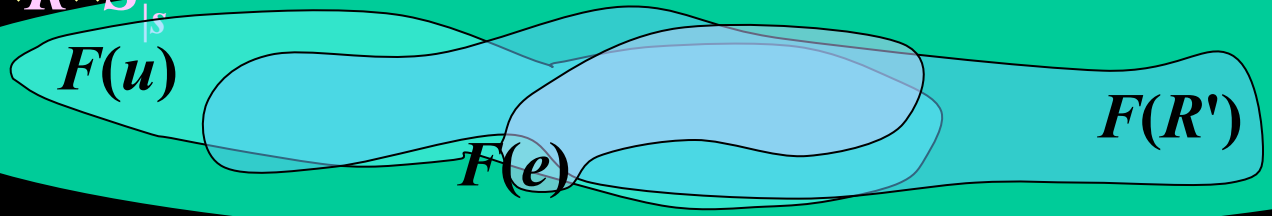
$A \times U \times E \times R_{|R'} \times S_{|S}$

$F(R')$ – привилегия запрашиваемых ресурсов

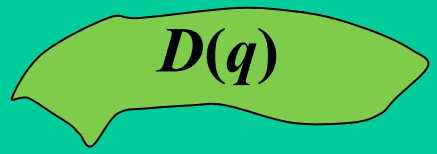
На основе $P=F(u)$, $P=F(e)$ и $P=F(R')$ образуется т.н. **домен полномочий запроса**:

$$D(q)= F(u) \cap F(e) \cap P=F(R')$$

$A \times U \times E \times R \times S_{|S}$



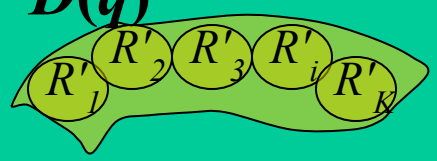
$A \times U_{|u} \times E_{|e} \times R_{|R'} \times S_{|S}$



2. Пятимерное пространство Хартсона

5. Убедиться, что запрашиваемый набор ресурсов R' полностью содержится в домене запроса $D(q)$, т.е. любой r из набора R' хотя бы один раз присутствует среди элементов $D(q)$.

$A \times U_{|u} \times E_{|e} \times R_{|R'} \times S_{|s}$

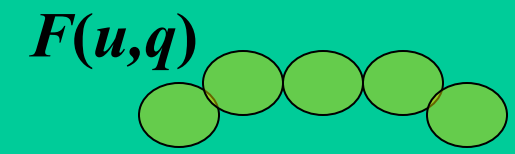


6. Осуществить разбиение $D(q)$ на эквивалентные классы, так, чтобы в один класс попадали полномочия (элементы $D(q)$), когда они специфицируют один и тот же ресурс r из набора R'.

В каждом классе произвести операцию логического **ИЛИ** элементов $D(q)$ с учетом типа операции e.

В результате формируется новый набор полномочий на каж-дую единицу ресурса, указанного в $D(q)$ - $F(u,q)$.Набор $F(u,q)$ назы-вается **привилегией пользователя** u **по отношению к запросу** q.

$A \times U_{|u} \times E_{|e} \times R_{|R'} \times S_{|s}$



2. Пятимерное пространство Хартсона

7. Вычислить условие фактического доступа (***EAC***), соответствующее запросу ***q*** , через операции логического **ИЛИ** по элементам полномочий ***F(u,q)*** и запрашиваемым ресурсам ***r*** из набора ***R'***, и получить тем самым набор ***R''*** - набор фактически доступных по запросу ресурсов

8. Оценить ***EAC*** и принять решение о доступе:
- разрешить доступ, если ***R''*** и ***R'*** полностью перекрываются;
- отказать в доступе в противном случае.

9. Произвести запись необходимых событий

10. Вызвать все программы, необходимые для организации доступа после "принятия решения".

11. Выполнить все вспомогательные программы, вытекающие для каждого случая по п.8.

12. При положительном решении о доступе завершить физическую обработку.

Но!!! Безопасность системы в строгом смысле не доказана

3. Модели на основе матрицы доступа

Система защиты -совокупность следующих множеств:

- множество исходных объектов $O\ (o_1,o_2,\ldots,o_M)$
- множество исходных субъектов $S\ (s_1,s_2,\ldots,s_N)$, при этом $S \subseteq O$
- множество операций (действий) над объектами $Op\ (Op_1,Op_2,\ldots,Op_L)$
- множество прав, которые м.б. даны субъектам по отношению к объектам $R\ (r_1,r_2,\ldots,r_K)$ – т.н. "общие права"
- NxM матрица доступа A, в которой каждому ***субъекту*** соответствует *строка*, а каждому ***объекту*** - ***столбец***. В ячейках матрицы располагаются права r соотв.субъекта над соотв. объектом в виде набора разрешенных операций Op_i

$A=$

Субъекты \ Объекты	o_1	o_2	. . .			o_M
s_1						
s_2						
				a_{ij}		
s_N						

$A[s_i,oj]= a_{ij}$ - право r из R (т. е. не общее, а конкр. право)

Каждый элемент прав r_k специфицирует совокупность операций над объектом

$r_k \sim (Op_{1k},Op_{2k},\ldots,Op_{Jk})$

3. Модели на основе матрицы доступа

Две разновидности моделей в зависимости от того, каким образом заполняются ячейки матрицы доступа *A*. Выделяют:

- ***системы с принудительным управлением доступа;***
- ***системы с добровольным управлением доступом.***

Принудительное управление доступом

- вводится т.н. доверенный субъект (администратор доступа), который и определяет доступ субъектов к объектам (централизованный принцип управления)
- в таких системах заполнять и изменять ячейки матрицы доступа может только администратор

Добровольное управление доступом

- вводится т.н. владение (владельцы) объектами и доступ субъектов к объекту определяется по усмотрению владельца (децентрализованный принцип управления)
- в таких системах субъекты посредством запросов могут изменять состояние матрицы доступа

3. Модели на основе матрицы доступа

Способы организации информационной структуры матрицы доступа

Централизованная единая информационная структура

Децентрализованная распределенная информационная структура

СУБД

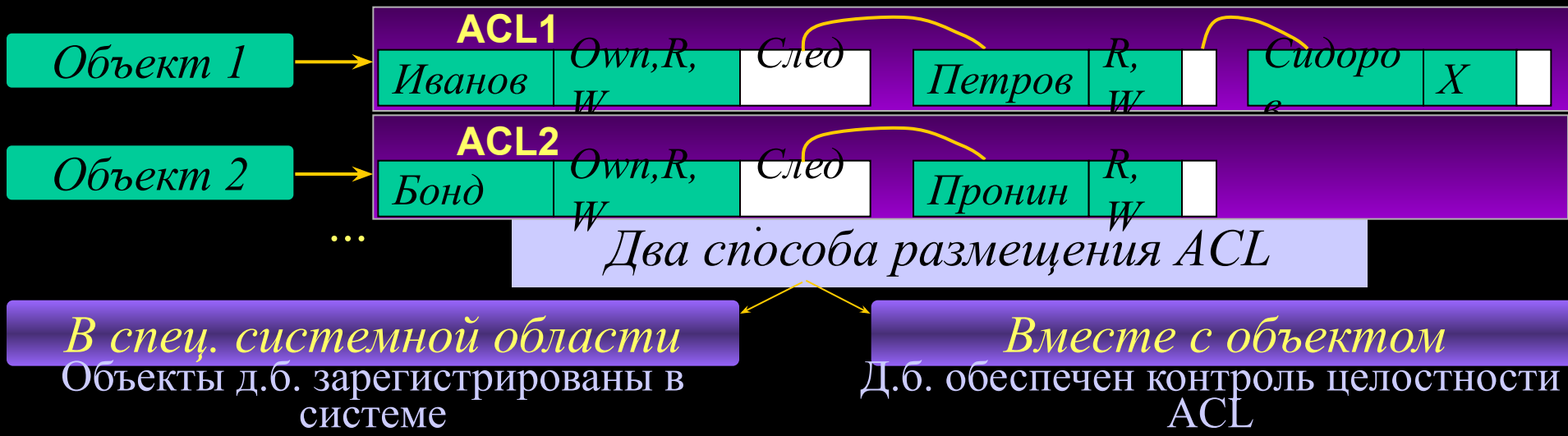
системная таблица с назначениями доступа

Биты защиты (UNIX)

	Владелец			*Группа*			*Остальные польз-ли*		
	Чтен ие	*Запис ь*	*Выпол нение*	*Чтен ие*	*Запис ь*	*Выпол нение*	*Чтен ие*	*Запис ь*	*Выпол нение*
Биты	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Объект									
Объект 2	1	1	0	1	1	0	1	0	0
…									

3. Модели на основе матрицы доступа

Списки доступа в файловой системе ОС Windows (Access Control List – ACL)



Структура списков доступа на примере NTFS

С каждым объектом *NTFS* связан т.н. дескриптор защиты, состоящий из:

ID влад.	*ID перв. гр. влад.*	*DACL*	*SACL*

Список дискр. контроля доступа

Список контроля доступа

DACL – последовательность произв. кол-ва *элементов контроля доступа – ACE, вида:*

Allowed / Denied	*ID субъекта (польз., группа)*	*Права доступа (отображ-е)*	*Флаги, атрибуты*

SACL – данные для генерации сообщений аудита

4.Модели распространения прав доступа. 4.1.Модель Харрисона-Руззо-Ульмана (модель HRU)

Наиболее типичный представитель систем с добровольным управлением доступом - ***модель Харрисона-Руззо-Ульмана***

Разработана для исследования дискреционной политики

В модели ***Харрисона-Руззо-Ульмана*** помимо элементарных операций доступа ***Read***, ***Write*** и т.д., вводятся также т.н. **прими-тивные операции** Op_k по ***изменению*** субъектами матрицы доступа:

- ***Enter r into (s,o)*** - ввести право ***r*** в ячейку ***(s,o)***
- ***Delete r from (s,o)*** - удалить право ***r*** из ячейки ***(s,o)***
- ***Create subject s*** - создать субъект ***s*** (т.е. новую строку матрицы ***A***)
- ***Create object o*** - создать объект ***o*** (т.е. новый столбец матрицы ***A***)
- ***Destroy subject s*** - уничтожить субъект ***s***
- ***Destroy object o*** - уничтожить объект ***o***

Состояние системы *Q* изменяется при выполнении команд $C(\alpha_1, \alpha_2, \ldots)$, изменяющих состояние матрицы доступа *A*. Команды инициируются пользователями-субъектами

Структура команды

Название
[Условия] (необяз.)
Операции

Command $\alpha(x_1, \ldots x_k)$
if r_1 in $A[s_1,o_1]$ and r_2 in $A[s_2,o_2]$ …
then; Op_2 ; …;
end

x_i – идентификаторы задействованных субъектов или объектов

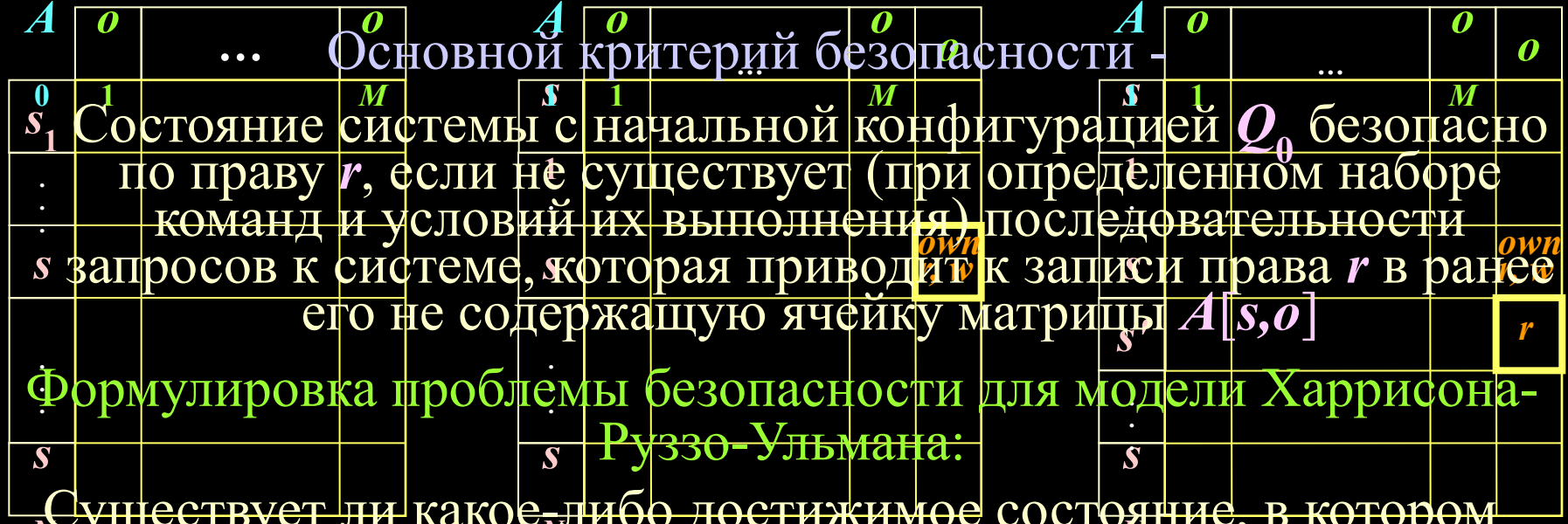
Команды с одной операцией – **монооперационные**, с одним условием - **моноусловные**

4. Модели распространения прав доступа. 4.1. Модель Харрисона-Руззо-Ульмана (модель HRU)

Примеры команд -

Command "создать файл"(*s, f*):
Create object f ;
Enter "own" into (*s, f*) ;
Enter "read" into (*s, f*) ;
Enter "write" into (*s, f*);
end

Command «ввести право чтения"(*s,s',f*):
if *own* ⊆ (*s, f*) ;
then
Enter r "read" into (*s', f*) ;
end



Основной критерий безопасности - Состояние системы с начальной конфигурацией Q_0 безопасно по праву *r*, если не существует (при определенном наборе команд и условий их выполнения) последовательности *s* запросов к системе, которая приводит к записи права *r* в ранее его не содержащую ячейку матрицы *A*[*s,o*]

Формулировка проблемы безопасности для модели Харрисона-Руззо-Ульмана:

Существует ли какое-либо достижимое состояние, в котором конкретный субъект обладает конкретным правом доступа к конкретному объекту? (т.е. всегда ли возможно построить такую последовательность запросов при некоторой исходной конфигурации когда изначально субъект этим правом не обладает?)

4.Модели распространения прав доступа. 4.1.Модель Харрисона-Руззо-Ульмана (модель HRU)

Харрисон, Руззо и Ульман показали :

Теорема 1. Проблема безопасности разрешима для ***моно-операционных*** систем, т.е. для систем которых запросы содержат лишь одну примитивную операцию

Док-во на основе моделирования системы машиной Тьюринга

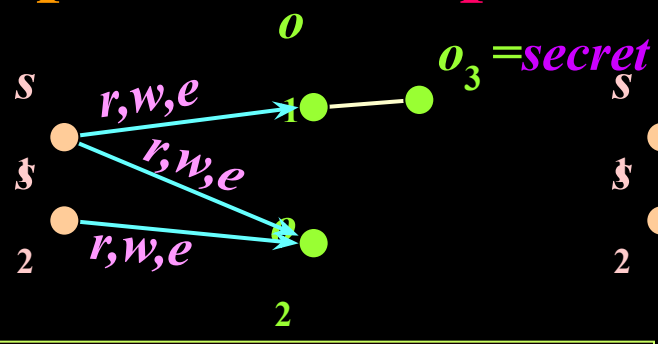
Теорема 2. Проблема безопасности неразрешима в общем случае

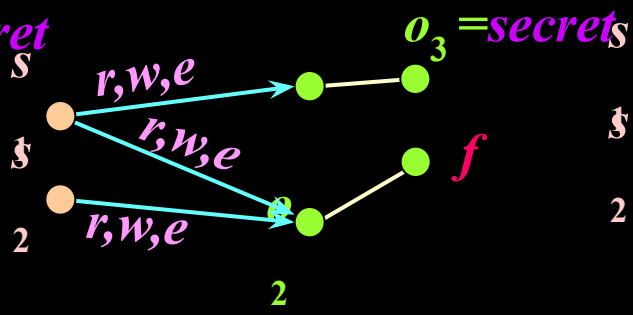
Выводы по модели Харрисона-Руззо-Ульмана:

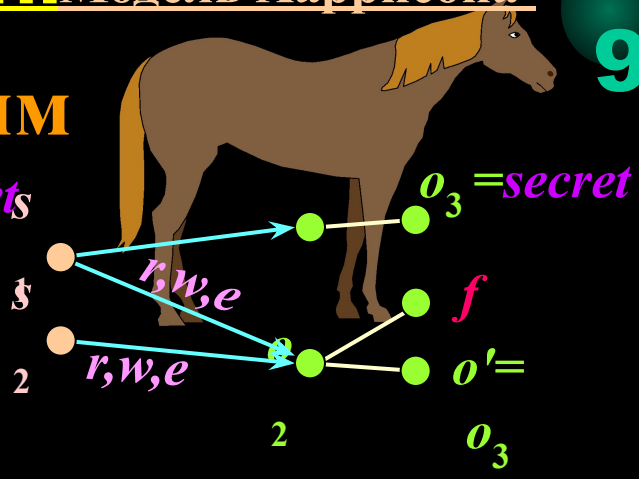
-данная модель в ее полном виде позволяет реализовать множество политик безопасности, но при этом проблема безопасности становится неразрешимой

-разрешимость проблемы безопасности только для монооперационных систем приводит к слабости такой модели для реализации большинства политик безопасности (т.к. нет операции автоматического наделения своими правами дочерних объектов, ввиду чего по правам доступа они изначально не различимы)

Проблема «троянских» программ



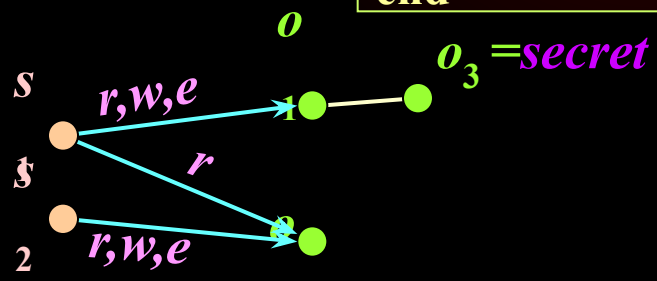




Command "создать файл" (s_2,f):
 if *write* ∈ [s_2, o_2] ;
 then
  Create object f ;
  Enter "read" into [s_2, f] ;
  Enter "write" into [s_2, f] ;
  Enter "execute" into [s_2, f];
 if *read* ∈ [s_1, o_2] ;
  then
  Enter "read" into [s_1, f] ;
 if *write* ∈ [s_1, o_2] ;
  then
  Enter "write" into [s_1, f] ;
 if *execute* ∈ [s_1, o_2] ;
  then
  Enter "execute" into [s_1, f] ;
end

Command "запустить файл"(s_1, f):
 if *execute* ∈ [s_1, f] ;
  then
  Create subject f' ;
  Enter "read" into [f',o_1];
  Enter "read" into [f',o_3];
 if *write* ∈ [s_1,o_2] ;
  then
  Enter "write" into [f',o_2];
end

Command "скопировать файл o_3 программой f' в o_2" (f',o_3, o_2):
 if *read* ∈ [f', o_3] and
  write ∈ [f', o_2]
  then
  Create object o';
  Write (f', o_3, o');
 if *read* ∈ [s_2, o_2] ;
  then
  Enter "read" into [s_2,o'];
end



Расширения модели HRU

Типизованная матрица доступа (Модель TAM) R. Sandhu,1992г.

Вводится фиксированное количество типов τ_k (например, "user"- пользователь, 'so"-офицер безопасности и "file"), которым могут соответствовать сущности КС (субъекты и объекты).

Command $\alpha(x_1:\tau_1, x_2:\tau_2,\ldots, x_k: \tau_k)$

Накладываются ограничения на условия и соответствие типов в монотонных операциях (порождающие сущности)

Смягчаются условия на разрешимость проблемы безопасности

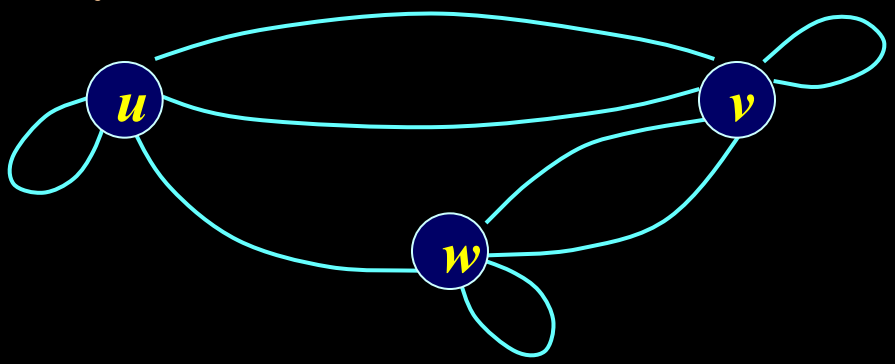
Анализ проблем безопасности в модели TAM основывается на понятии родительских и дочерних типов

Определение 1. *Тип τ_k является **дочерним** типом в команде создания $\alpha(x_1:\tau_1, x_2:\tau_2,\ldots, x_k:\tau_k)$, если и только если имеет место один из следующих элементарных операторов: **"Create subject x_k of type τ_k"** или **"Create object x_k of type τ_k"**. В противном случае тип τ_k является **родительским** типом.*

Вводится **Граф** отношений наследственности

4.Модели распространения прав доступа. 4.2.Модель типизованной матрицы доступа (модель TAM)

Пусть имеется три типа *u*, *v*, *w*



Функционирование системы осуществляется через последовательность следующих команд:

0-й шаг – в системе имеется субъект типа *u* - $(s_1{:}u)$

1-й шаг. $\alpha(s_1{:}u, s_2{:}w, o_1{:}v)$:
Create object o_1 *of type v* ;
Inter r into $[s_1, o_1]$;
Create subject s_2 *of type w* ;
Inter r' into $[s_2, o_1]$;
end

2-й шаг. $\alpha(s_3{:}u, o_1{:}v)$:
Create subject s_3 *of type u* ;
Inter r'' into $[s_3, o_1]$;
end

v – дочерний тип в команде **α**, в теле которой имеются еще типы *u*, *w*. Т. о. в **Графе отношений наследственности** возникают дуги (*u*,*v*), (*w*,*v*) и в т.ч. (*v*,*v*)

w – дочерний тип в команде **α**, в теле которой имеются еще типы *u*, *v*. Т. о. в **Графе отношений наследственности** возникают дуги (*u*,*w*), (*v*,*w*) и в т.ч. (*w*,*w*)

u – дочерний тип в команде **α**, в теле которой имеются еще тип *v*. Т.о. возникают дуги (*v*,*u*) и в т.ч. (*u*,*u*)

4.Модели распространения прав доступа. 4.2.Модель типизованной матрицы доступа (модель TAM)

Также, как и в модели **HRU**, используется понятие монотонной (**MTAM**) системы, которая не содержит примитивных операторов ***Delete*** и ***Destroy***.

Определение 2. *Реализация **MTAM** является **ациклличной** тогда и только тогда, когда ее граф отношений наследственности не содержит циклов*

Теорема 3. Проблема безопасности разрешима для ***ациклличных реализаций MTAM***

4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

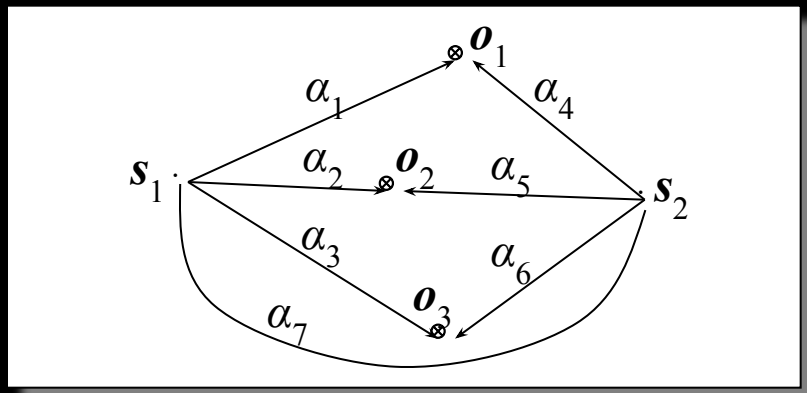
Джонс, Липтон, Шнайдер, 1976г.

Теоретико-графовая модель анализа распространения прав доступа в дискреционных системах на основе матрицы доступа

1.Также как и в модели HRU **система защиты** представляет совокупность следующих множеств:

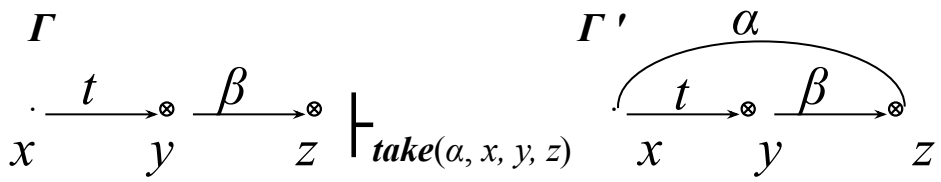
- множество исходных объектов $O\ (o_1,o_2,\ldots,o_M)$
- множество исходных субъектов $S\ (s_1,s_2,\ldots,s_N)$, при этом $S \subseteq O$
- множество прав, которые м.б. даны субъектам по отношению к объектам $(r_1,r_2,\ldots,r_K) \cup \{t, g\}$, в том числе с двумя специфическими правами – правом ***take*** (t – *право брать права доступа у какого-либо объекта по отношению к другому объекту*) и правом ***grant*** (g – *право предоставлять права доступа к определенному объекту другому субъекту*)

-множеством E установленных прав доступа (x, y, α) субъекта x к объекту y с правом α из конечного набора прав. При этом состояние системы представляется **Графом доступов** Γ



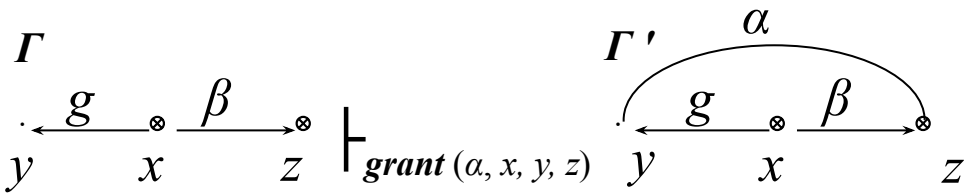
2.Состояние системы (**Графа доступов**) изменяется под воздействием элементарных команд 4-х видов

Команда "*Брать*" – *take*(*α, x, y, z*)



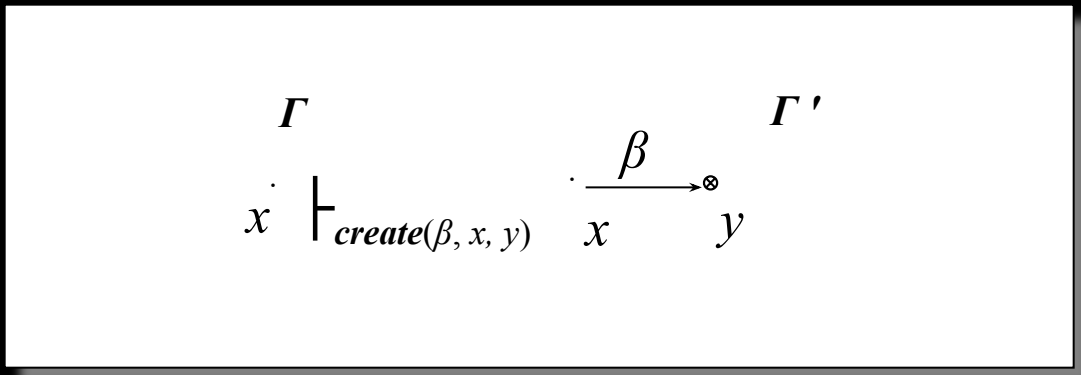
субъект ***x*** берет права доступа $\alpha \subseteq \beta$ на объект ***z*** у объекта ***y*** (обозначения: $\vdash_c$ – переход графа ***Г*** в новое состояние ***Г'*** по команде ***c*** ; $x \in S$; $y, z \in O$)

Команда «*Давать*" – *grant*(*α, x, y, z*)



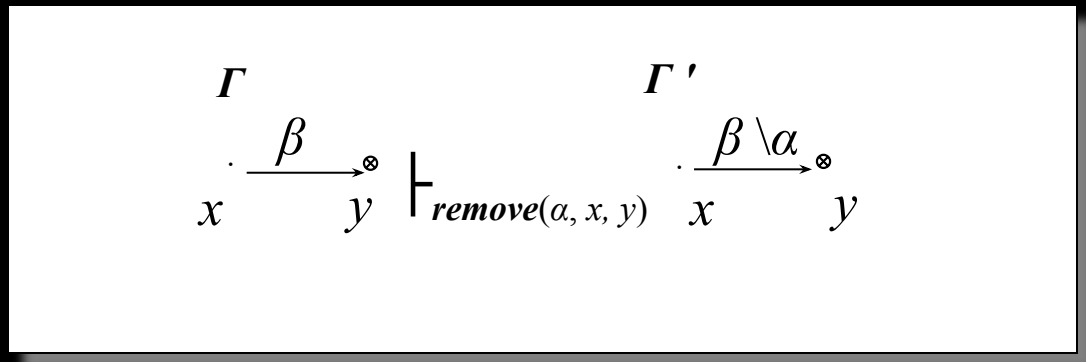
субъект ***x*** дает объекту ***y*** право $\alpha \subseteq \beta$ на доступ к объекту ***z***

Команда "*Создать*" – *create*(*β*, *x*, *y*)



субъект ***x*** создает объект ***y*** с правами доступа на него ***β*** ⊆ ***R*** (***y*** – новый объект, ***O'=O*** ∪ {***y***}), в т. ч. с правами ***t***, или ***g***, или {***t***, ***g***}.

Команда «*Изъять*" – *remove*(*α*, *x*, *y*)



субъект ***x*** удаляет права доступа ***α*** ⊆ ***β*** на объект ***y***

4. Модели распространения прав доступа. 4.4. Теоретико-графовая модель TAKE-GRANT

3. Безопасность системы рассматривается с точки зрения возможности получения каким-либо субъектом прав доступа к определенному объекту (в начальном состоянии $\Gamma_0 (O_0, S_0, E_0)$ такие права отсутствуют) при определенной кооперации субъектов путем последовательного изменения состояния системы на основе выполнения элементарных команд. Рассматриваются две ситуации – условия санкционированного, т.е. законного получения прав доступа, и условия «похищения» прав доступа

3.1. *Санкционированное получение прав доступа*

Определение **3**. *Для исходного состояния системы* $\Gamma_0 (O_0, S_0, E_0)$ *и прав доступа* $\alpha \subseteq R$ *предикат "**возможен доступ**(α, x, y, Γ_0)" является истинным тогда и только тогда, когда существуют графы доступов системы* $\Gamma_1 (O_1, S_1, E_1)$, $\Gamma_2 (O_2, S_2, E_2)$, ..., $\Gamma_N (O_N, S_N, E_N)$, *такие, что:*
$\Gamma_0 (O_0, S_0, E_0) \vdash_{c_1} \Gamma_1 (O_1, S_1, E_1) \vdash_{c_2} \ldots \vdash_{c_N} \Gamma_N (O_N, S_N, E_N)$ *и* $(x, y, \alpha) \in E_N$
где $c_1, c_2, \ldots, c_N$ *– команды переходов*

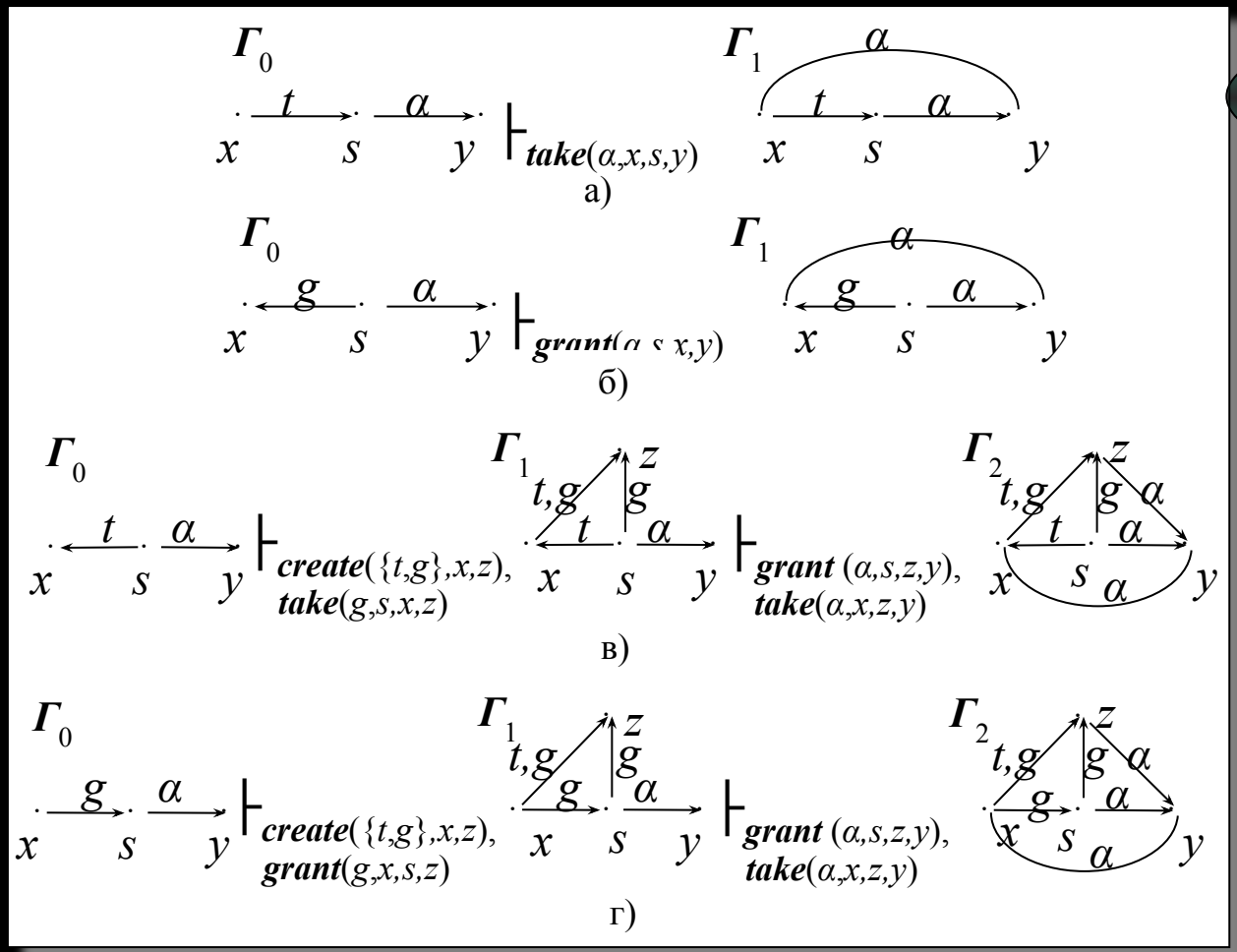
Определение **4**. *Вершины графа доступов являются **tg-связными** (соединены **tg**-путем), если в графе между ними существует такой путь, что каждая дуга этого пути выражает право **t** или **g** (без учета направления дуг)*

4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

Теорема 4. *В графе доступов* $\Gamma_0 (O_0, S_0, E_0)$ *, содержащем только вершины-субъекты, предикат "**возможен доступ**(α, x, y,* Γ_0 *)" истинен тогда и только тогда, когда выполняются следующие условия:*

- существуют субъекты $s_1,\ldots,s_m$ *такие, что* $(s_i, y, \gamma_i) \in E_0$ *для* $i=1, \ldots, m$ *и* $\alpha = \gamma_1 \cup \ldots \cup \gamma_m$.

- субъект x соединен в графе Γ_0 ***tg**-путем с каждым субъектом* s_i *для* $i=1, \ldots, m$



Доказательство

получение прав *α* доступа субъектом *x* у субъекта *s* на объект *y* при различных вариантах непосредственной *tg*-связности

4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

Определение 5. *Островом в произвольном графе доступов* ***Г (O, S, E)*** *называется его максимальный* ***tg-связный*** *подграф, состоящий только из вершин субъектов.*

Определение 6. *Мостом в графе доступов* ***Г (O, S, E)*** *называется* ***tg–путь****, концами которого являются вершины-субъекты; при этом словарная запись* ***tg–пути*** *должна иметь вид*

$$\vec{t}^{\,*}, \overleftarrow{t}^{\,*}, \vec{t}^{\,*}\vec{g}\,\overleftarrow{t}^{\,*}, \vec{t}^{\,*}\overleftarrow{g}\,\overleftarrow{t}^{\,*}$$

*где символ * означает многократное (в том числе нулевое) повторение.*

Определение 7. *Начальным пролетом моста в графе доступов* ***Г (O, S, E)*** *называется* ***tg-путь****, началом которого является вершина-субъект; при этом словарная запись* ***tg-пути*** *должна иметь вид*

$$\vec{t}^{\,*}\vec{g}$$

Определение 8. *Конечным пролетом моста в графе доступов* ***Г (O, S, E)*** *называется* ***tg-путь****, началом которого является вершина-субъект; при этом словарная запись* ***tg-пути*** *должна иметь вид*

$$\vec{t}^{\,*}$$

4.Модели распространения прав доступа. 4.4.Теоретико-графовая модель TAKE-GRANT

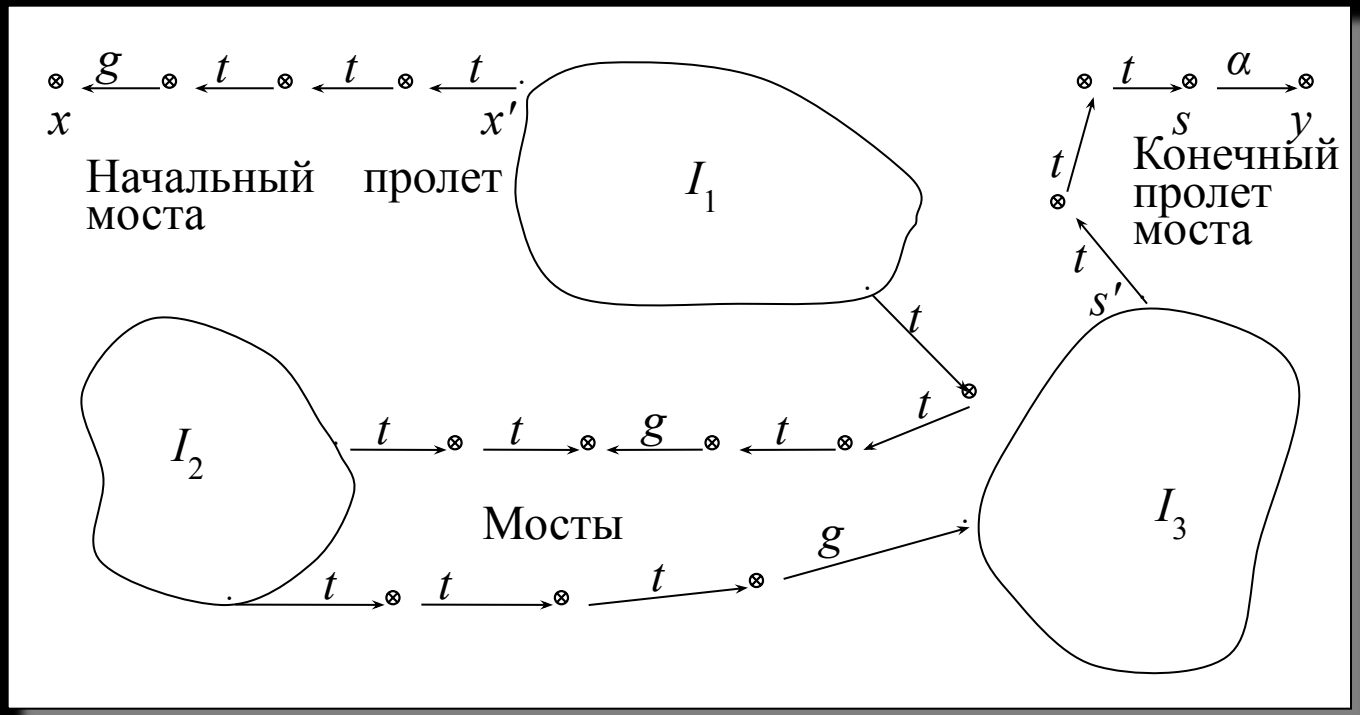
Теорема 4. *В произвольном графе доступов* $\Gamma_0 (O_0, S_0, E_0)$ *предикат "**возможен доступ**(α, x, y, Γ_0)" истинен тогда и только тогда, когда выполняются условия:*

- существуют объекты $s_1,\ldots,s_m$ *такие, что* $(s_i, y, \gamma_i)\in E_0$ *для* $i=1, \ldots, m$ *и* $\alpha =\gamma_1 \cup \ldots \cup \gamma_m$.

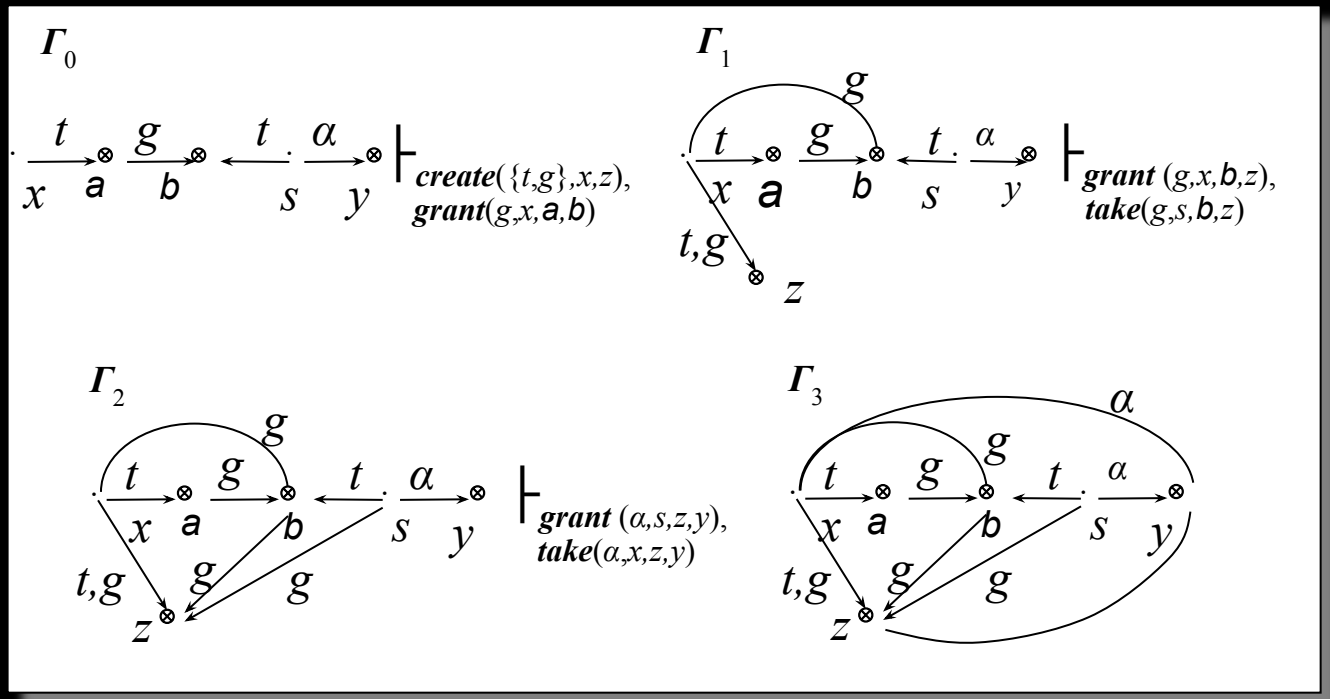
- существуют вершины-субъекты $x_1',\ldots,x_m'$ *и* $s_1',\ldots,s_m'$ *такие, что:*

-- $x = x_i'$ *или* x_i' *соединен с* x *начальным пролетом моста для* $i=1, \ldots, m$;

-- $s_i = s_i'$ *или* s_i' *соединен с* s_i *конечным пролетом моста для* $i=1, \ldots, m$.



Пример графа доступов с возможностью передачи объекту x прав доступа α на объект y



Пример передачи прав доступа по мосту вида

3.1. *Похищение прав доступа*

Определение 9. *Для исходного состояния системы* $\Gamma_0 (O_0, S_0, E_0)$ *и прав доступа* $\alpha \subseteq R$ *предикат "**возможно похищение**(α, x, y, Γ_0)" является истинным тогда и только тогда, когда существуют графы доступов системы* $\Gamma_1 (O_1, S_1, E_1)$, $\Gamma_2 (O_2, S_2, E_2)$, ..., $\Gamma_N (O_N, S_N, E_N)$ *такие, что:*

$\Gamma_0 (O_0, S_0, E_0) \vdash_{c_1} \Gamma_1 (O_1, S_1, E_1) \vdash_{c_2} \ldots \vdash_{c_N} \Gamma_N (O_N, S_N, E_N)$ *и* $(x, y, \alpha) \in E_N$

где $c_1, c_2, \ldots, c_N$ *– команды переходов;*

при этом, если $\exists (s, y, \alpha) \in E_0$, *то* $\forall z \in S_j$, $j=0,1,\ldots, N$ *выполняется:*

$c_1 \neq$ *grant*(α, s, z, y).

4. Модели распространения прав доступа. 4.4. Теоретико-графовая модель TAKE-GRANT

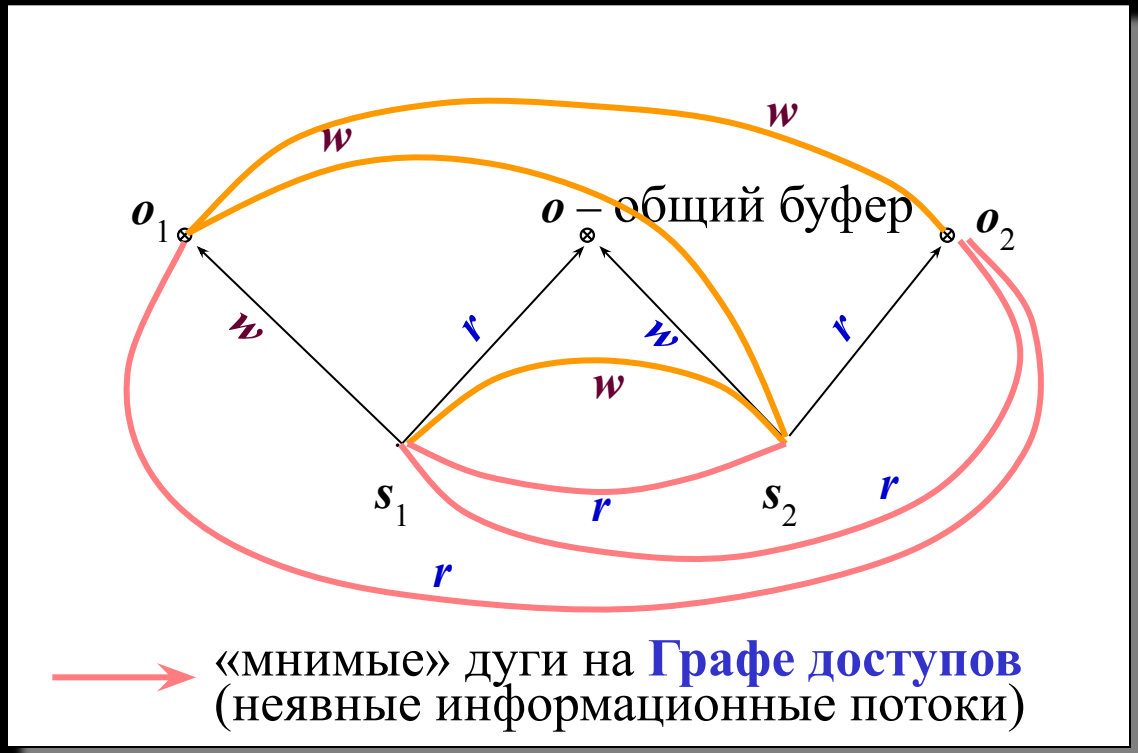
Теорема 4. *В произвольном графе доступов* $\Gamma_0 (O_0, S_0, E_0)$ *предикат "**возможно похищение**(*α, x, y, Γ_0*)" истинен тогда и только тогда, когда выполняются условия:*

- $(x, y, \alpha) \notin E_0$.
- *существуют субъекты* $s_1,\ldots,s_m$ *такие, что* $(s_i, y, \gamma_i) \in E_0$ *для* $i=1, \ldots, m$ *и* $\alpha = \gamma_1 \cup \ldots \cup \gamma_m$
- *являются истинными предикаты "**возможен доступ**(*t, x, s_i, Γ_0*)" для* $i=1, \ldots, m$.

Если политика разграничения доступа в КС запрещает субъектам, имеющим в исходном состоянии права доступа к определенным объектам, непосредственно предоставлять эти права другим субъектам, которые изначально такими правами не обладают, то, тем не менее, такие первоначально "обделенные" субъекты могут получить данные права при наличии в графе доступов возможностей получения доступа с правом t к первым субъектам

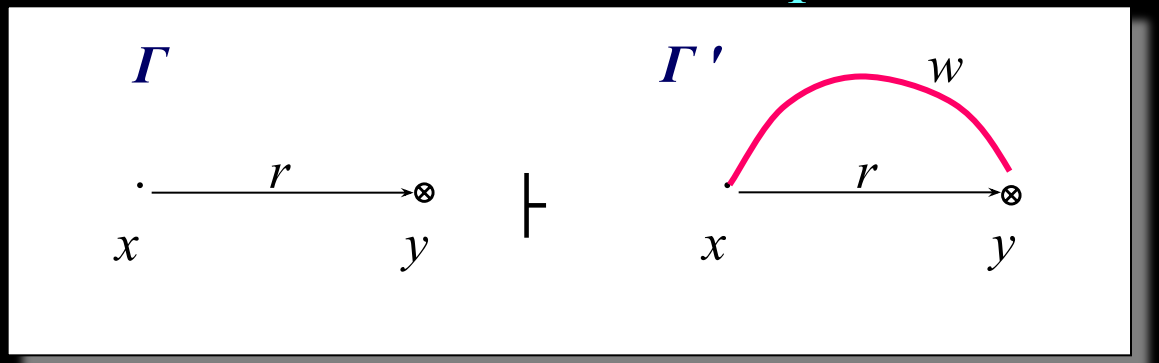
Теоретическая основа для анализа неявных (скрытых) каналов утечки информации в системах с дискреционным доступом

Определение **10**. *Неявным информационным потоком между объектами системы называется процесс переноса информации между ними без их непосредственного взаимодействия* (*операции* ***Read***, ***Write***)



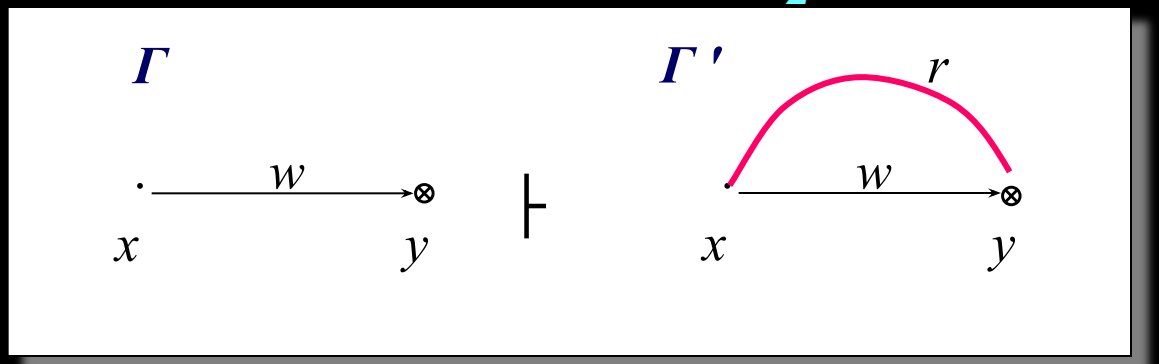
2.Состояние **Графа доступов** изменяется под воздействием элементарных команд 6-х видов (т.н. команды *де-факто*)

Команда без названия $\alpha_1(x, y)$



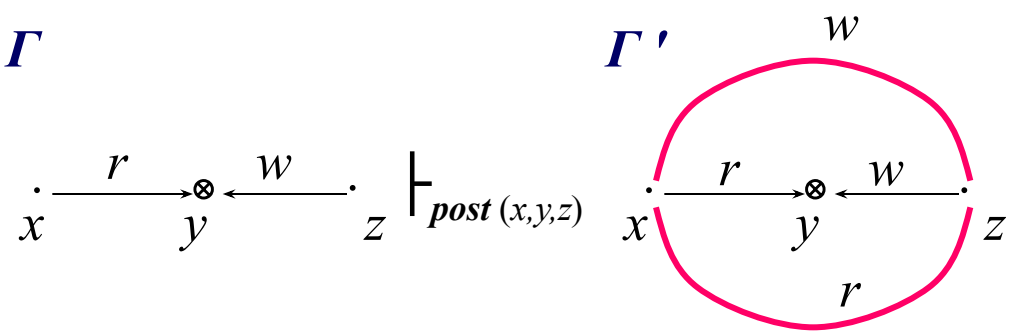
имеется неявная возможность передачи (записи) [конфиденциальной] информации из объекта *y* субъекту *x*, когда тот осуществляет доступ *r* к объекту *y*

Команда без названия $\alpha_2(x, y)$



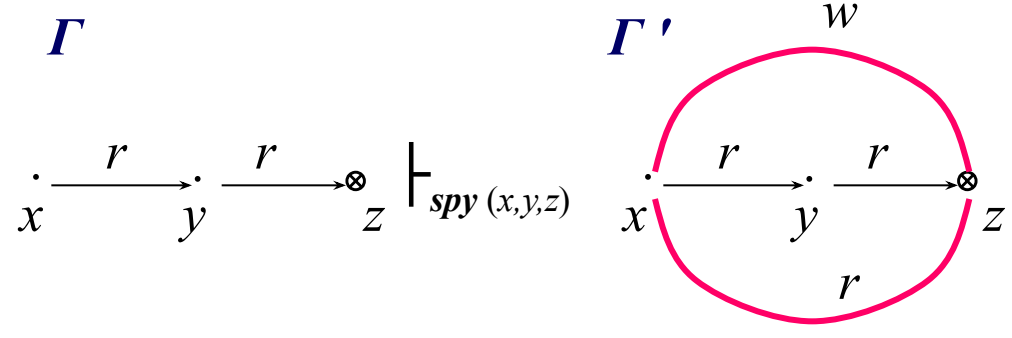
имеется неявная возможность получения (чтения) объектом *y* [конфиденциальной] информации от субъекта *x*], когда тот осуществляет доступ *w* к объекту *y*

Команда *post*(*x*, *y*, *z*)



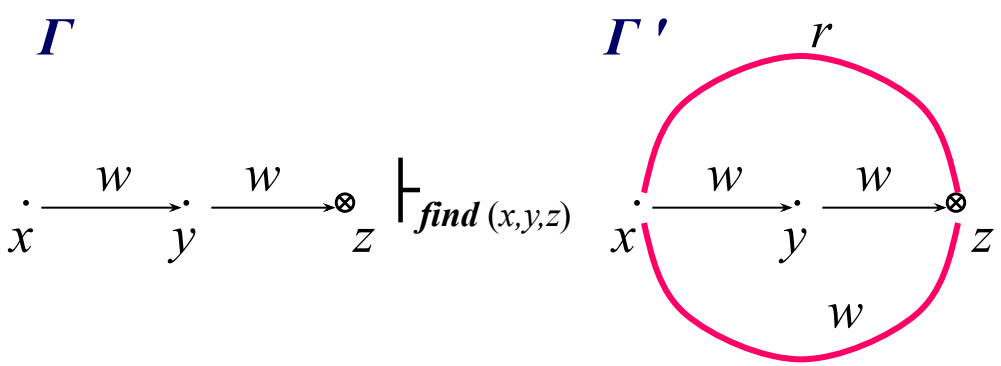
субъект *x* получает возможность чтения информации от (из) другого субъекта *z*, осуществляя доступ *r* к объекту *y*, к которому субъект *z* осуществляет доступ *w*, а субъект *z*, в свою очередь, получает возможность записи своей информации в субъект *x*

Команда *spy*(*x*, *y*, *z*)



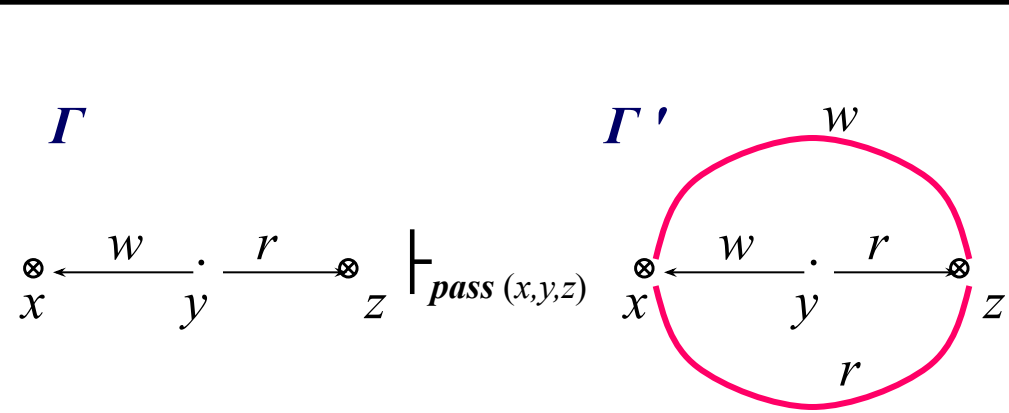
субъект *x* получает возможность чтения информации из объекта *z*, осуществляя доступ *r* к субъекту *y*, который, в свою очередь, осуществляет доступ *r* к объекту *z*, при этом также у субъекта *x* возникает возможность записи к себе информации из объекта *z*

Команда *find*(*x*, *y*, *z*)



субъект *x* получает неявную возможность передачи (записи) конф. информации в объект *z*, осуществляя доступ *w* к субъекту *y*, который, в свою очередь, осуществляет доступ *w* к объекту *z*, при этом также у субъекта *z* возникает неявн. возможность чтения конф. информации из субъекта *x*

Команда *pass*(*x*, *y*, *z*)



при осуществлении субъектом *y* доступа *r* к объекту *z* возникает неявная возможность внесения из него конф. информации в другой объект *x*, к которому субъект *y* осуществляет доступ *w*, и, кроме того, возникает возможность получения информации (чтения) объектом *x* из объекта *z*

Правила *де-юре* к мнимым дугам не применяются

4.Модели распространения прав доступа. 4.5.Расширенная (extended) модель TAKE-GRANT

3. Анализ возможности возникновения неявного информационного канала (потока) между двумя произвольными объектами (субъектами) ***x*** и ***y*** системы осуществляется на основе поиска и построения в графе доступов **пути** между ***x*** и ***y***, образованного **мнимыми дугами**, порождаемыми применением команд ***де-факто*** к различным фрагментам исходного **Графа доступов**

Расширенная модель TAKE-GRANT позволяет анализировать специфические проблемы в дискреционных системах разграничения доступа:

- при допущении возможности или при наличии достоверных фактов о состоявшемся неявном информационном потоке от одного объекта(субъекта) к другому объекту(субъекту), анализировать и выявлять **круг возможных субъектов-"заговорщиков"** несанкционированного информационного потока

- для какой-либо пары объектов (субъектов) осуществлять анализ не только возможности неявного информационного потока, но и **количественных** характеристик по тому или иному маршруту:

  возможно взвешивание мнимых дуг на Графе доступов посредством оценки вероятности их возникновения

  возможны количественные сравнения различных вариантов возникновения неявного потока по длине пути на Графе доступов

- **оптимизировать** систему назначений доступа по критериям минимизации возможных неявных информационных потоков

Достоинства дискреционных моделей

- *Хорошая гранулированность защиты (позволяют управлять доступом с точностью до отдельной операции над отдельным объектом)*
- *Простота реализации*

Недостатки дискреционных моделей

- *Слабые защитные характеристики из-за невозможности для реальных систем выполнять все ограничения безопасности*
- *Проблема "троянских коней"*
- *Сложности в управлении доступом из-за большого количества назначений прав доступа*

Лекция 2.2.

Модели безопасности на основе мандатной политики

Учебные вопросы:

1. **Общая характеристика моделей полномочного (мандатного) доступа**
2. **Модель Белла-ЛаПадулы**
3. **Расширения модели Белла-ЛаПадулы**

Литература:

1. **Зегжда Д.П.,Ивашко А.М.** Основы безопасности информационных систем. - М.:Горячая линия - Телеком, 2000. - 452с
2. **Грушо А.А.,Тимонина Е.Е.**Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с
3. **Прокопьев И.В., Шрамков И.Г., Щербаков А.Ю.** Введение в теоретические основы компьютерной безопасности : Уч. пособие. М., 1998.- 184с.
11. **Девянин П.Н.** Модели безопасности компьютерных систем Учеб. пособие. – М.: Изд.центр «Академия», 2005. – 144 с.

1. Общая характеристика моделей мандатного доступа

Основаны:
-на *субъектно-объектной* модели КС
- на *правилах организации секретного делопроизводства*
принятых в гос. учреждениях многих стран

Информация (точнее документы, ее содержащие) категорируется специальными метками конфиденциальности – т.н. ***грифы секретности*** документов

Сотрудники по уровню благонадежности (доверия к ним) получают т.н. ***допуска*** определенной ***степени***

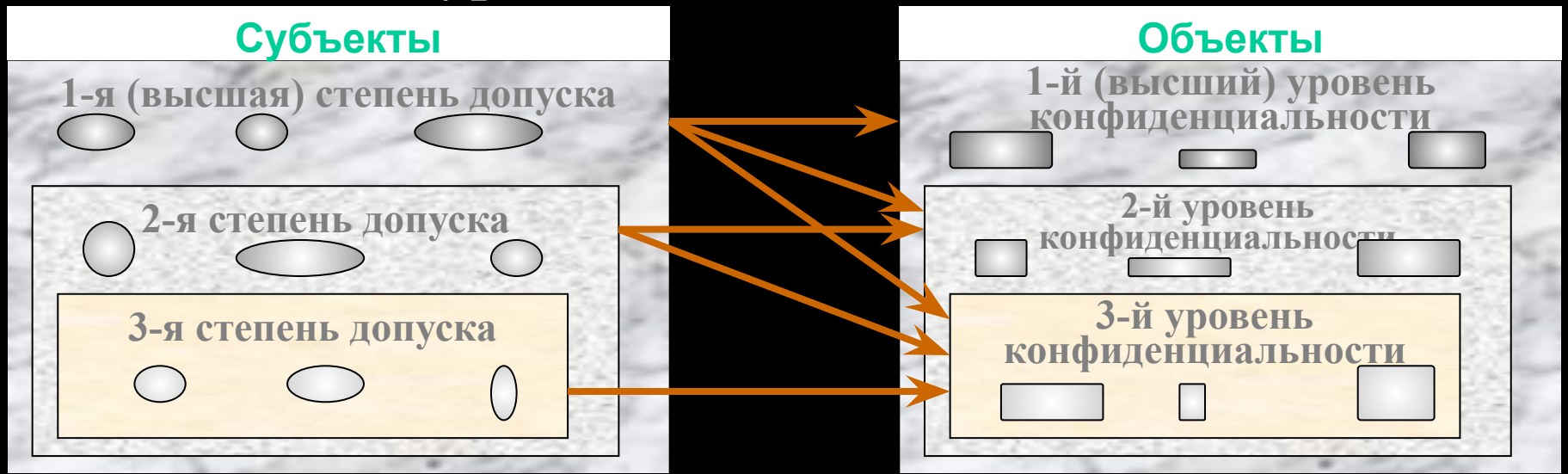
Сотрудники с допуском определенной степени приобретают ***полномочия*** работы с документами определенного грифа секретности

Гл. задача:
-не допустить утечки информации из документов
с высоким грифом секретности к сотрудникам
с низким уровнем допуска

Основные положения *моделей мандатного доступа*

- Вводится система "***уровней безопасности***" – решетка с оператором доминирования
- Устанавливается функция (процедура) присваива-ния субъектам и объектам уровней безопасности
- Управление и контроль доступом субъектов к объектам производится на основе двух правил:

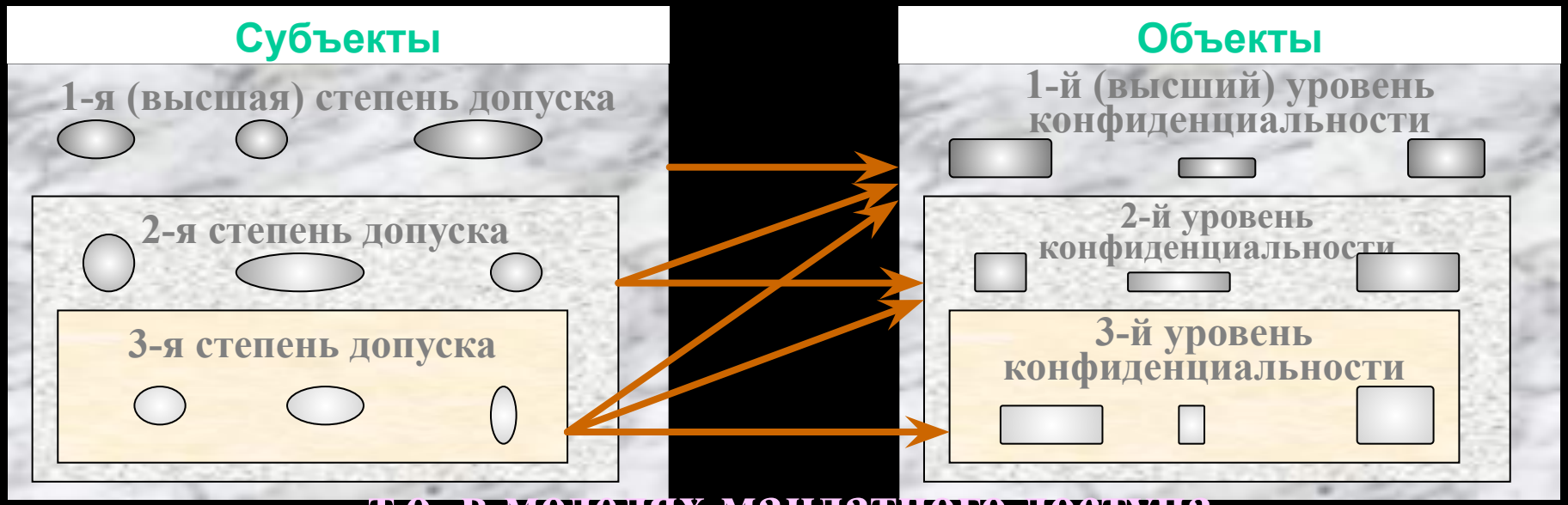
1.Запрет чтения вверх (*no read up - NRU*) - субъект не может читать объект с уровнем безопасности, большим своего уровня безопасности



1

2

2.Запрет записи вниз (*no write down - NWD*) - субъект не может писать информацию в объект, уровень безопасности которого ниже уровня безопасности самого субъекта (т.н. ****-свойство***)



т.о. в моделях мандатного доступа устанавливается жесткое управление доступом с целью контроля не столько операций, а потоков между сущностям с разным уровнем безопасности

- Для управления (разграничения) доступом к объектам одного уровня конфиденциальности используют дискреционный принцип, т.е. дополнительно вводят матрицу доступа

Решетка уровней безопасности Λ_L

- алгебра $(L, \leq, \cdot, \otimes)$, где

L – базовое множество уровней безопасности

$\leq$ – оператор доминирования, определяющий частичное нестрогое отношение порядка на множестве **L**. Отношение, задаваемое $\leq$, *рефлексивно*, *антисимметрично* и *транзитивно*:

$\forall\, l \in L: l \leq l$;

$\forall\, l_1, l_2 \in L: (l_1 \leq l_2 \wedge l_2 \leq l_1) \Rightarrow l_1 = l_2$;

$\forall\, l_1, l_2, l_3 \in L: (l_1 \leq l_2 \wedge l_2 \leq l_3) \Rightarrow l_1 \leq l_3$;

$\cdot$ – оператор, определяющий для любой пары $l_1, l_2 \in L$ наименьшую верхнюю границу -

$l_1 \cdot l_2 = l \Leftrightarrow l_1, l_2 \leq l \wedge \forall\, l' \in L: (l' \leq l) \Rightarrow (l' \leq l_1 \vee l' \leq l_2)$

$\otimes$ – оператор, определяющий для любой пары $l_1, l_2 \in L$ наибольшую верхнюю границу -

$l_1 \otimes l_2 = l \Leftrightarrow l \leq l_1, l_2 \wedge \forall\, l' \in L: (l' \leq l_1 \wedge l' \leq l_2) \Rightarrow (l' \leq l)$

Функция уровня безопасности $f_L: X \rightarrow L$

- однозначное отображение множества сущностей КС $X = S \cup O$ во множество уровней безопасности L решетки Λ_L .

Обратное отображение $f_L^{-1}: L \rightarrow X$ задает разделение всех сущностей КС на **классы безопасности** X_i, такие что:

$X_1 \cup X_2 \cup \ldots \cup X_N = X$,

где N - мощность базового множества уровней безопасности L;

$X_i \cap X_j \equiv \varnothing$, где $i \neq j$;

$\forall x' \in X_i \Rightarrow f_L(x') = l_i$, где $l_i \in L$

2. Модель Белла-ЛаПадулы

D.Elliott **Bell**, Leonard J.**LaPadula**, 1973-75

Система защиты - совокупность

- множества субъектов S
- множества объектов O
- множества прав доступа R (в исх. виде всего два элемента - *read* и *write*)
- матрицы доступа $A[s,o]$
- решетки уровней безопасности L субъектов и объектов (допуска и грифы секретности)
- функции уровней безопасности f_L, отображающей элементы множеств S и O в L
- множества состояний системы V, которое определяется множеством упорядоченных пар (f_L,A)
- начального состояния v_0
- набора запросов Q субъектов к объектам, выполнение которых переводит систему в новое состояние
- функции переходов $\mathcal{F}_T : (V \times Q) \rightarrow V$, которая переводит систему из одного состояния в другое при выполнении запросов

Белл и ЛаПадула ввели следующее определение безопасного состояния системы

1. Состояние называется **безопасным по чтению** (или *просто безопасным*) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта:

$$\forall s \in S,\ \forall o \in O,\ read \in A[s,o] \rightarrow f_L(s) \geq f_L(o)$$

2. Состояние называется **безопасным по записи** (или **-безопасным*) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности объекта доминирует над уровнем безопасности этого субъекта:

$$\forall s \in S,\ \forall o \in O,\ write \in A[s,o] \rightarrow f_L(o) \geq f_L(s)$$

3. Состояние **безопасно** тогда и только тогда, когда оно безопасно *и по чтению, и по записи*

На основе определений 1,2 и 3 *критерий безопасности:*

Система $\Sigma(v_0, Q, F_T)$ безопасна тогда и только тогда, когда ее начальное состояние v_0 безопасно и все состояния, достижимые из v_0 путем применения конечной последовательности запросов из Q безопасны

Белла и ЛаПадула доказали т.н. *Основную теорему безопасности:*

Теорема ОТБ. **Система $\Sigma(v_0, Q, \mathcal{F}_T)$ безопасна тогда и только тогда, когда:**

1. Состояние v_0 безопасно

2. Функция переходов $\mathcal{F}_T$ такова, что любое состояние v, достижимое из v_0 при выполнении конечной последовательности запросов из множества Q, также безопасно

3. Если при $\mathcal{F}_T(v,q)=v^*$, где $v=(f_L, A)$ и $v^*=(f_L^*, A^*)$, переходы системы из состояния в состояние подчиняются следующим ограничениям для $\forall s \in S$ и для $\forall o \in O$:

- если $read \in A^*[s,o]$ и $read \notin A[s,o]$, то $f_L^*(s) \geq f_L^*(o)$
- если $read \in A[s,o]$ и $f_L^*(s) < f_L^*(o)$, то $read \notin A^*[s,o]$
- если $write \in A^*[s,o]$ и $write \notin A[s,o]$, то $f_L^*(s) \leq f_L^*(o)$
- если $write \in A[s,o]$ и $f_L^*(o) < f_L^*(s)$, то $write \notin A^*[s,o]$

Правила доступа и ограничения NRU и NWD должны работать независимо от предыстории конкретных объектов и субъектов

При переходе в новое состояние не возникает никаких новых и не сохраняется никаких старых отношений доступа, которые небезопасны по отношению к функции уровня безопасности нового

2. Модель Белла-ЛаПадулы

Достоинства модели Белла-ЛаПадулы:

- ясность и простота реализации
- отсутствие проблемы "Троянских коней" (контролируется направленность потоков, а не взаимоотношения конкретного субъекта с конкретным объектом, поэтому недекларированный поток троянской программы «сверху-вниз» будет считаться опасным и отвергнут МБО)
- каналы утечки не заложены в саму модель, а могут возникнуть только в практической реализации

Недостатки модели Белла-ЛаПадулы:

- возможность ведения операций доступа (Delete), не влияющих с т.зр. модели на безопасность, которые тем не менее могут привести к потери данных
- проблема Z-системы (Мак-Лин) - такая система, в которой при запросе все сущности м.б. деклассифицированы до самого низкого уровня и тем самым м.б. осуществлен любой доступ (в модели не заложены принципы и механизмы классификации объектов)
- отсутствие в модели доверенных субъектов-администраторов Типовые действия администраторов (создание пользователей, установление их полномочий и т.д.) не могут ни приводить к нарушениям безопасности с т. зр. модели Белла-ЛаПадулы

Безопасная функция перехода (*Мак-Лин*)

Гарантии безопасности в процессе осуществления переходов между состояниями

Функция перехода $F_T(v,q)=v^*$ *безопасна* по чтению когда:

1. Если $read \in A^*[s,o]$ и $read \notin A[s,o]$, то $f_{Ls}(s) \geq f_{Lo}(o)$ и $f_L = f_L^*$
2. Если $f_{Ls} \neq f_{Ls}^*$, то $A=A^*$, $f_{Lo}=f_{Lo}^*$, для $\forall$ s и o, у которых $f_{Ls}^*(s) < f_{Lo}^*(o)$, - $read \notin A[s,o]$
3. Если $f_{Lo} \neq f_{Lo}^*$, то $A=A^*$, $f_{Ls}=f_{Ls}^*$, для $\forall$ s и o, у которых $f_{Ls}^*(s) < f_{Lo}^*(o)$, - $read \notin A[s,o]$

Функция перехода $F_T(v,q)=v^*$ *безопасна* по записи когда:

1. Если $write \in A^*[s,o]$ и $write \notin A[s,o]$, то $f_{Lo}(o) \geq f_{Ls}(s)$ и $f_L = F_L^*$
2. Если $f_{Ls} \neq f_{Ls}^*$, то $A=A^*$, $f_{Lo}=f_{Lo}^*$, для $\forall$ s и o, у которых $f_{Ls}^*(s) > f_{Lo}^*(o)$, - $write \notin A[s,o]$
3. Если $f_{Lo} \neq f_{Lo}^*$, то $A=A^*$, $f_{Ls}=f_{Ls}^*$, для $\forall$ s и o, у которых $f_{Ls}^*(s) > f_{Lo}^*(o)$, - $write \notin A[s,o]$

Нельзя изменять одновременно более одного компонента состояния системы. Можно:
-либо ввести новое отношение доступа
-либо изменить уровень субъекта
-либо изменить уровень объекта

Критерий безопасности Мак-Лина для функции перехода

Функция перехода $F_T(v,q)=v^*$ является безопасной тогда и только тогда, когда она *изменяет только один* из компонентов состояния и изменения не приводят к нарушению безопасности системы

Теорема безопасности Мак-Лина.

Система безопасна в любом состоянии и в процессе переходов между ними, если ее начальное состояние безопасно, а функция перехода удовлетворяет критерию безопасности Мак-Лина

Но! Нет контроля самого процесса изменения уровней безопасности сущностей в процессе осуществления переходов

Уполномоченные (доверенные) субъекты (*Мак-Лин*)

В базовую модель дополнительно вводится подмножество доверенных субъектов, которым (и только им) разрешается инициировать переходы с изменениями уровней безопасности сущностей системы – $C(S)$

Соответственно функция переходов системы $\Sigma(v_0, Q, \mathcal{F}_T^a)$ – $\mathcal{F}_T^a$ приобретает дополнительный параметр *авторизации*

Функция перехода $\mathcal{F}_T^a(v,s,q)$ в модели с называется авторизованной тогда и только тогда, когда для каждого перехода $\mathcal{F}_T^a(v,s,q)=v^*$, при котором:

для $\forall x \in S \cup O$**:** если $f_L(x) \neq f_L(x)$, то $s \in C(S)$

Система $\Sigma(v_0, Q, \mathcal{F}_T^a)$ с доверенными субъектами безопасна если :

1. Начальное состояние v_0 безопасно и все достижимые состояния безопасны по критерию Белла-ЛаПадулы
2. Функция переходов $\mathcal{F}_T^a$ является ***авторизованной***

Другие расширения модели Белла-ЛаПадулы

Модель *Low-WaterMark*

Вводится дополнительная операция *reset*(*s*,*o*), которая повышает до максимального уровень безопасности объекта при условии *F*(*s*)>*F*(*o*). В результате субъекту м.б. доступен по *write* любой объект

Модифицируется *write*(*s*,*o*) Если при операции *write* уровень объекта выше уровня субъекта то:

- происходит понижение уровня безопасности объекта до уровня безопасности субъекта;

- перед внесением новой старая информация в объекте стирается (чтобы потом нельзя было прочесть)

Модель *совместного доступа*

Доступ к определенной информации или модификация ее уровня безопасности может осуществляться только в результате совместных действий нескольких пользователей (т.е. только в результате группового доступа- z.b. гриф секретности документа м.б. изменен только совместными действиями владельца-исполнителя и администратора безопасности)

В матрице доступа вводятся групповые объекты и др.

Другие недостатки модели Белла-ЛаПадулы

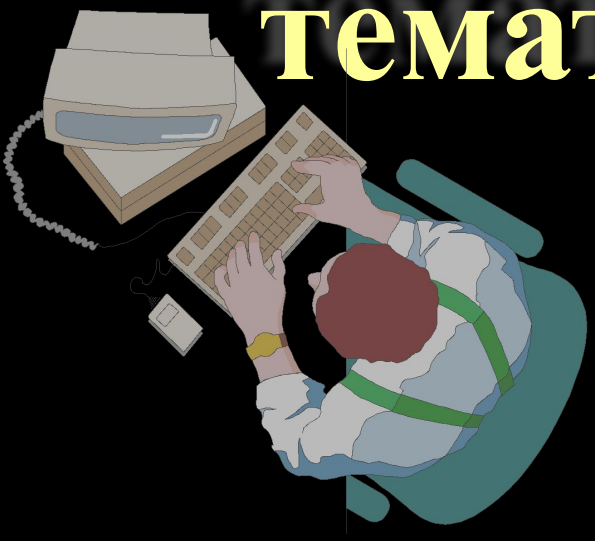
- **возможность скрытых каналов утечки** - механизм, посредством которого субъект с высоким уровнем безопасности м. предоставить определенные аспекты конфиденциальной информации субъекту, уровень безопасности которого ниже уровня безопасности конф. информации
- **проблема удаленного доступа**. В распределенных системах осуществление доступа всегда сопровождается потоком информации в прямом и обратном направлении, что результате может приводить к нарушениям привил NRU и NWD
- **проблема избыточности прав доступа**. Без учета матрицы доступа (т.е. без использования дискреционного доступа) мандатный принцип доступа организует доступ более жестко, но и более грубо, без учета потребностей конкретных пользователей-субъектов

Тем не менее **модель Белла-ЛаПадулы оказала сильное влияние на развитие моделей безопасности и *стандартов защищенности КС***

Тема 2. **Модели безопасности компьютерных систем**

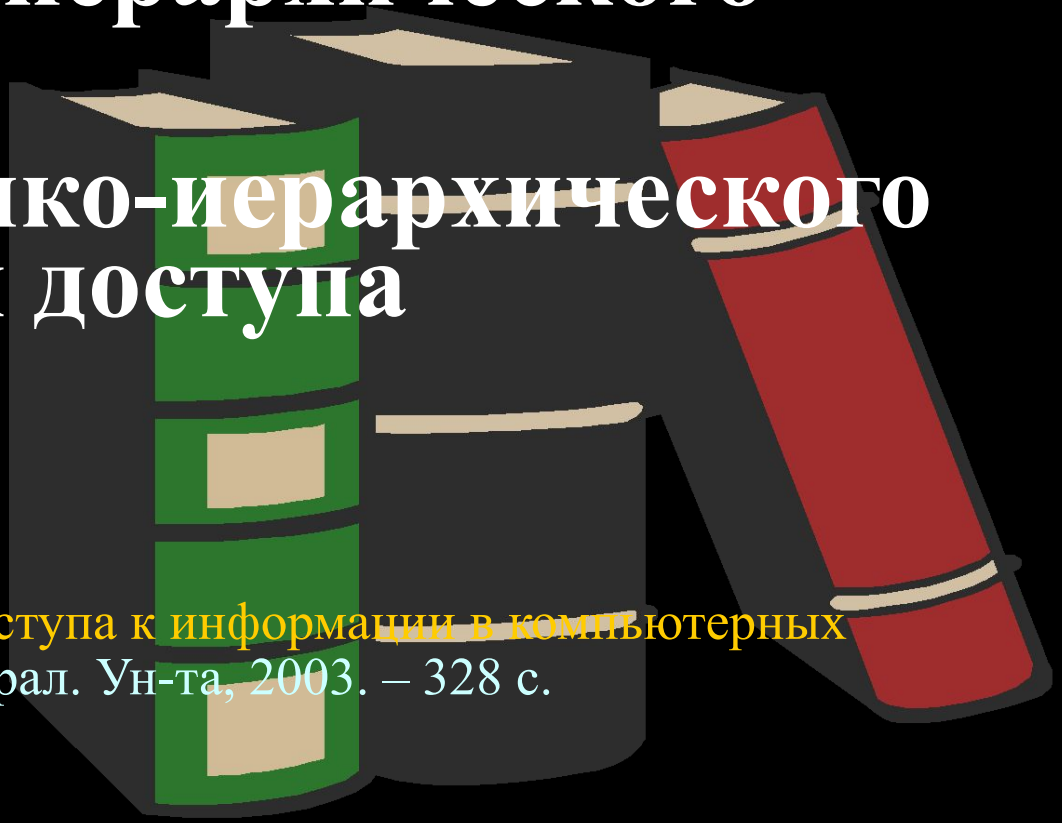
Лекция 2.3.

Модели безопасности на основе тематической политики



Учебные вопросы:

1. Общая характеристика тематического разграничения доступа
2. Тематическая решетка мультирубрик иерархического рубрикатора
3. Модели тематико-иерархического разграничения доступа

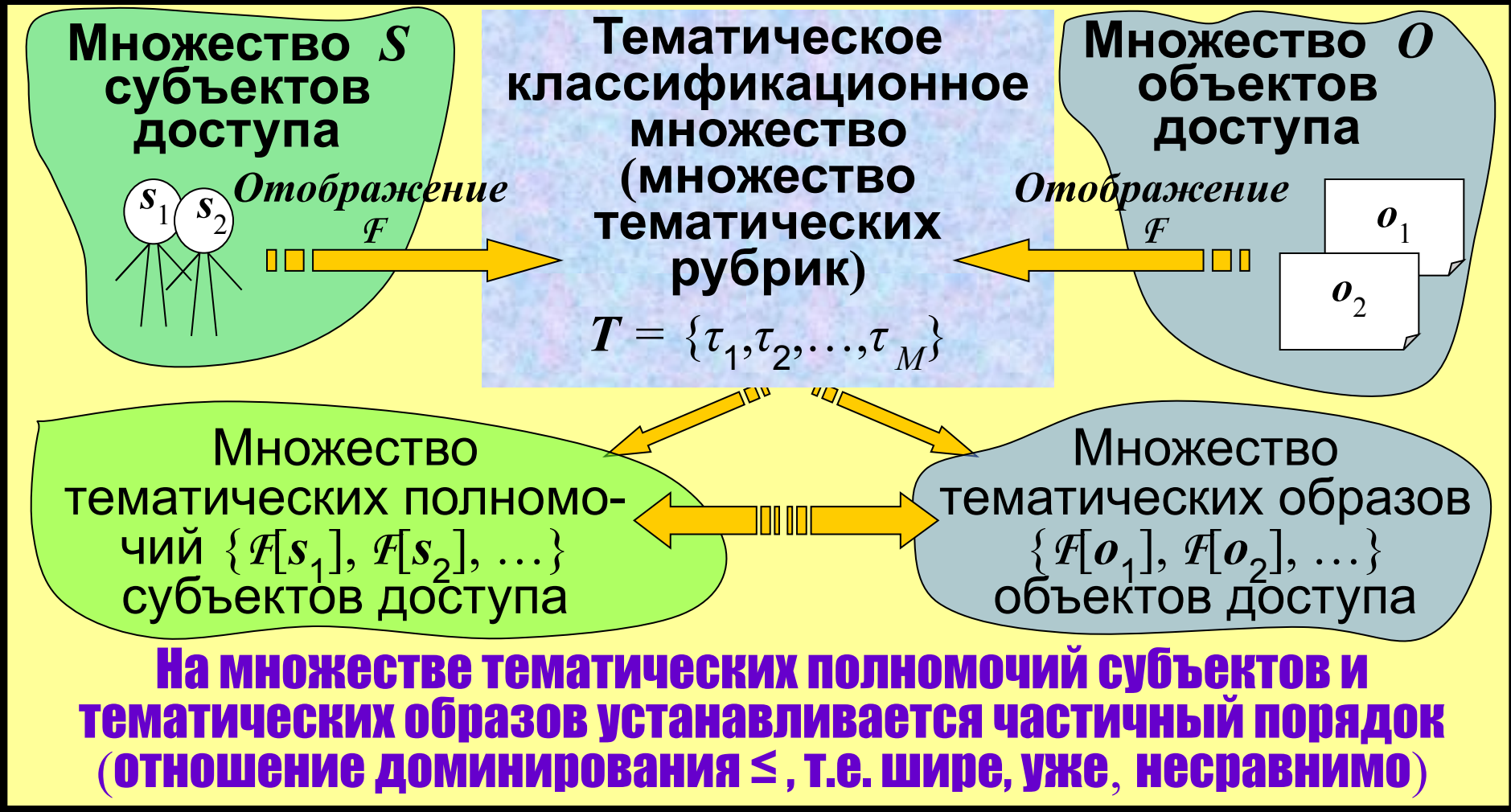


Литература:

Гайдмакин Н.А. Разграничение доступа к информации в компьютерных системах. - Екатеринбург: Изд-во Урал. Ун-та, 2003. – 328 с.

Политика тематического разграничения доступа

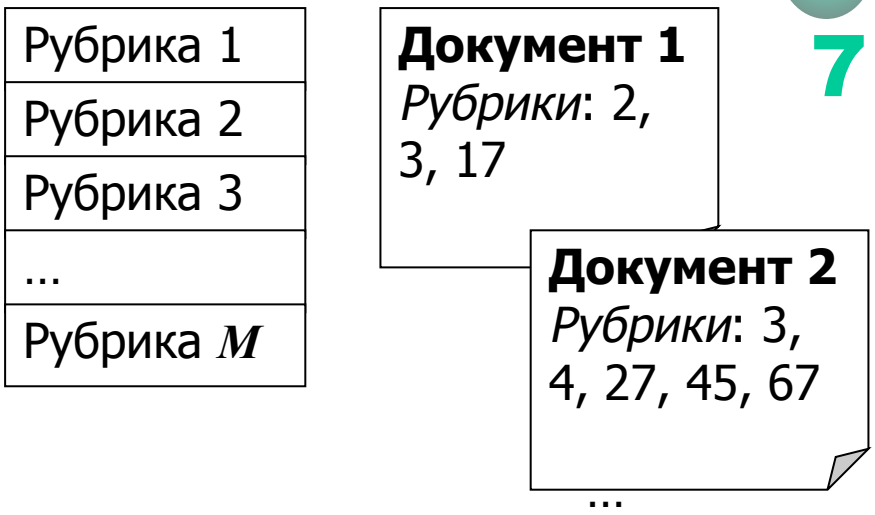
1.Множество субъектов и объектов доступа $X = S \cup O$ тематически классифицируются



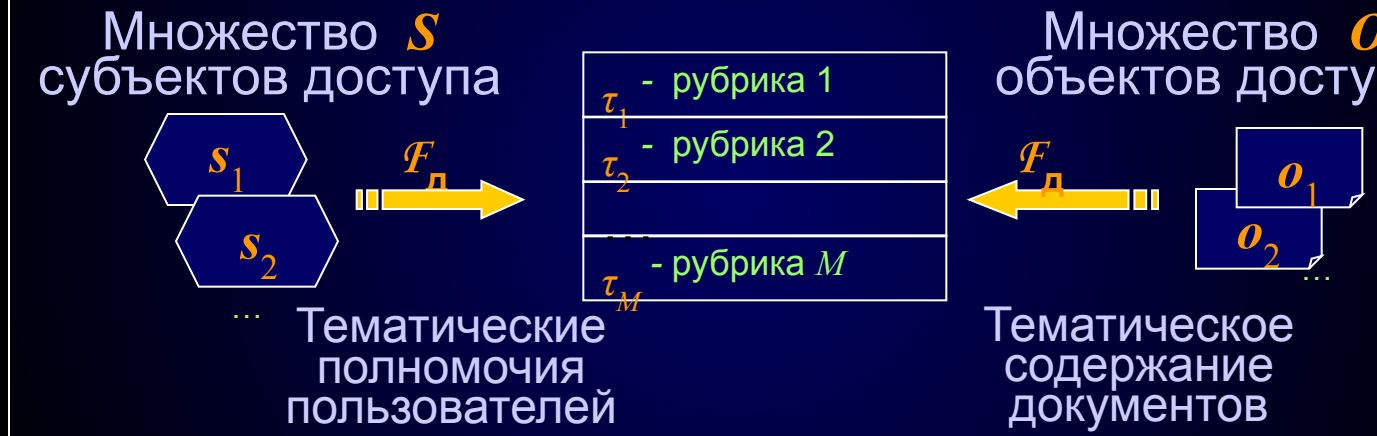
На множестве тематических полномочий субъектов и тематических образов устанавливается частичный порядок (отношение доминирования ≤, т.е. шире, уже, несравнимо)

2. Три способа тематической классификации

- дескрипторная
- иерархическая
  - -- монорубрицированная
  - -- мультирубрицированная
- фасетная



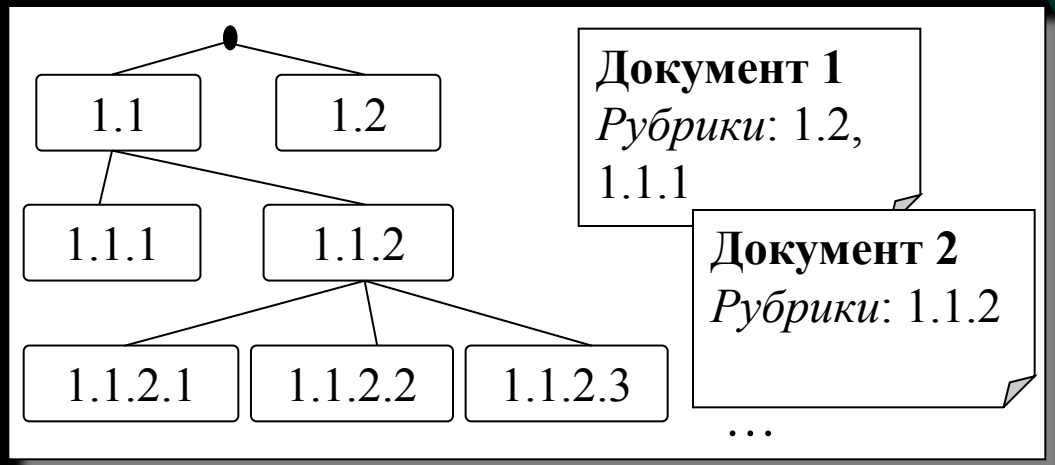
Дескрипторное классифицирующее тематическое множество $T_д$ – множество неупорядоченных тематических рубрик (дескрипторов)



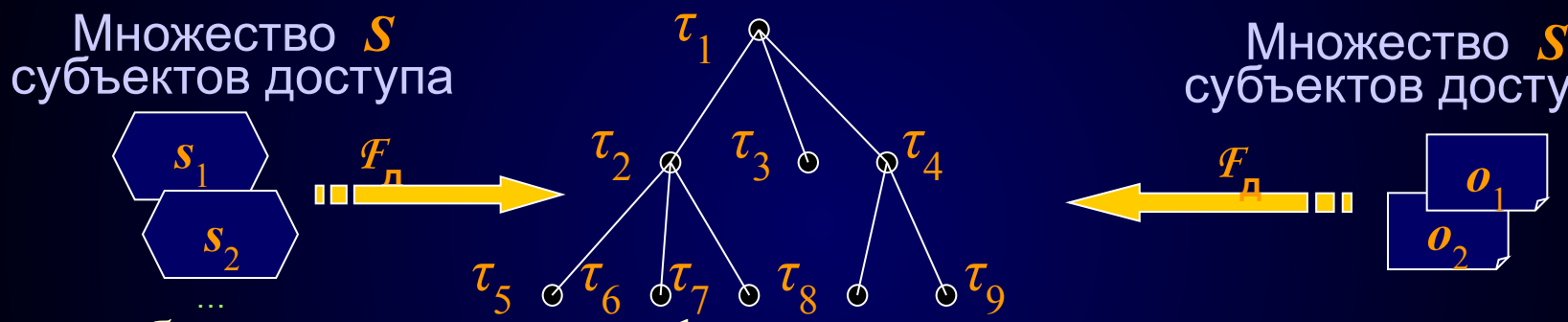
$$F_д[x_i] = \{\tau_{i1}, \tau_{i2}, \ldots, \tau_{iI}\} \wedge \tau_{ik} \neq \tau_{im}, \quad x_i \in S \cup O, I \leq M$$

Дескрипторная тематическая классификация

Иерархическая тематическая классификация



Иерархический тематический классификатор – множество рубрик $T_и$, на котором посредством корневого дерева установлено отношение частичного порядка элементов $\leq$



Монорубрицованная классификация

$\mathcal{F}_{имн}[x_i] = \tau_i \cup \{\tau_{i1}, \tau_{i2}, \ldots, \tau_{iI}\}$, где $\tau_{ik} \leq \tau_i$, $x_i \in S \cup O$, $I < M$.

Мультирубрицированная классификация

$\mathcal{F}_{имл}[x_i] = \{\tau_{i1}, \tau_{i2}, \ldots, \tau_{iI}\} \cup \{\tau_{i11}, \tau_{i12}, \ldots, \tau_{i21}, \tau_{i22}, \ldots, \tau_{iI1}, \tau_{iI2}, \ldots\} \wedge \tau_{im} \not\leq\geq \tau_{in}$

$\wedge \vee_{и} \{\tau_{k1}, \tau_{k2}, \ldots, \tau_{kL}\} = \varnothing$, $\tau_{ik} \leq \tau_{ikj}$

1.Общая характеристика тематического разграничения доступа

Политика тематического разграничения доступа

3.Недопустимы доступы (вызывающие опасные потоки)

- от сущностей x_1 с более широкой тематикой к сущностям x_2 с более узкой тематикой $(x_1 \rightarrow x_2)$

  $\mathcal{F}[x_1] \geq \mathcal{F}[x_2]$

- между сущностями x_1 и x_2 с несравнимой тематикой

  $(x_1 \leftrightarrow x_2)$ $\mathcal{F}[x_2] \geq \leq \mathcal{F}[x_2]$

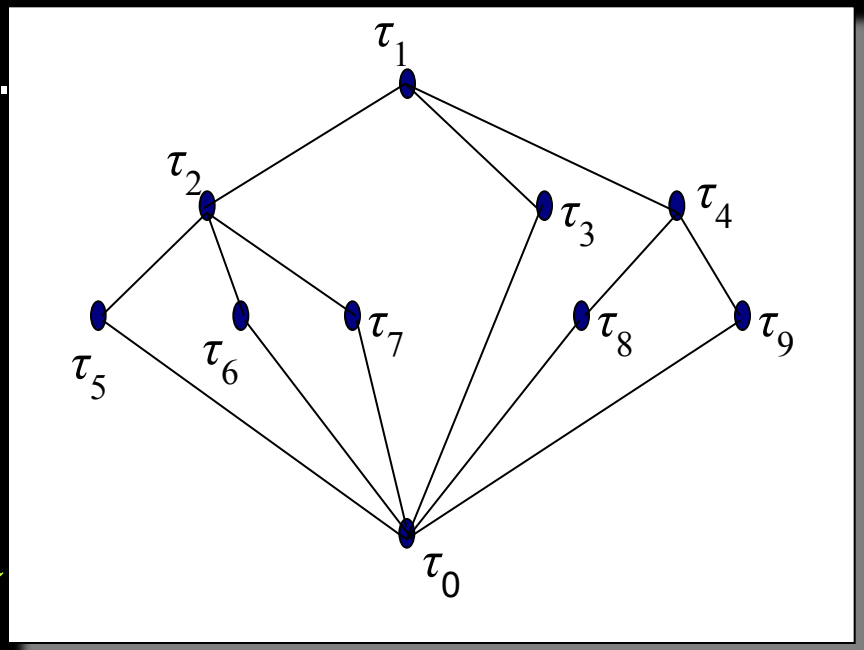
Тематические решетки

1. При дескрипторной тематической классификации

- решетка $\Lambda_д(P_д, \subseteq, \cup, \cap)$ подмножеств множества $T_д = \{\tau_1,\tau_2,\ldots,\tau_M\}$, где $P_д = \mathcal{F}_д[x] \subseteq T_д$, $x \in S \cup O$

2. На иерархическом рубрикаторе при монорубрицированной классификации

- решетка $\Lambda_и(T_{и\varnothing}, \leq, \sup_и, \inf_и)$ на корневом дереве рубрикатора $T_и = \{\tau_1,\tau_2,\ldots,\tau_M\}$ путем добавления вершины τ_0 (с пустой тематикой) и замыкания на нее всех листовых вершин



- решетка $\Lambda_и(\mathcal{T}^{\sqcap}, \subseteq, \cup_{ил}, \cap)$ листовых подмножеств вершин на корневом дереве рубрикатора. Решетки $\Lambda_и(T_{и\varnothing}, \leq, \sup_и, \inf_и)$ и $\Lambda_и(\mathcal{T}^{\sqcap}, \subseteq, \cup_{ил}, \cap)$ изоморфны

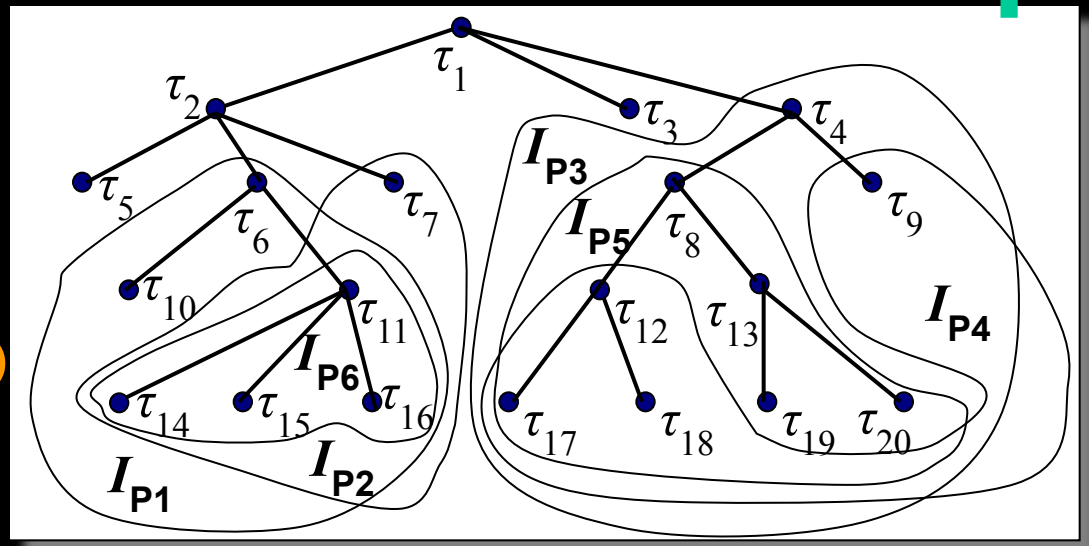
Тематические решетки (продолжение)

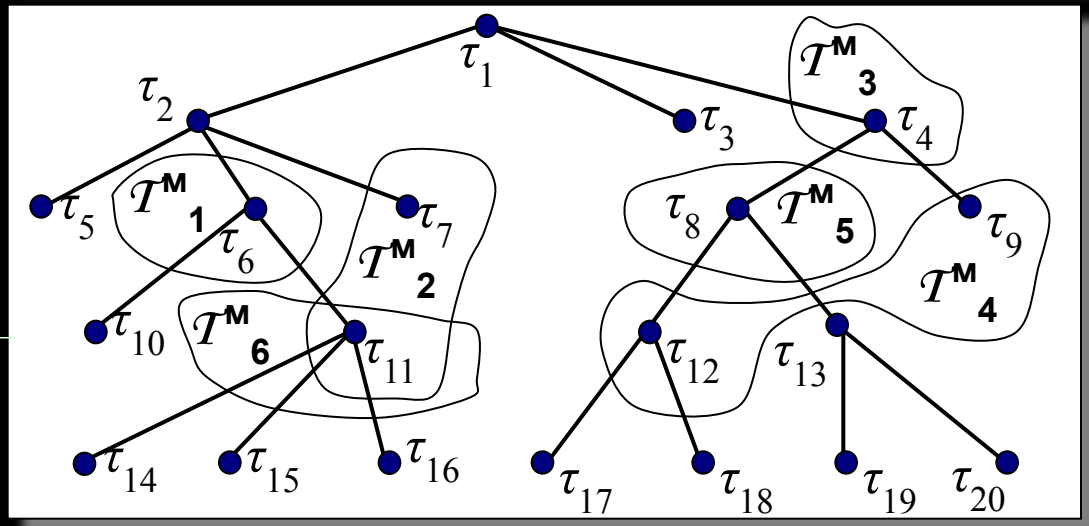
3. На иерархическом рубрикаторе при мультирубрицированной классификации

- **решетка $\Lambda_и(I_P, \subseteq, \cup_{ир}, \cap)$ рубрикаторных идеалов**

$I_{P2} \subseteq I_{P6}$, $I_{P2} \subseteq I_{P1}$, $I_{P4} \subseteq I_{P3}$, $I_{P5} \subseteq I_{P3}$, $I_{P6} = I_{P1} \cap I_{P2}$, $I_{P3} = I_{P4} \cup_{ир} I_{P5}$

- **решетка мультирубрик $\Lambda_и(T^м, \leq_м, \cup_м, \cap_м)$**





Определение 1. *Мультирубрика $T^м_i$ **доминирует** над мультирубрикой $T^м_j$ $\{\tau^{(j)}_1, \tau^{(j)}_2, \ldots, \tau^{(j)}_J\} \leq \{\tau^{(i)}_1, \tau^{(i)}_2, \ldots, \tau^{(i)}_I\}$ в том и только в том случае, когда для любого $m=1,\ldots,J$ существует $k=1,\ldots,I$ такое, что $\tau^{(j)}_m \leq \tau^{(i)}_k$ (вершина $\tau^{(j)}_m$ подчинена по корневому дереву вершине $\tau^{(i)}_k$):*

$$\forall\, \tau^{(j)}_m \in T^м_j, \quad \exists\, \tau^{(i)}_k \in T^м_i \wedge \tau^{(j)}_m \leq \tau^{(i)}_k$$

$T^м_2 \leq_м T^м_6$, $T^м_4 \leq_м T^м_3$, $T^м_5 \leq_м T^м_3$,
$T^м_6 = T^м_1 \cap_м T^м_2$, $T^м_3 = T^м_4 \cup_м T^м_5$

2. Тематическая решетка мультирубрик иерархического рубрикатора

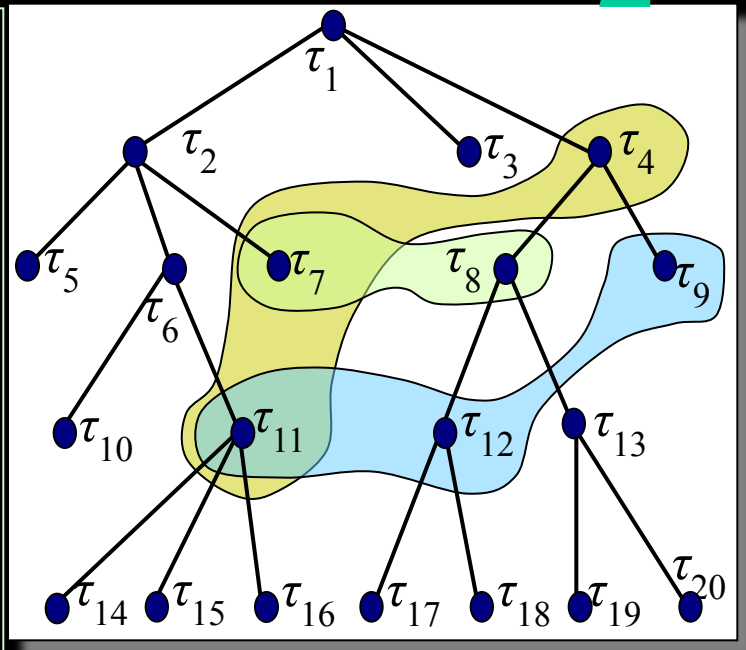
Решетка мультирубрик $\Lambda_{и}(T^{м}, \leq_{м}, \cup_{м}, \cap_{м})$

Определение 2. ***Объединением*** $\cup_{м}$ *мультирубрик* $T^{м}_{i}=\{\tau^{(i)}_{1},\tau^{(i)}_{2},\ldots,\tau^{(i)}_{I}\}$ и $T^{м}_{j}=\{\tau^{(j)}_{1},\tau^{(j)}_{2},\ldots,\tau^{(j)}_{J}\}$ *называется операция формирования множества вершин иерархического рубрикатора* $T^{м\cup} = T^{м}_{i} \cup_{м} T^{м}_{j}$ *на основе следующего алгоритма:*

1) *Формируется теоретико-множественное объединение множеств вершин, составляющих мультирубрики –*
$T^{\cup} = \{\tau^{(i)}_{1}, \tau^{(i)}_{2},\ldots, \tau^{(i)}_{I}\} \cup \{\tau^{(j)}_{1}, \tau^{(j)}_{2},\ldots, \tau^{(j)}_{J}\}$;

2) *Формируется набор вершин* $T^{м\cup'}$ *путем исключения из него тех вершин из* $T^{\cup}$, *которые доминируются хотя бы одной вершиной из того же набора* $T^{\cup}$ –
$(\tau_{k} \in T^{\cup} \wedge \tau_{k} \in T^{м\cup}) \equiv (\exists\, \tau_{m} \in T^{\cup} \wedge \tau_{m} \leq \tau_{k})$;

3) *Формируется итоговый набор вершин* $T^{м\cup}$ *путем добавления в него результатов иерархического сжатия по всем подмножествам набора вершин* $T^{м\cup'}$ *и одновременным исключением соответствующих наборов сыновей при непустом результате сжатия*



$\{\tau_{7}, \tau_{8}\} \cup_{м} \{\tau_{11}, \tau_{12}, \tau_{9}\}$

1) $\{\tau_{7}, \tau_{8}, \tau_{11}, \tau_{12}, \tau_{9}\}$

2) $\{\tau_{7}, \tau_{8}, \tau_{11}, \tau_{9}\}$

3) $\{\tau_{11}, \tau_{7}, \tau_{4}\}$

Лемма 1. *Множество рубрик* $T^{м\cup} = T^{м}_{i} \cup_{м} T^{м}_{j}$, *формируемое на основе объединения мультирубрик по определению 2,*

a) является мультирубрикой;

b) доминирует над мультирубриками $T^{м}_{i}$ *и* $T^{м}_{j}$, *т.е.* $T^{м}_{i} \leq T^{м\cup} \wedge T^{м}_{j} \leq T^{м\cup}$;

c) является наименьшей верхней границей мультирубрик $T^{м}_{i}$ *и* $T^{м}_{j}$.

2. Тематическая решетка мультирубрик иерархического рубрикатора

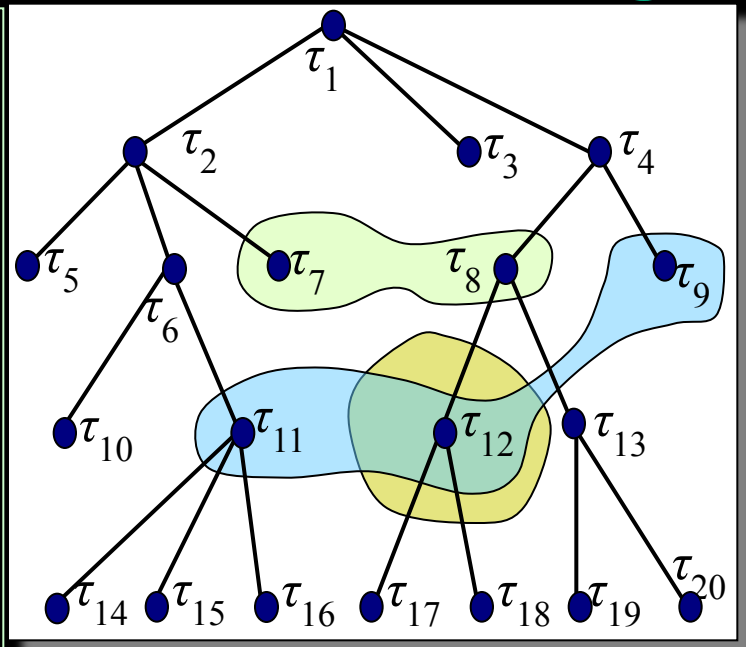
Решетка мультирубрик $\Lambda_{и}(T^{м}, \leq_{м}, \cup_{м}, \cap_{м})$

Определение 3. ***Пересечением*** $\cap_{м}$ *мультирубрик* $T^{м}_{i} = \{\tau^{(i)}_{1}, \tau^{(i)}_{2}, \ldots, \tau^{(i)}_{I}\}$ и $T^{м}_{j} = \{\tau^{(j)}_{1}, \tau^{(j)}_{2}, \ldots, \tau^{(j)}_{J}\}$ *называется операция формирования множества вершин иерархического рубрикатора* $T^{м\cap} = T^{м}_{i} \cap_{м} T^{м}_{j}$ *на основе следующего алгоритма:*

1) *Из множества вершин мультирубрики* $T^{м}_{i} = \{\tau^{(i)}_{1}, \tau^{(i)}_{2}, \ldots, \tau^{(i)}_{I}\}$ *формируются множество вершин* $T^{м\prime}_{i}$, *которые доминируются хотя бы одной вершиной из множества вершин другой мультирубрики* $T^{м}_{j} = \{\tau^{(j)}_{1}, \tau^{(j)}_{2}, \ldots, \tau^{(j)}_{J}\}$;

2) *Из множества вершин мультирубрики* $T^{м}_{j} = \{\tau^{(j)}_{1}, \tau^{(j)}_{2}, \ldots, \tau^{(j)}_{J}\}$ *формируются множество вершин* $T^{м\prime}_{j}$, *которые доминируются хотя бы одной вершиной из множества вершин первой мультирубрики* $T^{м}_{i} = \{\tau^{(i)}_{1}, \tau^{(i)}_{2}, \ldots, \tau^{(i)}_{I}\}$;

3) *Формируется теоретико-множественное объединение* $T^{м\cap} = T^{м\prime}_{i} \cup T^{м\prime}_{j}$



$\{\tau_7, \tau_8\} \cap_{м} \{\tau_{11}, \tau_{12}, \tau_9\}$

1) $\{\tau_7, \tau_8\} \rightarrow \varnothing$

2) $\{\tau_{11}, \tau_{12}, \tau_9\} \rightarrow \{\tau_{12}\}$

3) $\varnothing \cup \{\tau_{12}\} = \{\tau_{12}\}$

Лемма 2. *Множество рубрик* $T^{м\cap} = T^{м}_{i} \cap_{м} T^{м}_{j}$, *формируемое на основе пересечения мультирубрик по определению 3,*

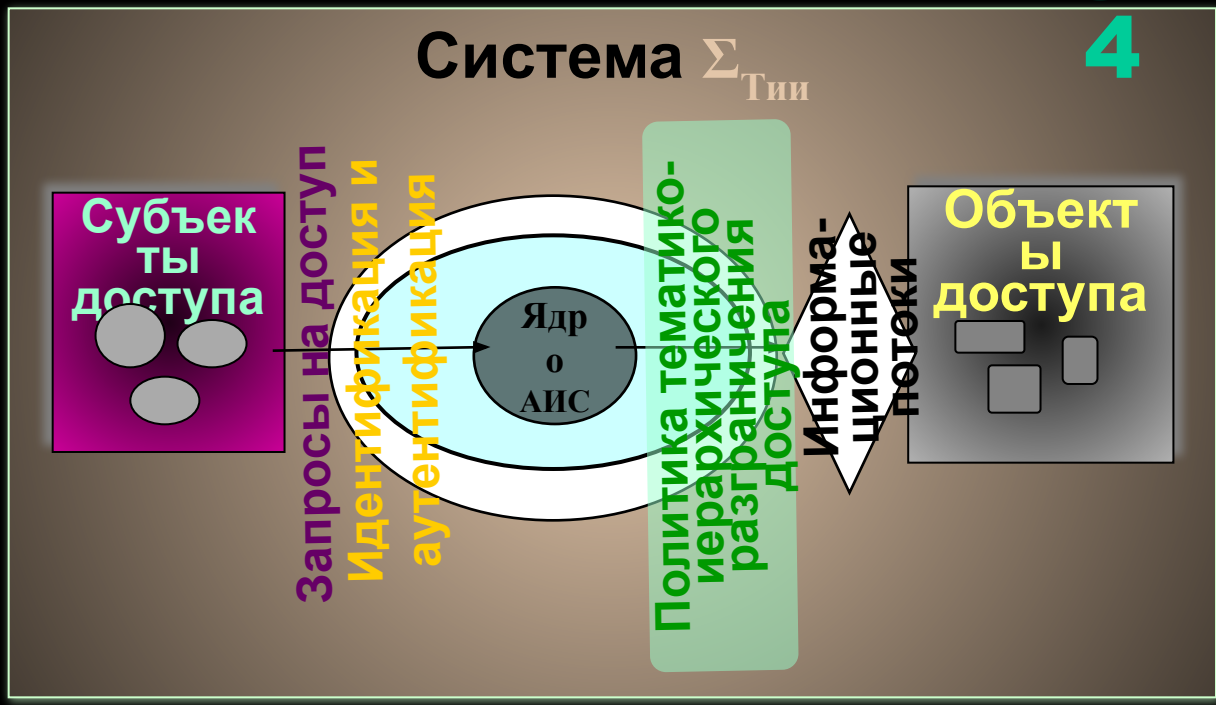
a) является мультирубрикой;

b) доминируется мультирубриками $T^{м}_{i}$ *и* $T^{м}_{j}$, *т.е.* $T^{м\cap} \leq T^{м}_{i} \wedge T^{м\cap} \leq T^{м}_{j}$;

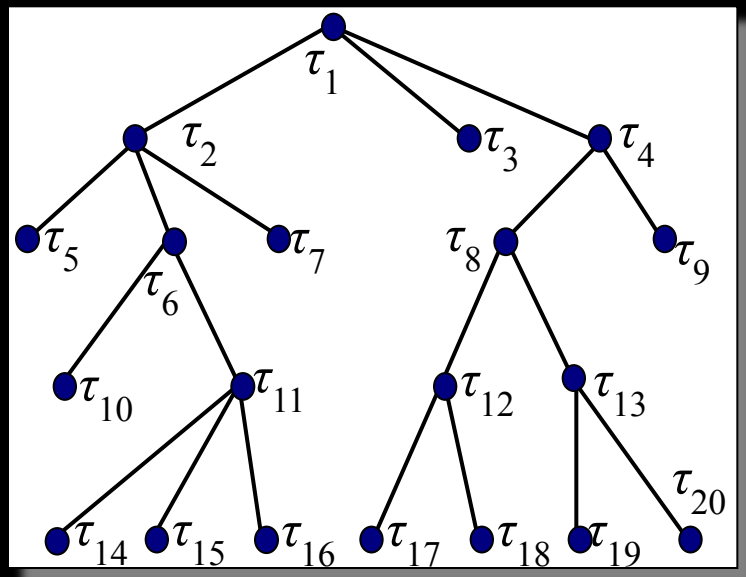
c) является наибольшей нижней границей мультирубрик $T^{м}_{i}$ *и* $T^{м}_{j}$.

3. Модель тематико-иерархического разграничения доступа

1. Компьютерная система $\Sigma_{Тии}$ представляется совокупностью субъектов и объектов доступа. В системе $\Sigma_{Тии}$ действует **МБО**, санкционирующий запросы субъектов на доступ к объектам, и **МБС**, управляющий инициализацией субъектов



2. Информационно-логическая схема предметной области системы $\Sigma_{Тии}$ представляется тематическим иерархическим классификатором (рубрикатором). Рубрикатор включает конечное множество тематических рубрик $T_и = \{\tau_1, \tau_2, \ldots, \tau_M\}$, на котором установлен частичный порядок, задаваемый корневым деревом



3. Модель тематико-иерархического разграничения доступа

3. Множество сущностей системы $X = S \cup O$ тематически классифицируется на основе отображения на множество мультирубрик $T^{м}$, определенных на корневом дереве иерархического рубрикатора.

Существует функция тематического окрашивания $f_{м}$, которая в каждый момент времени для любой сущности системы $x \in X$ определяет соответствующую ей мультирубрику:

$$f_{м}[x] = \mathcal{T}^{м}_{i}, \quad \mathcal{T}^{м}_{i} \in T^{м}.$$

4. **Тематический критерий безопасности.** *Система* $\Sigma_{Тии}$ *безопасна тогда и только тогда, когда в ней отсутствуют потоки следующих видов:*

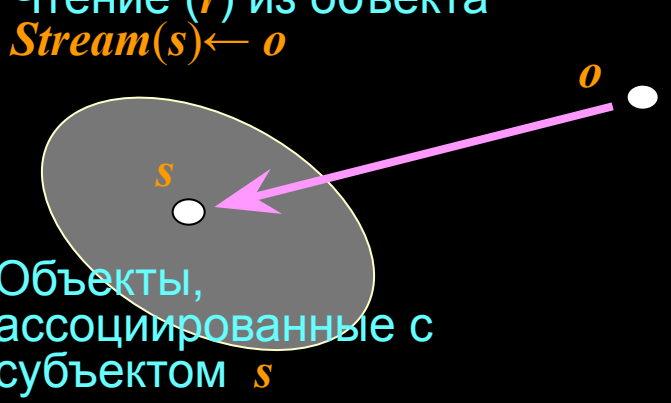
- *от сущностей с более широкой тематикой к сущностям с более узкой тематикой;*
- *между несравнимыми по тематике сущностями.*

3. Модель тематико-иерархического разграничения доступа

5. Переходы системы $\Sigma_{\text{Тии}}$, обусловленные запросами и осуществлением доступов существующих субъектов к существующим объектам, санкционируются МБО на основе следующих правил:

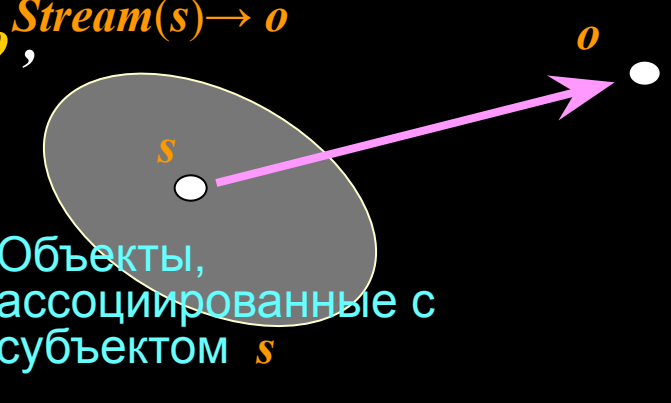
Правило 1. *Доступ субъекта s к объекту o, вызывающий поток по чтению Stream(s)←o , неопасен и может быть МБО разрешен тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта:*

$$f_{\text{м}}[s] \geq f_{\text{м}}[o]$$



Правило 2. *Доступ субъекта s к объекту o, вызывающий поток по записи Stream(s)→o, неопасен и может быть МБО разрешен тогда и только тогда, когда мультирубрика объекта доминирует над мультирубрикой субъекта:*

$$f_{\text{м}}[o] \geq f_{\text{м}}[s]$$



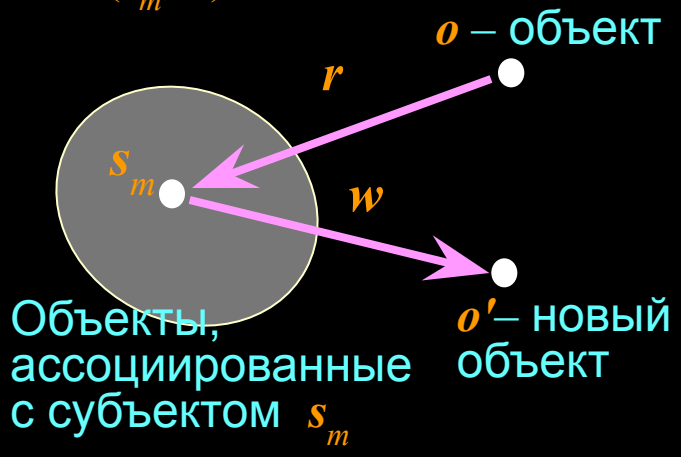
3. Модель тематико-иерархического разграничения доступа

6. Переходы системы $\Sigma_{\text{Тии}}$, связанные с порождением новых объектов и субъектов доступа, санкционируются МБО и МБС на основе следующих правил:

Правило 3. *Порождение субъектом s нового объекта o', в том числе и за счет чтения из другого объекта o, неопасно и может быть МБО разрешено тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта o, при этом МБО присваивает новому объекту o' мультирубрику, равную или доминирующую над мультирубрикой субъекта:*

$$f_{\text{м}}[o] \le f_{\text{м}}[s] \le f_{\text{м}}[o']$$

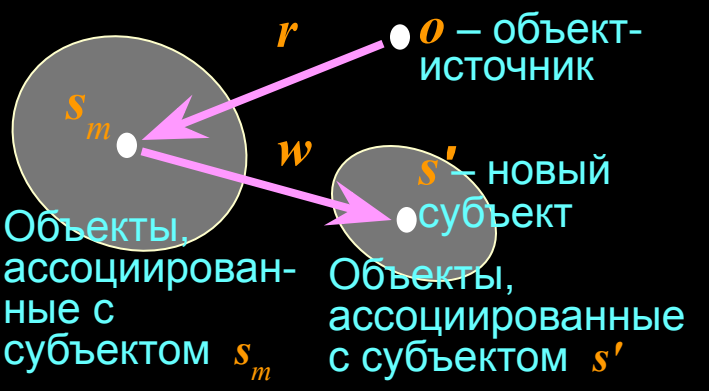
Создание нового объекта $Create(s_m, o) \to o'$



Правило 4. *Инициализация субъектом s нового субъекта s' посредством воздействия на объект источник o неопасна и может быть МБС разрешена тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта-источника, при этом МБС присваивает новому субъекту мультирубрику, тождест-венную мультирубрике инициализирующего субъекта:*

$$f_{\text{м}}[o] \le f_{\text{м}}[s] \equiv f_{\text{м}}[s']$$

Инициализация нового субъекта $Create(s_m, o) \to s'$



3. Модель тематико-иерархического разграничения доступа

7. Переходы системы $\Sigma_{\text{Тии}}$, обусловленные запросами на предоставление множественных доступов, санкционируются МЯО на основе следующего правила:

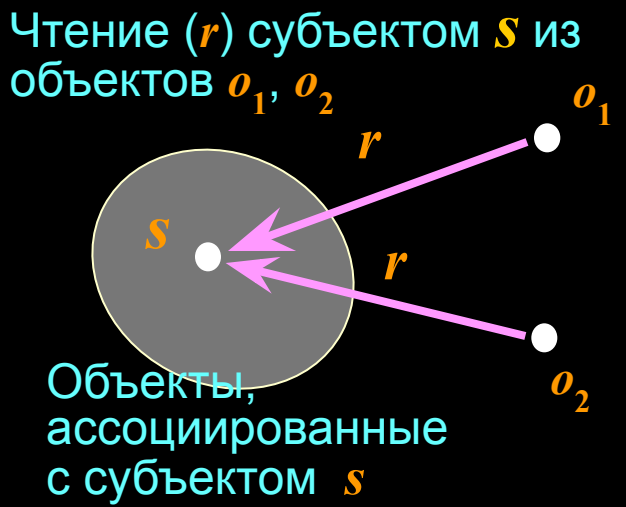
Правило 5. ***Одновременный множественный доступ субъекта s к объектам o_1, o_2,… или субъектов s_1, s_2,… к объекту o может быть разрешен (неопасен) тогда и только тогда, когда выполняются следующие условия:***

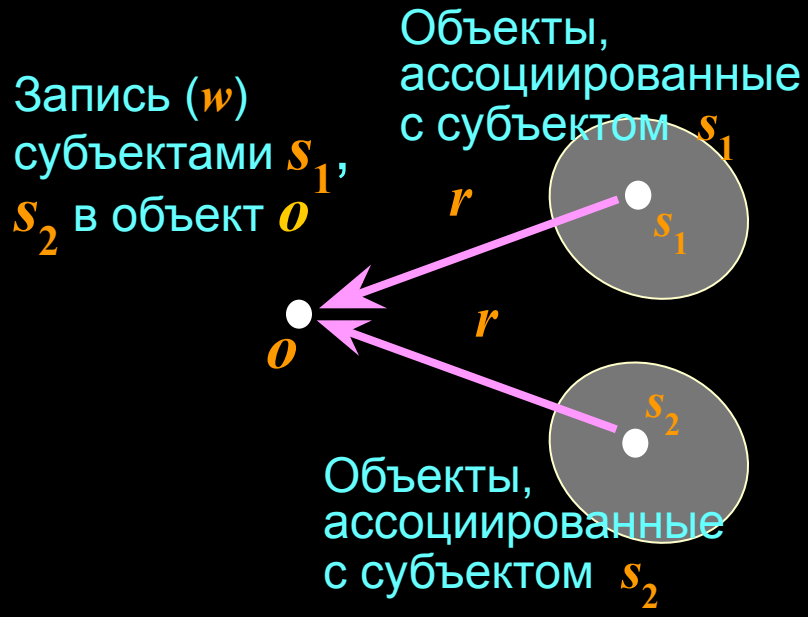
- ***при доступе по чтению***

$$f_{\text{м}}[s] \geq \cup_{\text{м}}\{f_{\text{м}}[o_1], f_{\text{м}}[o_2],\ldots\}$$
$$f_{\text{м}}[o] \leq \cup_{\text{м}}\{f_{\text{м}}[s_1], f_{\text{м}}[s_2],\ldots\}$$

- ***при доступе по записи***

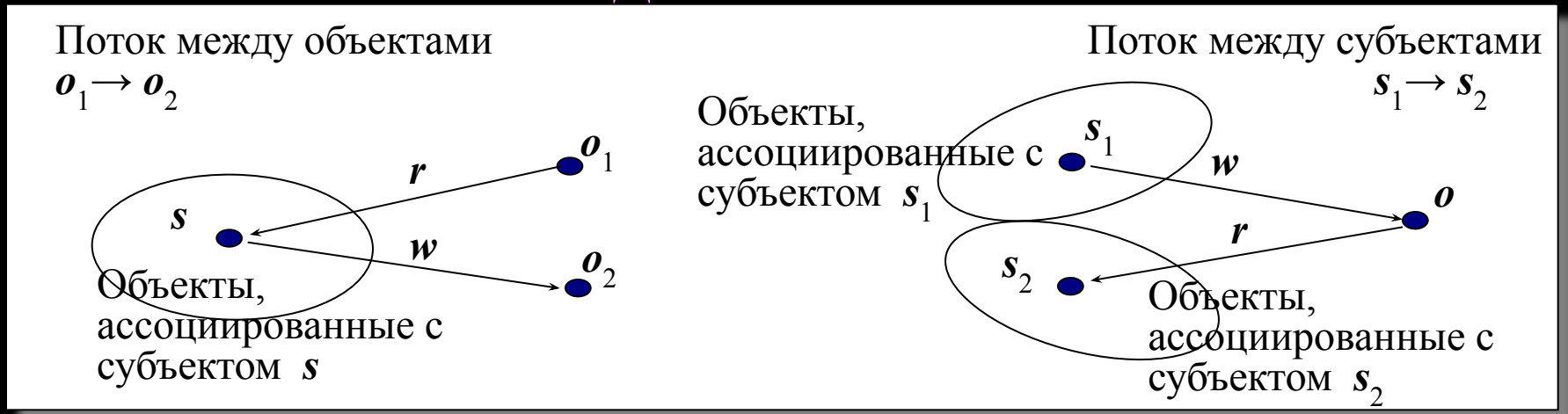
$$f_{\text{м}}[s] \leq \cap_{\text{м}}\{f_{\text{м}}[o_1], f_{\text{м}}[o_2],\ldots\}$$
$$f_{\text{м}}[o] \geq \cap_{\text{м}}\{f_{\text{м}}[s_1], f_{\text{м}}[s_2],\ldots\}$$





Теорема 1. *В системе $\Sigma_{\text{Тии}}$ с отображением множества субъектов и объектов доступа на множество тематических мультирубрик, в которой доступы санкционируются по правилам 1, 2, 3, 4 и 5, реализуется множество только таких потоков, которые удовлетворяют тематическому критерию безопасности*

Доказательство



По условиям теоремы при санкционировании потока $o_1 \to o_2$ имеем:

$$f_{\text{м}}[s] \geq f_{\text{м}}[o_1] \quad \wedge \quad f_{\text{м}}[o_2] \geq f_{\text{м}}[s]$$

Отсюда следует, что: $f_{\text{м}}[o_2] \geq f_{\text{м}}[o_1]$

Аналогично по условиям теоремы при санкционировании потока $s_1 \to s_2$ имеем

$$f_{\text{м}}[s_1] \leq f_{\text{м}}[o] \quad \wedge \quad f_{\text{м}}[s_2] \geq f_{\text{м}}[o] .$$

Отсюда следует, что: $f_{\text{м}}[s_2] \geq f_{\text{м}}[s_1]$

Тема 2. Модели безопасности компьютерных систем

Лекция 2.4.

Модели безопасности на основе ролевой политики

Учебные вопросы:

1. Модели ролевого доступа
2. Модели индивидуально-группового доступа
3. MMS-модель

Литература:

1. **Зегжда Д.П.,Ивашко А.М.** Основы безопасности информационных систем. - М.:Горячая линия - Телеком, 2000. - 452с
2. **Гайдамакин Н.А.** Разграничение доступа к информации в компьютерных системах. - Екатеринбург: Изд-во Урал. Ун-та, 2003. – 328 с.
3. **Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240с.**
4. **Девянин П.Н.** Модели безопасности компьютерных систем: Учеб. Пособие. – М.Издательский центр «Академия», 2005. – 144с.

1. *Модели ролевого доступа*

Осн. идея:
-политика и система защиты должны учитывать
организационно-технологическое взаимодействие пользователей

Впервые в продуктах управления доступом корп. IBM(70-80.гг.)

Вместо субъекта
- ***пользователь*** (конкретная активная сущность)
- ***роль*** (абстрактная активная сущность)

Неформально ***Роль***: - типовая работа в КС (ИС) определенной группы пользователей

Аналог -нормативное положение, функциональные обязанности и права сотрудников по определенной должности

например м.б. роли-
кассира, бухгалтера, делопроизводителя, менеджера и т.п.

Формально ***РОЛЬ*** - активно действующая в КС абстрактная сущность, обладающая логически взаимосвязанным набором полномочий, необходимых для выполнения определенных функциональных обязанностей

- выделенная и обособленная совокупность полномочий над определенной группой или тематикой ресурсов (объектов), имеющая отдельное и самостоятельное значение в предметной области КС (ИС)

1. *Модели ролевого доступа*

Организация доступа в ***две стадии***-

-создаются роли и для каждой из них определяются полномочия

-каждому пользователю назначается список доступных ролей

Система защиты при ролевой политики

U - множество пользователей;

$\mathcal{R}$ - множество ролей;

P - множество полномочий на доступ к объектов;

S - множество сеансов системы

Устанавливаются ***отношения:***

$F_{P\mathcal{R}}$ - P x $\mathcal{R}$ - отображение множества полномочий на множество ролей, например в виде ролевой матрицы доступа ($A_{p\rho}$)

$F_{U\mathcal{R}}$ - U x $\mathcal{R}$ - отображение множества пользователей на множество ролей, например, в виде матрицы "пользователи-роли", задающая набор доступных пользователю ролей ($A_{u\rho}$)

1. Модели ролевого доступа

Устанавливаются ***функции:***

f_{user} - $S \rightarrow U$ - для каждого сеанса s функция f_{user} определяет пользователя, который осуществляет этот сеанс работы с системой - $f_{user}(s)=u$

f_{roles} - $S \rightarrow P(\mathcal{R})$ - для каждого сеанса s функция f_{roles} определяет набор ролей, которые могут быть одновременно доступны пользователю в этом сеансе:

$f_{roles}(s)=\{\rho_i \mid (f_{user}(s), \rho_i) \in A_{up}\}$

$f_{permissions}$ - $S \rightarrow P$ - для каждого сеанса s функция $f_{permissions}$ задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе

$f_{permissions}(s)= \bigcup_{\rho \in froles(s)} \{p_i \mid (p_i, \rho) \in A_{pp}\}$

Критерий безопасности:

-система считается безопасной, если любой пользователь, работающий в сеансе s, может осуществить действия, требующие полномочий p, только в том случае , если

$p=f_{permissions}(s)$

1. Модели ролевого доступа

Ролевая политика – особый тип политики, основанный на ***компромиссе*** между ***гибкостью*** *управлением доступа* ***дискреционных*** *моделей и* ***жесткостью*** *правил контроля доступа* ***мандатных*** *моделей*

Разновидности *ролевых моделей определяется особенностями функций* f_{user}, f_{roles}, $f_{permissions}$, *и ограничений, накладываемых на отношения* A_{pp} *и* A_{up}

Наиболее распространены модели с ***иерархической организацией ролей***

-чем выше роль по иерархии, тем больше полномочий

-если пользователю присвоена какая-то роль, то ему автоматически присваиваются все роли ниже по иерархии

Отношения и функции при иерархической организации ролей

Отношения:

F^h_{RR} - R x R - частичное отношение порядка на множестве R, которое определяет иерархию ролей и задает на множестве R оператор доминирования $\geq$, такой, что если $\rho_1 \geq \rho_2$, то роль ρ_1 находится выше по иерархии, чем роль ρ_2

F^h_{UR} - U x R - назначает каждому пользователю набор ролей, причем вместе с каждой ролью в него (набор ролей) включаются все роли, подчиненные ей по иерархии, т.е. для $\forall\ \rho, \rho' \in R, u \in U: \rho \geq \rho' \wedge (u,\rho) \in A^h_{u\rho} \Rightarrow (u,\rho') \in A^h_{u\rho}$

Функции:

f^h_{roles} - $S \rightarrow (R)$ – назначает каждому сеансу s определяет набор ролей из иерархии ролей пользователя, работающего в этом сеансе: $f^h_{roles}(s)=\{\rho_i \mid (\exists\ \rho' \geq \rho_i (f_{user}(s), \rho') \in A^h_{u\rho})\}$

$f^h_{permissions}$ - $S \rightarrow P$ – определяет полномочия сеанса s как совокупность полномочий всех задействованных пользователем в нем ролей и полномочий всех ролей, подчиненных им: $f^h_{permissions}(s)= \cup_{\rho \in f^h_{roles}(s)} \{p_i \mid (\exists\ \rho'' \leq \rho\ (p_i,\rho'') \in A_{p\rho})\}$

Агрегация прав при иерархической организации ролей (виды отношения $\mathcal{F}_{PR}$)

- строго таксономический листовой подход;
- нетаксономический листовой подход;
- иерархически охватный подход

Строго таксономический листовой подход

$$\mathcal{F}^h_{PR}(\rho^{л}_j) = \{p^{(j)}_1, p^{(j)}_2, \dots\},$$

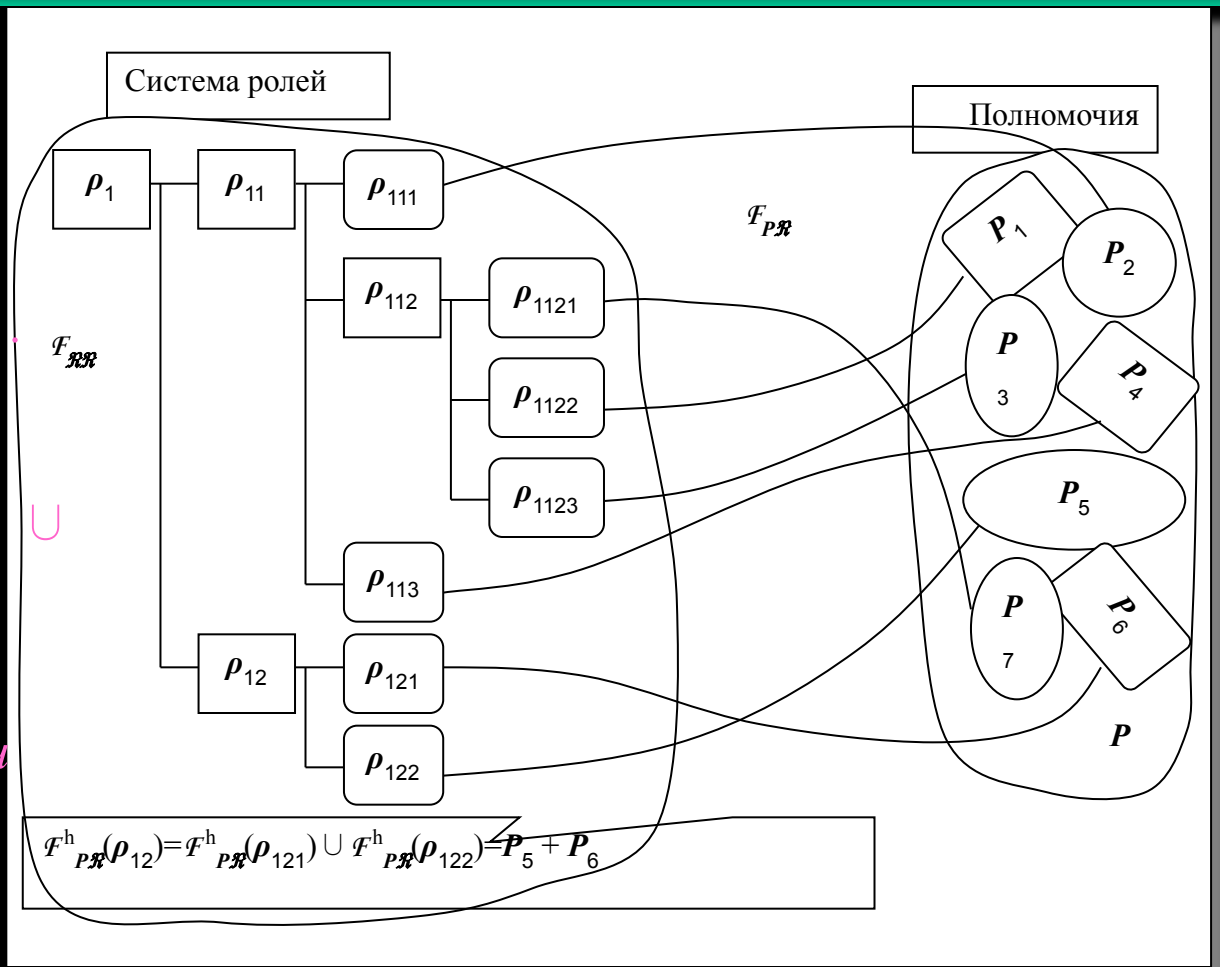
$$\mathcal{F}^h_{PR}(\rho^{л}_j) \cap \mathcal{F}^h_{PR}(\rho^{л}_i) \cap \dots = \varnothing,$$

$$\mathcal{F}^h_{PR}(\rho^{л}_j) \cup \mathcal{F}^h_{PR}(\rho^{л}_i) \cup \dots = P.$$

$$\mathcal{F}^h_{PR}(\rho^{и}_k) = \mathcal{F}^h_{PR}(\rho^{(k)}_i) \cup \mathcal{F}^h_{PR}(\rho^{(k)}_j) \cup \dots,$$

где $\{\rho^{(k)}_i, \rho^{(k)}_j, \dots\}$ *– полный набор ролей-сыновей для роли* $\rho^{и}_k$.

$$\mathcal{F}^h_{PR}(\rho^{и}_1) = P$$



Агрегация прав при иерархической организации ролей (виды отношения $\mathcal{F}_{PR}$)

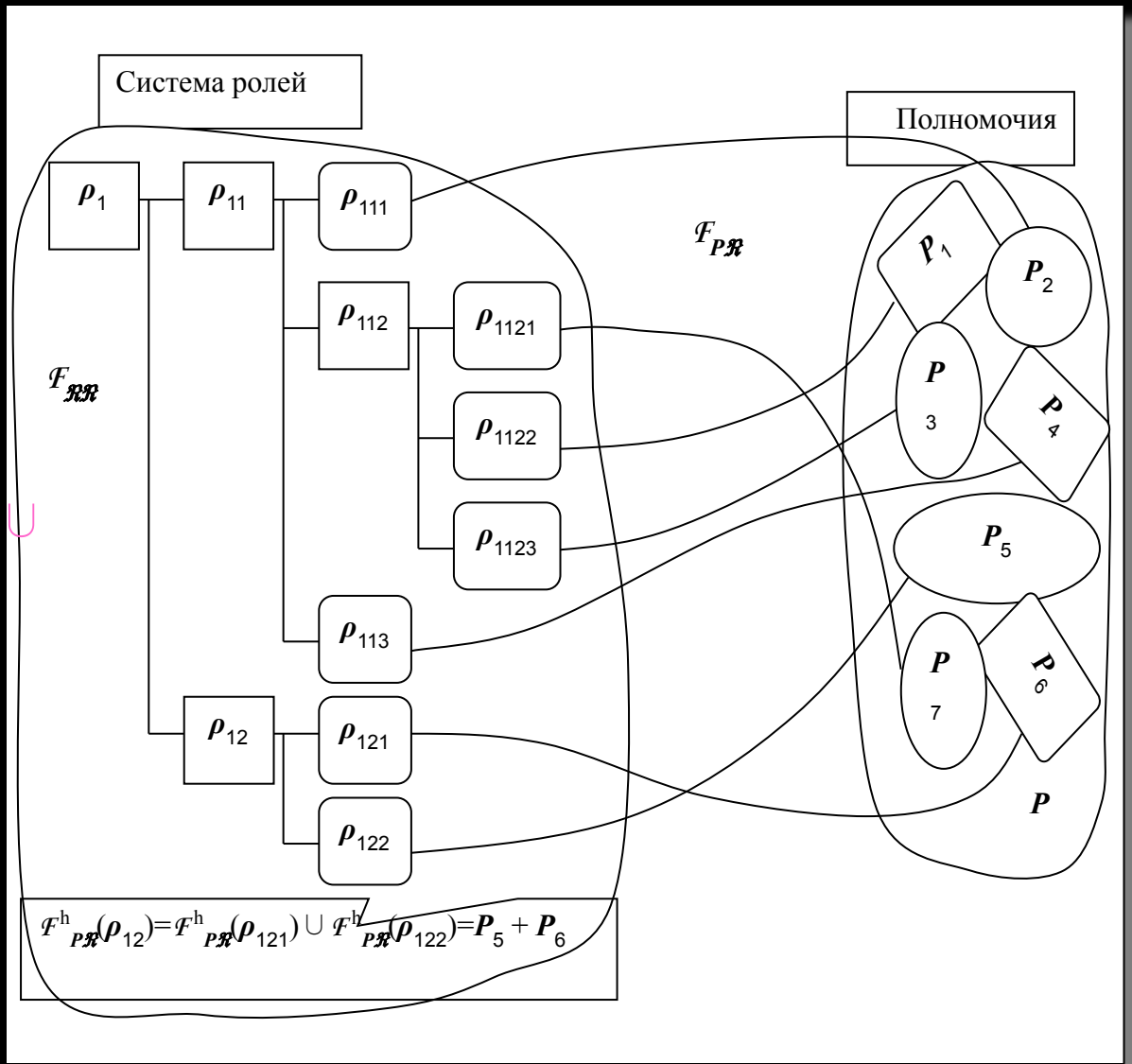
Нетаксономический листовой подход

$$\mathcal{F}^h_{PR}(\rho^{л}_j) = \{p^{(j)}_1, p^{(j)}_2, \dots\},$$

$$\mathcal{F}^h_{PR}(\rho^{л}_j) \cap \mathcal{F}^h_{PR}(\rho^{л}_i) \cap \dots \neq \varnothing,$$

$$\mathcal{F}^h_{PR}(\rho^{и}_k) = \mathcal{F}^h_{PR}(\rho^{(k)}_i) \cup \mathcal{F}^h_{PR}(\rho^{(k)}_j) \cup \dots,$$

где $\{\rho^{(k)}_i, \rho^{(k)}_j, \dots\}$ *– полный набор ролей-сыновей для роли* $\rho^{и}_k$.



Агрегация прав при иерархической организации ролей (виды отношения $\mathcal{F}_{PR}$)

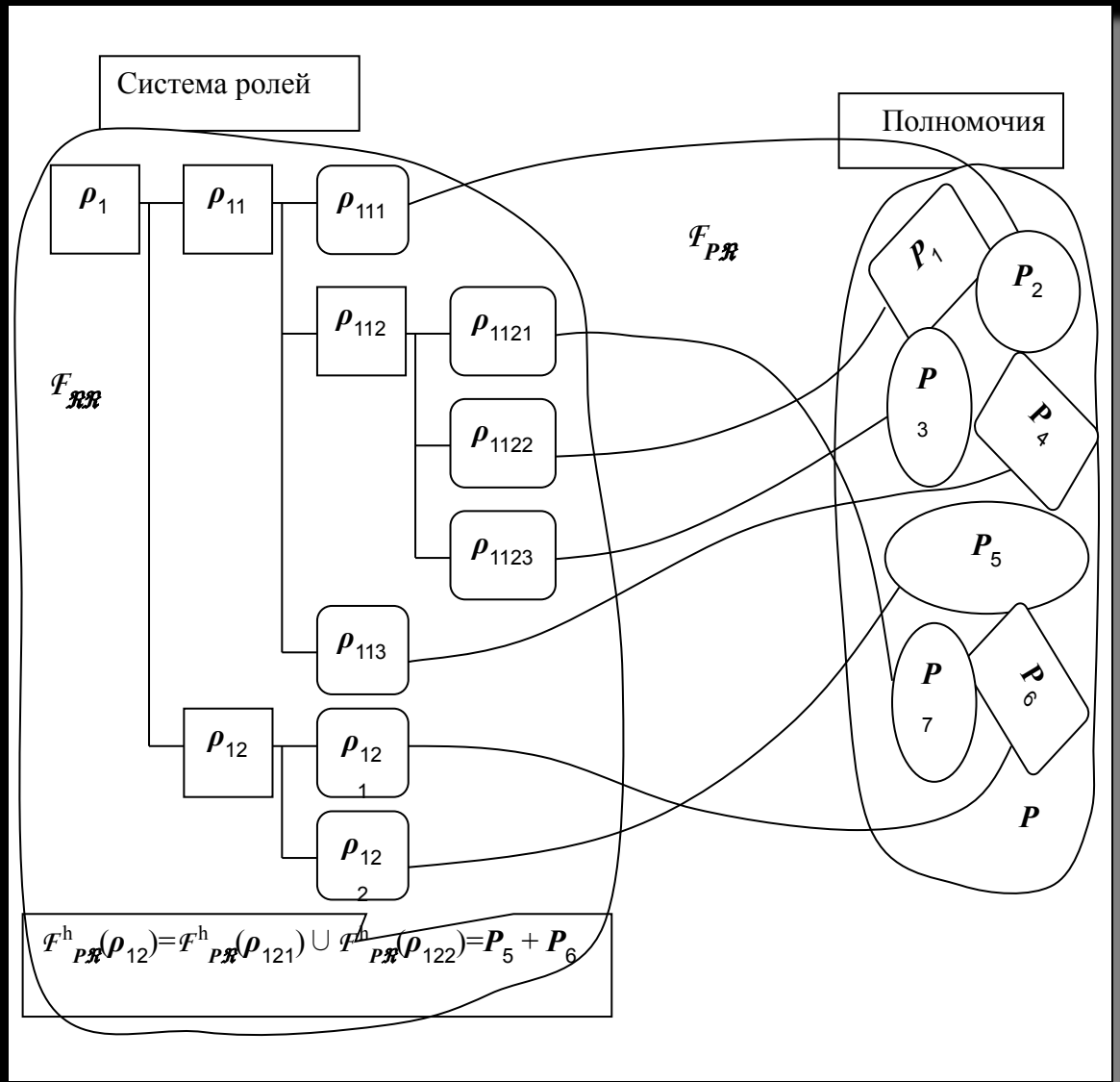
Иерархически охватный подход

$$\mathcal{F}^h_{PR}(\rho^{л}_j) = \{p^{(j)}_1, p^{(j)}_2, \dots\},$$

$$\mathcal{F}^h_{PR}(\rho^{л}_j) \cap \mathcal{F}^h_{PR}(\rho^{л}_i) \cap \dots \neq \varnothing,$$

$$\mathcal{F}^h_{PR}(\rho^{и}_k) \cap \mathcal{F}^h_{PR}(\rho_i) = \varnothing,$$

где $\{\rho^{и}_k \geq \rho_i\}$.



Другие разновидности организации ролей

т.н. ***статическое разделение обязанностей***

Взаимоисключающие роли

- множество ролей разбивается на подмножества, объединяющие роли, которые не м.б. назначены одновременно одному пользователю (z.b. "кассир"-"контроллер"). Задается функция $f_{exclusive}: \mathcal{R} \rightarrow P(\mathcal{R})$, которая для каждой роли определяет множество несовместимых с ней ролей.

т.н. ***динамическое разделение обязанностей***

Ограничения на одновременное использование ролей в одном сеансе

- множество ролей разбивается на подмножества, несовместимых ролей(z.b. "администратор"-"аудитор"). В ходе одного сеанса пользователь может активизировать из каждого подмножества не более одной роли.

Количественные ограничения по назначению ролей одному пользователю

Групповое назначение ролей одному пользователю

- роль м.б. назначена тогда, когда одновременно назначена еще группа обязательных для данной роли других ролей

2. Модели индивидуально-группового доступа

1. КС представляется совокупностью следующих наборов сущностей:

множества объектов доступа $O\ (o_1, o_2, \ldots, o_M)$;

множества пользователей $U\ (u_1, u_2, \ldots, u_N)$;

множества рабочих групп пользователей $G\ (g_1, g_2, \ldots, g_K)$;

множества прав доступа и привилегий $R\ (r_1, r_2, \ldots, r_J)$;

матрицей доступа A размерностью $((N+K) \times M)$, каждая ячейка которой специфицирует права доступа и привилегии пользователей или их рабочих групп к объектам из конечного набора прав доступа и привилегий $R\ (r_1, r_2, \ldots, r_J)$, т. е. $A[u, o] \subseteq R$, $A[g, o] \subseteq R$.

Определение. **Рабочей группой** называется совокупность пользователей, объединенных едиными правами доступа к объектам и (или) едиными привилегиями (полномочиями) выполнения определенных процедур обработки данных

Рабочая группа в отличие от роли не является самостоятельным субъектом доступа

$A=$

Группы Пользователи	Объекты o_1	o_2	. . .			o_M
u_1						
u_2						
				a_{ij}		
u_N						
g_1						
g_K						

2. Модели индивидуально-группового доступа

2. Групповые отношения в системе устанавливаются отображением множества пользователей на множество рабочих групп:

$\mathcal{F}_{UG} : U \times G$ – такое, что одна рабочая группа объединяет нескольких пользователей, а один пользователь может входить в несколько рабочих групп.

$f_{groups}: U \rightarrow G$ – значением функции $f_{groups}(u) = G$ является набор рабочих групп $G = \{g_{u1}, g_{u2}, \ldots\} \subseteq G$, в которые пользователь u включен по отображению $\mathcal{F}_{UG}$;

$f_{users}: G \rightarrow U$ – значением функции $U = f_{users}(g)$ является набор пользователей $U = \{u_{g1}, u_{g2}, \ldots\} \subseteq U$, которые рабочая группа g включает по отношению $\mathcal{F}_{UG}$.

Рабочие группы

$W =$

Пользователи	g_1	g_2	. . .			g_K
u_1		0				
u_2						
				1		
u_N						

Отношение «Пользователи-группы» - «многие-ко-многим»

2. *Модели индивидуально-группового доступа*

3. Управление индивидуально-групповым доступом в системе осуществляется на основе следующего правила (критерия безопасности) индивидуально-группового доступа.

Критерий безопасности индивидуально-группового доступа: *Система функционирует безопасно, если и только если любой пользователь* $u \in U$ *по отношению к любому объекту* $o \in O$ *может осуществлять доступ с правами* $\mathcal{R}$*, не выходящими за пределы совокупности индивидуальных прав* $A[u,o]$ *и прав рабочих групп* $A[g^u_i,o]$*, в которые пользователь входит по отношению* $\mathcal{F}_{UG}$:

$$\mathcal{R} \subseteq \{A[u,o] \cup A[g^u_1, o] \cup A[g^u_2, o] \cup \ldots\},$$

где $\{ g^u_1, g^u_2, \ldots\} = f_{\text{groups}}(u)$.

Разделение процесса функционирования на КС не является существенным, поскольку пользователь всегда получает полномочия всех групп, в которые входит

2. *Модели индивидуально-группового доступа*

4. Членами рабочих групп могут быть *коллективные члены*, т.е. другие рабочие группы. Вхождение одних групп в другие д.б. *транзитивно*, *антисимметрично* и *рефлексивно*:

$\mathcal{F}_{GG} : G \times G$ - отношение частичного порядка, определяющее иерархию (вложенность) рабочих групп и задающее оператор доминирования $\geq$ такое, что

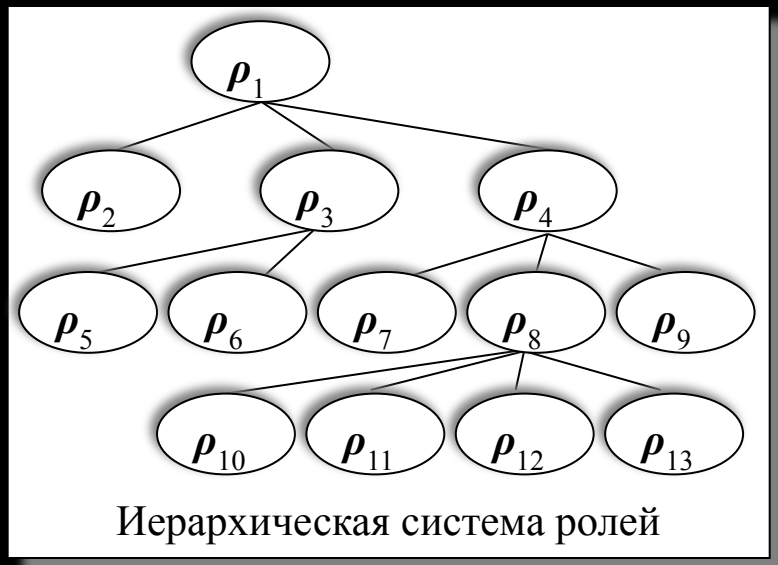
если для $g_1, g_2 \in G$, $g_1 \geq g_2$, то g_1 включает g_2 .

$f_{\text{hgroups}} : G \rightarrow G$ – значением функции $f_{\text{groups}}(g)$ является набор рабочих групп $\{g_{g1}, g_{g2}, \ldots\} \subseteq G$, в которые рабочая группа g включена по отношению $\mathcal{F}_{GG}$.

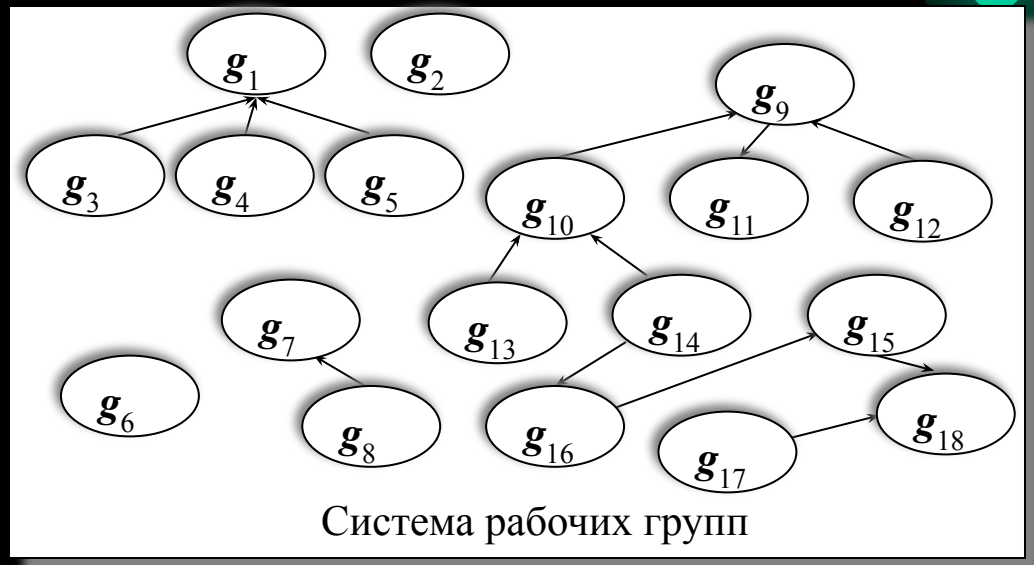
Наследование прав по групповой иерархии происходит «сверху-вниз»

$\mathcal{R}_g = A[g,o] + A[g_{g1},o] + A[g_{g2},o] + \ldots$, где $\{g_{g1}, g_{g2}, \ldots\} = f_{\text{groups}}(g)$

2. Модели индивидуально-группового доступа



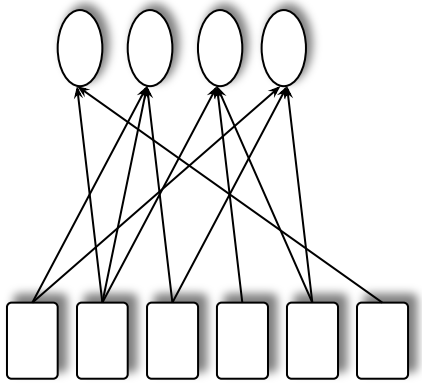
Иерархическая система ролей



Система рабочих групп

5. На графе вхождения одних групп в другие не должно быть циклов

Теоретико-графовые методы поиска циклов, в т.ч. по матрице смежности



Группы, которые не могут входить в другие группы, но могут включать как пользователей, так и группы

Группы, включающие только пользователей

3. *MMS (military message system)-модель*

Лендвер, МакЛин, 1984г.

Определения MMS-модели (*формализация системы защиты*)

Классификация- обозначение, накладываемое на информацию, отражающее ущерб, который м.б. причинен неавторизованным доступом (TOP SECRET, SECRET, + возможно дополн. функц. разгр. - CRYPTO, NUCLEAR и т.п.)

Степень доверия пользователю- уровень благонадежности персоны (иначе допуск пользователя) - априорно заданная характеристика

Пользовательский идентификатор- строка символов, используемая для того, чтобы отметить пользователя в системе. Для использования системы пользователь д. предъявить ей идентификатор, система должна провести аутентификацию пользователя (login)

Пользователь- персона, уполномоченная для использования системы

Роль - работа, исполняемая пользователем. Пользователь в любой момент времени (после login до logon) всегда ***ассоциирован*** как минимум с одной ролью из нескольких. Для действий в данной роли пользователь д.б. ***уполномочен***. Некоторые роли в конкр. момент времени м.б. связаны *только с одним пользователем*. С любой ролью связана способность выполнения определенных ***операций***

Объект- одноуровневый блок информации. Это минимальный блок информации в системе, который м. иметь классификацию, т.е. м.б. раздельно от других поименован. Объект не содержит других объектов (т.е. он не многоуровневый)

3. *MMS (military message system)-модель*

Определения MMS-модели (продолжение)

Контейнер- многоуровневая информационная структура. Имеет классификацию и м. содержать объекты (со своей классификацией) и др. контейнеры (также со своей классификацией)

Сущность- объект или контейнер

Требование степени доверия объектов- атрибут некоторых контейнеров. Для некоторых контейнеров важно требовать минимум степени доверия, т.е. пользователь, не имеющий соответствующего уровня благонадежности, не может просматривать содержимое контейнера. Такие контейнеры помечаются соотв. атрибутом.

Идентификатор (ID)- имя сущности без ссылки на другие сущности

Ссылка на сущность ***прямая-*** если это идентификатор сущности

Ссылка на сущность ***косвенная-*** если это последовательность двух и более идентификаторов (имен) сущностей, первая из которых - контейнер.

Операция- функция, которая м.б. применена к сущности (читать, модифицировать и т.д.). Некоторые операции м. использовать более одной сущности (z.b. Copy)

Множество доступа- множество троек (*Пользовательский идентификатор* или *роль* - *Операция* - *Индекс операнда*), которое связано с сущностью (т.е. дескрипторы доступа объекта)

3. *MMS (military message system)-модель*

Основная схема функционирования системы -пользователи после ***идентификации*** запрашивают у системы операции над сущностями от своего ***ID*** или от имени ***Роли***, с которой в данный момент ***авторизованы***

Система функционирует безопасно, если

-пользователи ведут себя корректно (не компрометируют систему) на основе некоторых предположений

- система защиты (монитор безопасности) реализует определенные ограничения политики безопасности)

Предположения MMS-модели*,которым д. следовать* ***пользователи*** *системы*

A1. Администратор безопасности корректно присваивает уровни доверия, классификацию устройств и правильные множества ролей

A2. Пользователь определяет корректную классификацию, когда вводит, изменяет, объединяет или переклассифицирует информацию

A3. В пределах установленной классификации пользователь классифицирует сообщения (информацию) и определяет набор (множество) доступа (роли,операции,требуемые степени доверия) для сущностей, которые он создает

A4. Пользователь должным образом контролирует информацию объектов, требующих благонадежности

3. *MMS (military message system)-модель*

Ограничения безопасности в MMS-модели

B1. Авторизация - пользователь м. запрашивать операции над сущностями, если только пользовательский идентификатор или его текущая роль присутствуют в множестве доступа сущностей вместе с этой операцией и с этим значением индекса, соответствующим позиции операнда,в которой сущность относят в требуемой операции

B2. Классификационная иерархия - классификация контейнера всегда больше или равна классификации сущностей, которые он содержит

B3. Изменения в объектах - информация, переносимая из объекта всегда содержит классификацию объекта. Информация, вставляемая в объект, должна иметь классификацию ниже классификации этого объекта (аналог NWD)

B4. Просмотр - пользователь может просматривать (на некотором устройстве вывода) только сущности с классификацией меньше, чем классификация устройства вывода и степень доверия контейнера устройства вывода к пользователям (аналог NRU + NRUустроств)

B5. Доступ к объектам, требующим степени доверия - пользователь может получить доступ к косвенно адресованной сущности внутри контейнера, требующего степени доверия, если только его степень доверия не ниже классификации контейнера

B6. Преобразование косвенных ссылок - пользовательский индикатор признается законным для сущности, к которой он обратился косвенно, если только он авторизован для просмотра этой сущности через ссылку

3. *MMS (military message system)-модель*

Ограничения безопасности в MMS-модели (*продолжение*)

B7. Требование меток - сущности, просмотренные пользователем, д.б. помечены его степенью доверия (т.е. впоследствии они ему доверяют)

B8. Установка степеней доверия, ролей, классификация устройств - только пользователь с ролью администратора безопасности системы м. устанавливать данные значения. Текущее множество ролей пользователя м.б. изменено только администратором безопасности системы или самим же этим пользователем

B9. Понижение классификации информации - никакая классифицированная информация не м.б. понижена в уровне своей классификации, за исключением случая, когда эту операцию выполняет пользователь с ролью "Пользователь, уменьшающий классификацию информации"

B10. Уничтожение - операция уничтожения информации проводится только пользователем с ролью "Пользователь, уничтожающий информацию"

Модель Лендвера-Маклина (MMS) сочетает принципы:

ролевого, дискреционного и мандатного принципов и оказывает сильное влияние на модели и технологии современных защищенных КС

Тема 2. **Модели безопасности компьютерных систем**

Лекция 2.5. Автоматные и теоретико-вероятностные модели невлияния и невыводимости

Учебные вопросы:

1. Понятие и общая характеристика скрытых каналов утечки информации
2. Автоматная модель невлияния Гогена-Месигера (GM-модель)
3. Теоретико-информационные модели невыводимости и невлияния (невмешательства)

Литература:

1. **Теория и практика обеспечения информационной безопасности** / Под ред. **П.Д. Зегжды.** М.: Яхтсмен, 1996. - 302с
2. **Грушо А.А.,Тимонина Е.Е.**Теоретические основы защиты информации. М.: Яхтсмен, 1996. - 192с
3. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / **П.Н.Девянин, О.О.Михальский, Д.И.Правиков** и др.- М.: Радио и Связь, 2000. - 192с.
4. **Корт СС.** Теоретические основы защиты информации: Учебное пособие. - М.: Гелиос АРВ, 2004. – 240с.
5. **Девянин П.Н.** Модели безопасности компьютерных систем: Учеб. пособие. – М.: Изд.центр «Академия», 2005. – 144 с.

1. Понятие и общая характеристика скрытых каналов утечки информации

Одна из самых сложных проблем безопасности КС: скрытые каналы утечки информации

Определение 1.- механизм, посредством которого в КС может осуществляться информационный поток (передача информации) между сущностями в обход политики (правил) разграничения доступа

В моделях дискреционного доступа

- возможность осуществления доступа субъектов к объектам вне области безопасного доступа, к примеру, вне явных разрешений, "прописанных" в матрице доступа (*потоки за счет **"троянских программ"** и **неявные** информационные потоки – за счет доступа к общим объектам*).

В моделях мандатного доступа

- потоки "сверху вниз" – от сущностей с высоким уровнем безопасности к сущностям более низких уровней безопасности вне явного нарушения правил ***NRU*** и ***NWD*** (*т.е. без непосредственного доступа к объектам на чтение или запись*)

Три вида:

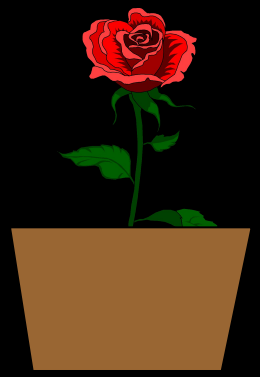
- скрытые каналы ***по памяти*** (на основе анализа объема и других статических параметров объектов системы);
- скрытые каналы ***по времени*** (на основе анализа временных параметров протекания процессов системы);
- скрытые ***статистические каналы*** (на основе анализа статистических параметров процессов системы

1. *Понятие и общая характеристика скрытых каналов утечки информации*

Пример скрытого канала по памяти

Пусть имеется система, в которой работают доверенный и недоверенный пользователь, разделяющие общий ресурс памяти

Состояние системы	*Информация, полученная по скрытому каналу*
1. Соотношение памяти 50Х50	
2. Соотношение памяти 70Х30	1 бит
3. Соотношение памяти 50Х50	1 бит
4. Соотношение памяти 70Х30	1 бит



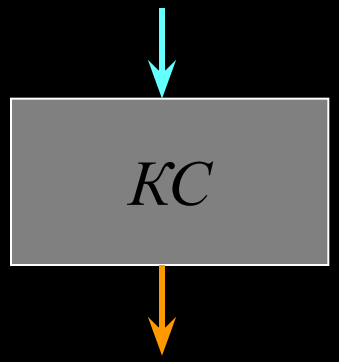
Подходы к перекрытияю скрытых каналов информационное нвлияние и невыводимость

2. *Автоматная модель невлияния Гогена-Месигера (GM-модель)*

Особая (автоматная) разновидность класса моделей конечных состояний

КС можно представить детерминированным автоматом, на вход которого поступает последовательность команд пользователей

для каждой команды каждого пользователя задана функция вывода, определяющая то, что каждый пользователь "видит" на выходе (на устройстве вывода)



***J.Goguen, J.Meseguer**, 1982г.*
*Идеология **невлияния** (**невмешательства**) вводов (команд) одних пользователей на (в) выводы других пользователей (выводы – то, что они «видят» на выходе)*

два уровня безопасности (решетка из 2-х элементов) – высокий (*high*) и низкий (*low*)

соответственно в системе работает две группы пользователей – высокоуровневые и низкоуровневые

Критерий безопасности в GM-модели - ввод ***высокоуровневого пользователя*** не может смешиваться с выводом ***низкоуровневого пользователя***

2. *Автоматная модель невлияния Гогена-Месигера (GM-модель)*

Основные тезисы и определения GM-модели

1. Состояние системы описывается 4-мя элементами:

-высокий ввод (*high-in*) -высокий вывод (*high-out*)

-низкий ввод (*low-in*) -низкий вывод (*low-out*)

2. На множестве пользователей *u* вводится функция ***cl***(*u*), отражающая уровень доверия пользователю (*низкий* или *высокий*)

3. Переходы системы по командам пользователей описываются функцией:

- ***out***(*u*, ***hist.command***(*u*))

где ***hist.command***(*u*) - история вводов системы (*traces*) *от момента, когда был осуществлен последний ввод* ***in***(*u*) *пользователя u.*

4. Вводится функция очищения ввода *purge* - очищает историю ввода *traces* от наличия в ней команд пользователей, чей уровень доверия ниже уровня доверия пользователя *u*

2. Автоматная модель невлияния Гогена-Месигера (GM-модель)

6

4. Формальное определение функции очищения :

7

purge: users,traces → traces (функция, отображающая историю ввода системы с момента действий конкретного пользователя *u* в область же историй ввода), такая, что:

- *purge*(*u*, < >) = < >, где < > - пустая история ввода

-*purge*(*u*, *hist.command*(*u*)) = *hist.command*(*u*)/*command*(*w*), если *command*(*w*) - ввод, исполненный пользователем *w* с момента ***in***(*u*) и *cl*(*u*)<*cl*(*w*)

- *purge*(*u*, *hist.command*(*u*))=*hist.command*(*u*) ∧ *hist.command*(*w*), если *command*(*w*) - ввод, исполняемый пользователем *w* с момента ***in***(*u*), и *cl*(*u*) ≥*cl*(*w*)

Основное правило в GM-модели невлияния

Система удовлетворяет требованию ***невлияния*** (***невмешательства***), если и только если:

для всех пользователей *u*,
всех историй *hist*,
и всех команд вывода *command*

out(*u*, *hist.command*(*u*)) = *out*(*u*, *purge*(*u*, *hist.command*(*u*)))

т.е. когда вывод в системе организован так, что система всегда чиста по смешиванию высоких и низких вводов в предыстории каждого вывода)

Осн. Достоинство - запрещаются многие скрытые каналы утечки

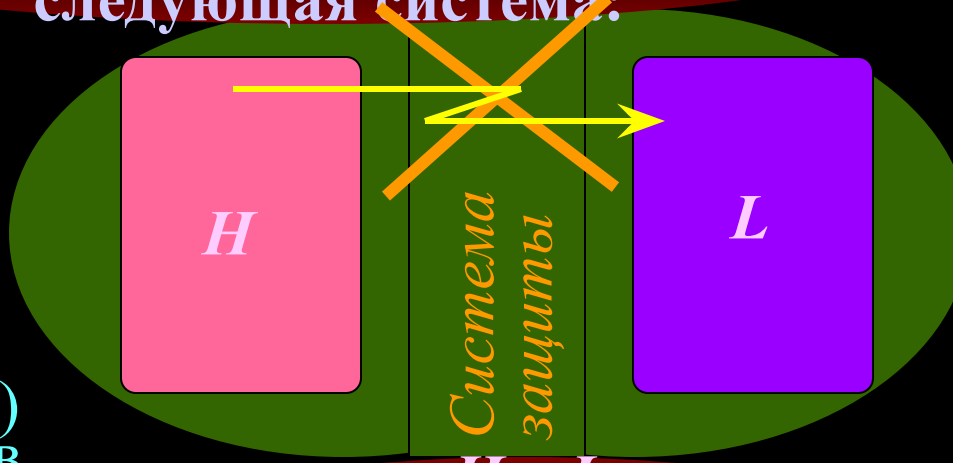
3. Теоретико-информационные модели невыводимости и невлияния (

Подходы к решению проблемы скрытых каналов на основе *теоретико-информационной интерпретации* моделей КС (Сен и Д. Денинга):

- КС (многопользовательские ОС и СУБД, глобальные сети) в реальности представляют не детерминированные, а ***вероятностные системы***

Состояния КС и т.д. в части конфиденциальных объектов имеют вероятностный характер. Понятие информационных потоков расширяется в рамках трактовки информации по Шеннону

На этой основе политики полномочного доступа рассматривается следующая система:



H и L являются случайными величинами

- Решетка уровней безопасности **Λ** имеет всего два уровня:
  - высокий – ***H***
  - низкий – ***L***
- Соответственно все сущности системы (субъекты + объекты) делятся на два класса – ***H*** и ***L***
- Главная задача системы (монитора) безопасности не допустить потоков информации от высокоуровневых объектов к низкоуровневым

→ подход

Информационная невыводимость

Информационное невлияние (невмешательство)

3. Теоретико-информационные модели невыводимости и невлияния (невмешательства)

Модели ***информационной невыводимости*** и ***информационного невлияния***

- теоретическая основа недопущения и нейтрализации ***скрытых каналов*** утечки информации и несанкционированного воздействия

Понятие информации по Шеннону

- изменение степени неопределенности знания о состоянии объекта или само изменение степени неопределенности состояния объекта

Информационная невыводимость

Определение 2. В системе присутствует информационный поток от высокоуровневых объектов ***H*** к низкоуровневым ***L***, если некое возможное значение переменной в некотором состоянии низкоуровневого объекта ***L*** невозможно одновременно с возможными значениями переменных состояния высокоуровневых объектов ***H***

т.е. наблюдая ***L*** можно вывести информацию о состоянии ***H*** (утечка по скрытому каналу «сверху-вниз»)

Определение 3. Система ***безопасна*** в смысле ***информационной невыводимости***, если в ней отсутствуют информационные потоки вида, описанного в Определении 1

*иначе - нет информационного потока от **H** к **L** тогда и только тогда, когда выполняется следующее условие:*

если $p(H)>0, p(L)>0,$ то $p(H|L)>0$

т.е. при каком-либо ***L*** м.б. различные ***H*** с ненулевой вер-ю

Но – при $p(H)>0, p(L)>0 \Rightarrow p(L|H) = p(H,L)/p(H) = p(H|L)p(L)/p(H)$

Отсюда из $p(H|L)>0 \Rightarrow p(L|H)>0$

отсутствие и обр. потоков – фактически полная изоляция ***H*** и ***L***

3. Теоретико-информационные модели невыводимости и невлияния (невмешательства)

т.о. в модели информационной невыводимости требуется, чтобы низкоуровневая информация была независима от высокоуровневой:

$p(L|H) = p(L)$, что при $p(H)>0$, $p(L)>0$ равносильно $p(H|L) = p(H)$

Вместе с тем:

потоки «снизу-вверх» неопасны и допустимы

при полной изоляции разноуровневых объектов существенно снижается функциональность КС

Другой подход

Информационное невлияние (невмешательство)

Определение 4. Система ***безопасна***, если на состояние высокоуровневых объектов ***не влияет*** состояние низкоуровневых объектов в предшествующие моменты времени, и наоборот

$$p(L_t|H_{t-1}) = p(L_t) \qquad p(H_t|L_{t-1}) = p(H_t)$$

Также слишком жесткое требование

z.b. несекретный файл (L) и файл аудита (H)

!!! значения низкоуровневых объектов могут содержать информацию о последующих значениях высокоуровневых объектах

$p(H_t|L_{t-1})$ не обяз-но $= p(H_t)$

С другой стороны нельзя также требовать - $p(L_t|H_{t-1}) = p(L_t)$ (z.b. после сбоя значение несекретного файла может определяться на основе состояния файла аудита до сбоя)

3. Теоретико-информационные модели невыводимости и невлияния (невмешательства)

Поэтому требования информационного невлияния смягчаются - низкоуровневые объекты не должны иметь возможности **накапливать** информацию о значениях высокоуровневых объектах (чтобы знание L_{t-1} и L_t не давало бы новой информации о H_{t-1}):

$$p(L_t|H_{t-1}, L_{t-1}) = p(L_t|L_{t-1})$$

что равносильно -

$$p(H_{t-1}|L_t, L_{t-1}) = p(H_{t-1}|L_{t-1})$$

т.е. запрещается поток из L_t в H_{t-1}, но !!! не запрещается из L_t в H_{t+1}

т.о. высокоуровневые объекты могут принимать информацию о состоянии низкоуровневых объектов в предыдущие моменты времени (неопасные потоки «снизу-вверх»)

запрещаются т.н. ***временны́е*** каналы утечки

Определение 5. Система ***безопасна*** в смысле ***информационного невмешательства (невлияния)***, если выполняется равенство:

$$p(L_t|H_s, L_s) = p(L_t|L_s) \ ,$$

где $s,t = 0,1,2, \ldots$ и $s < t$

3. *Теоретико-информационные модели невыводимости и невлияния (невмешательства)*

Реализации моделей информационной невыводимости и информационного невмешательства

- Технологии «представлений» (views) в СУБД и ОС
- Технологии «разрешенных процедур» в АС

3. Теоретико-информационные модели невыводимости и невлияния (невмешательства)

Определение 6. *"**Представлением**" информации КС называется процедура формирования и предоставления именованному пользователю после его входа в систему и аутентификации необходимого ему подмножества информационных объектов КС, в том числе, с возможным их количественным и структурным видоизменением, исходя из задач разграничения доступа к информации*

На языке SQL

CREATE VIEW ИмяПредставления [(*поле*1[, *поле*2[, ...]])] *AS инструкция_SELECT__ ;*

GRANT SELECT ON ИмяПредставления TO ИмяПользователя;

- эффективное средство решения проблемы скрытых каналов утечки информации ***по памяти***, но не защищает от скрытых каналов ***второго*** **и** ***третьего вида*** – т.е. от каналов, возникающих на основе анализа ***временных*** и ***статистических*** параметров процессов в системах коллективного доступа к общим информационным ресурсам

3. *Теоретико-информационные модели невыводимости и невлияния (невмешательства)*

- часть из проблем по скрытым каналам ***по времени*** связаны с интерфейсом АС и, основывается, в частности, на технике "разрешенных процедур"

Определение 7. *"**Системой разрешенных** процедур" называется разновидность **интерфейса** АС, когда при входе в систему после идентификации и аутентификации пользователям предоставляет только лишь возможность запуска и исполнения конечного набора логико-технологических процедур обработки информации без возможности применения элементарных методов доступа (read, write, append, update, create, delete и т.п.) к объектам системы*

3. Теоретико-информационные модели невыводимости и невлияния (невмешательства)

Теоретико-вероятностная трактовка GM-автомата

Система – не детерминированный, а вероятностный автомат, состояния которого реализуются с вероятностью {0,1}

Определение 8. Система, функционирование которой представляется совокупностью четырех событий с вероятностью {0,1} - *high-in*, *high-out*, *low-in* и *low-out* обладает свойством ***информационного невмешательства***, если выполняется равенство:

$$p(low\text{-}out_t | high\text{-}in_s, low\text{-}in_s) = p(low\text{-}out_t | low\text{-}in_s)$$

где $s,t = 0,1,2, \ldots$ и $s < t$

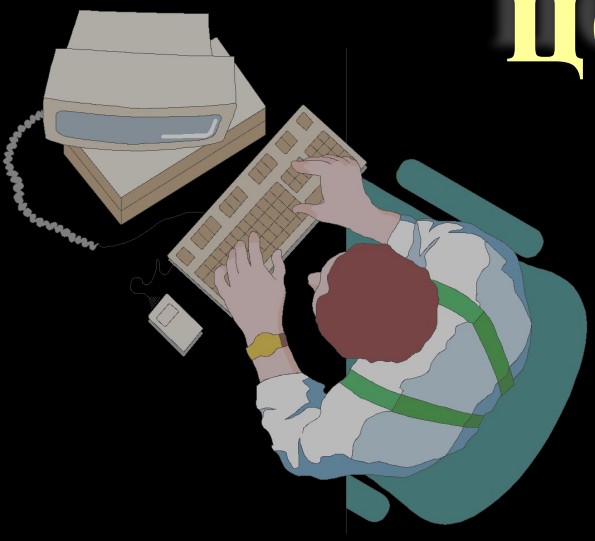
т.о. - модели ***невыводимости*** и *невмешательства* "сильнее" и ближе к реальности, чем классическая модель полномочного доступа Белла-ЛаПадулы, т.к. более гибко контролируют потоки информации между сущностями с разным уровнем безопасности

- дают методологию борьбы со скрытыми каналами утечки информации, лежащую в основе, в частности ***технологий "представлений"*** и ***"разрешенных процедур"***

Тема 2. Модели безопасности компьютерных систем

Лекция 2.6.

Модели и технологии обеспечения целостности данных



Учебные вопросы:

1. **Общая характеристика моделей и технологий обеспечения целостности данных**
2. **Мандатная модель Кен Биба и дискреционная модель Кларка-Вильсона**
3. **Технологии ЭЦП**
4. **Мониторы транзакций в СУБД «Клиент-сервер»**

Литература:

1. **Зегжда Д.П., Ивашко А.М.** Основы безопасности информационных систем. - М.:Горячая линия - Телеком, 2000. - 452с

2. **Грушо А.А.,Тимонина Е.Е.** Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с

3.Теоретические основы компьютерной безопасности : Учеб. Пособи для вузов / П.Н.Девянин, О.О.Михальский, Д.И.Правиков и др. - М Радио и связь, 2000.-192с.

4.**Гайдамакин Н.А.** Автоматизированные информационные системы, базы и банки данных. Вводный курс. – М.: Гелиос АРВ, 2003. 368с

1. *Общая характеристика моделей обеспечения целостности данных*

Понятие ЦЕЛОСТНОСТИ данных

-свойство, гарантирующее точность и полноту информации, а также методов ее обработки

-такое свойство информации, при котором ее содержание и структура (данных) определены уполномоченными лицами и процессами

неизменность — объектов, содержащих код ПО

неискаженность — отсутствие подделки при:
- передаче данных
- обработке данных

правильность — отсутствие ошибок в:
- структуре данных
- содержании данных

***модели* обеспечения *целостности* в рамках *субъектно-объектной* формализации КС** (модель Биба, модель Кларка-Вильсона)

криптографические технологии *электронной цифровой подписи*

технологии *параллельного выполнения транзакций* в клиент-серверных СУБД

2. *Мандатная модель Биба* (*сер.70-х годов, Кен Биба*), *Дискреционная модель Кларка Вильсона* (*1987г.*)

Система защиты - совокупность

- множества субъектов ***S***
- множества объектов ***O***
- множества операций над объектами доступа ***R*** (два элемента - ***read*** и ***write***)
- решетки уровней безопасности **Λ** субъектов и объектов (решетка уровней целостности данных)
- функции ***F***, отображающей элементы множеств ***S*** и ***O*** в **Λ**
- множества состояний системы ***V***, которое определяется множеством упорядоченных пар (***F,A***)
- начального состояния v_0
- набора запросов ***Q***
- функции переходов $T: (V \times Q) \rightarrow V$, которая переводит систему из одного состояния в другое при выполнении запросов субъектов на доступ к объектам

2. *Мандатная модель Биба* (*сер.70-х годов, Кен Биба*), *Дискреционная модель Кларка-Вильсона* (*1987г.*)

Критерии безопасности (обеспечения целостности)

- недопустимы потоки «снизу вверх», т.к. могут нарушить целостность объектов более высокого уровня безопасности:

- запись данных субъектом $s \in S$ в объект $o \in O$ с более высоким уровнем безопасности – $F(s) < F(o)$

(no write up - NWU) **– нельзя писать вверх**, т.к. в результате может произойти нарушение целостности («загрязнение») объекта

- чтение данных субъектом $s \in S$ из объекта $o \in O$ с более низким уровнем безопасности – $F(o) < F(s)$

(no read down - NRD) **– нельзя читать вниз**, т.к. в результате может произойти нарушение целостности («загрязнение») субъекта

Модель Биба - инверсия модели Белла-ЛаПадулы

Разновидности модели Биба

1

Модель *с понижением уровня субъекта*

Субъекты могут читать любые объекты

но, т.к. в результате они могут быть загрязнены, то после завершения операции чтения, уровень целостности субъектов должен быть понижен до уровня целостности прочитанного объекта

– $F(o) < F(s)$

– $F^*(s) \equiv F(o)$

Модель *с понижением уровня объекта*

Субъекты могут писать в любые объекты

но, т.к. в результате объект может быть загрязнен, то после завершения операции записи, уровень целостности измененного объекта должен быть понижен до уровня целостности изменяющего субъекта

– $F(s) < F(o)$

– $F^*(o) \equiv F(s)$

Главный недостаток - «деградация» системы

Возможности объединения мандатной модели обеспечения конфиденциальности Белла-ЛаПадулы с мандатной моделью обеспечения целостности Биба

1. На основе двух различных решеток в одной КС

- решетка $\Lambda_к$ уровней конфиденциальности и функция отображения на нее субъектов и объектов доступа $\mathcal{F}_к(x) = l_к \in \Lambda_к,\ x \in S \cup O$
- решетка $\Lambda_ц$ уровней целостности и функция отображения на нее субъектов и объектов доступа $\mathcal{F}_ц(x) = l_ц \in \Lambda_ц,\ x \in S \cup O$
- принятие решения на доступ одновременно по правилам *NRU* и *NWD* по функции $\mathcal{F}_к(x)$ и правилам *NRD* и *NWU* по функции $\mathcal{F}_ц(x)$

но м.б. противоречия и тупики

2. На основе одной общей решетки

- операции *read* и *write* возможны только в пределах одного уровня безопасности $\mathcal{F}(s) = \mathcal{F}(o)$ - полностью изолированная по уровням безопасности система (т.н. «*равное чтение*» и «*равная запись*»)

3. На основе одной общей решетки, но со спецификой отображения

- субъекты и объекты с высокими требованиями *целостности* располагаются на *нижнем* уровнем иерархии решетки (сист.ПО и прогр-ст)
- субъекты и объекты с высокими требованиями *конфиденциальности* располагаются на *самом высоком* уровне иерархии решетки (секр. данные и доверенные пользователи)

2. *Мандатная модель Биба* (*сер.70-х годов, Кен Биба*), *Дискреционная модель Кларка-Вильсона* (*1987г.*)

Главная идея «тройки целостности»:
«субъект-
-операция(транзакция), не нарушающая
целостность-
-объект»

Исходные положения

1. **Все множество объектов *D* разделяется на объекты *CDI*, требующие контроля целостности (*constrained data items*), и объекты *UDI*, не требующие контроля целостности (*unconstrained data items*)**

$$D = CDI \cup UDI, \quad CDI \cap UDI = \varnothing$$

2. **На множестве элементарных операций над объектами выделяются совокупности (последовательности), обособляющиеся в логически самостоятельные сущности, называемые процедурами преобразования *TP* (*transformation procedures*)**
3. **Дополнительно вводится особый класс процедур *IVP* над данными, которые обеспечивают проверку целостности контролируемых данных (*integrity verification procedures*)**
4. **Те процедуры преобразования данных *TP*, применение к результатам которых процедур проверки целостности *IVP* дает положительный результат, называются «*корректно (правильно, хорошо) сформированными транзакциями*»**

2. *Дискреционная модель Кларка-Вильсона (1987г.)*

Правила функционирования системы

C1. Множество всех процедур контроля целостности *IVP* должно содержать процедуры контроля целостности любого элемента данных из множества всех *CDI*

C2. Все процедуры преобразования *TP* должны быть хорошо сформированными транзакциями, т.е. не нарушать целостности данных, и применяться только по отношению к списку элементов (объектов) *CDI*, устанавливаемых администратором системы

E1. Система должна контролировать допустимость применения *TP* к элементам *CDI* в соответствии со списками, указанными в правиле C2

E2. Система должна поддерживать список разрешенных конкретным пользователям процедур преобразования *TP* с указанием допустимого для каждой *TP* и данного пользователя набора обрабатываемых элементов *CDI* (т.е. тройки «субъект-*TP*-объект *CDI*»)

C3. Список, определенный правилом C2, должен отвечать требованию разграничения функциональных обязанностей (в т.ч. совм. вып-я)

E3. Система должна аутентифицировать всех пользователей, пытающихся выполнить какую-либо процедуру преобразования *TP*

C4. Каждая *TP* должна записывать в журнал регистрации информацию, достаточную для восстановления полной картины каждого применения этой *TP*. Журнал регистрации – это специальный элемент *CDI*, предназначенный только для добавления в него информации

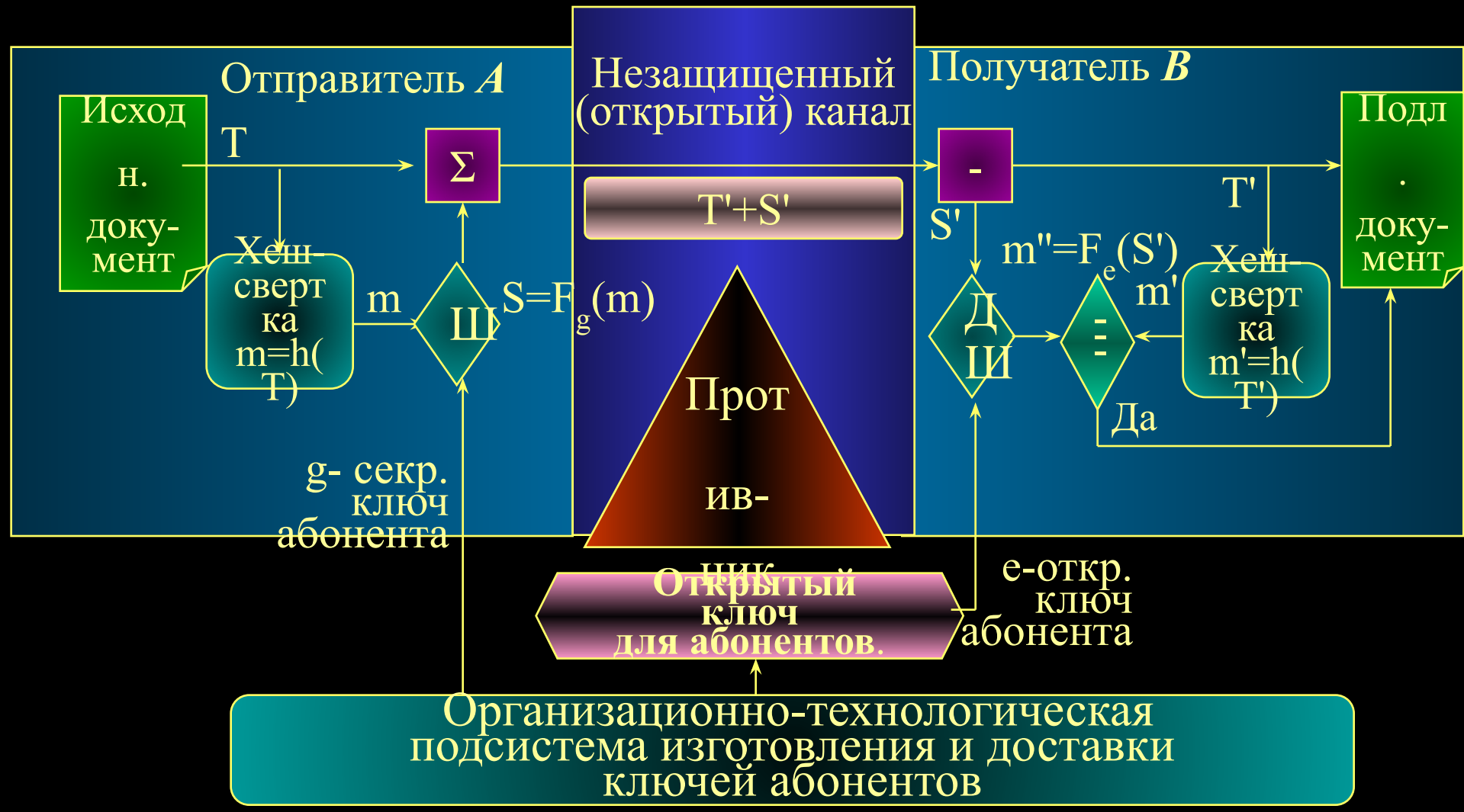
C5. Специальные *TP* могут корректно обрабатывать *UDI*, превращая их в *CDI*

E4. Только специально уполномоченный субъект (пользователь) может изменять списки, определенные в правилах C2 и E2. Этот субъект не имеет права выполнять какие-либо действия, если он уполномочен изменять регламентирующие эти действия списки

3. Криптографические технологии ЭЦП

Системы ЭЦП основываются на идеологии асимметричных криптосистем

Система ЭЦП включает два этапа:
- процедуру постановки подписи
- процедуру проверки подписи



3. Криптографические технологии ЭЦП

Электронная цифровая подпись в стандарте *RSA* (1977, Массачуссетс)

При условии сохранении в тайне секретных ключей *ЭЦП* удостоверяет :

- подлинность ***автора*** (защита *от маскарада*)
- подлинность ***переданных данных*** (защита *от активного перехвата*)

Для подтверждения *факта* и *подлинности* доставки данных получатель ***B*** должен направить отправителю ***A*** *уведомление* (*квитанцию*) *о вручении* (ЭЦП подтверждающего ответного сообщения)

3. Криптографические технологии ЭЦП

Хеш-функции (хеш-свертка)

- криптографическое преобразование данных произвольной длины в строку битов фиксированной длины (обычно 160-256 бит)

Требования к хеш-функциям

Необратимость – вычисление исходных данных по их хеш-свертке невозможно или представляет непреодолимую вычислительную преграду

это свойство называют «стойкостью в сильном смысле»

Стойкость к коллизиям – вероятность того, что для двух различных исходных данных их хеш-свертки совпадут д.б. = 0, или ничтожной

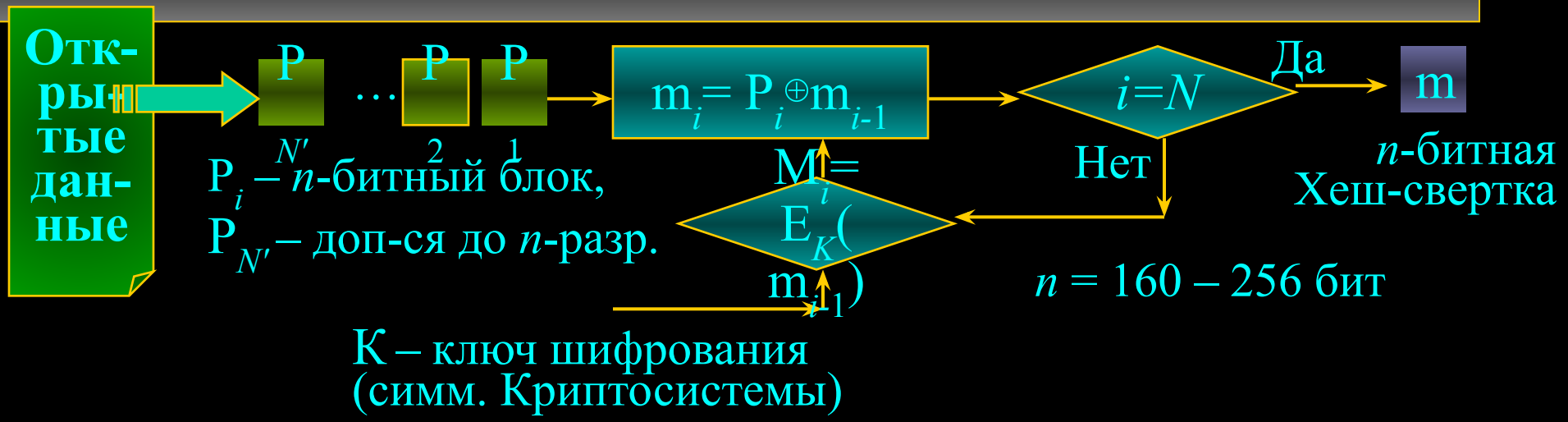
- подобрать по известным исходным данным и их хеш-свертке другие исходные данные с той-же хеш-сверткой невозможно или представляет непреодолимую вычислительную преграду

Чувствительность – изменение даже одного бита исходных данных, д. приводить к существенному изменению хеш-свертки

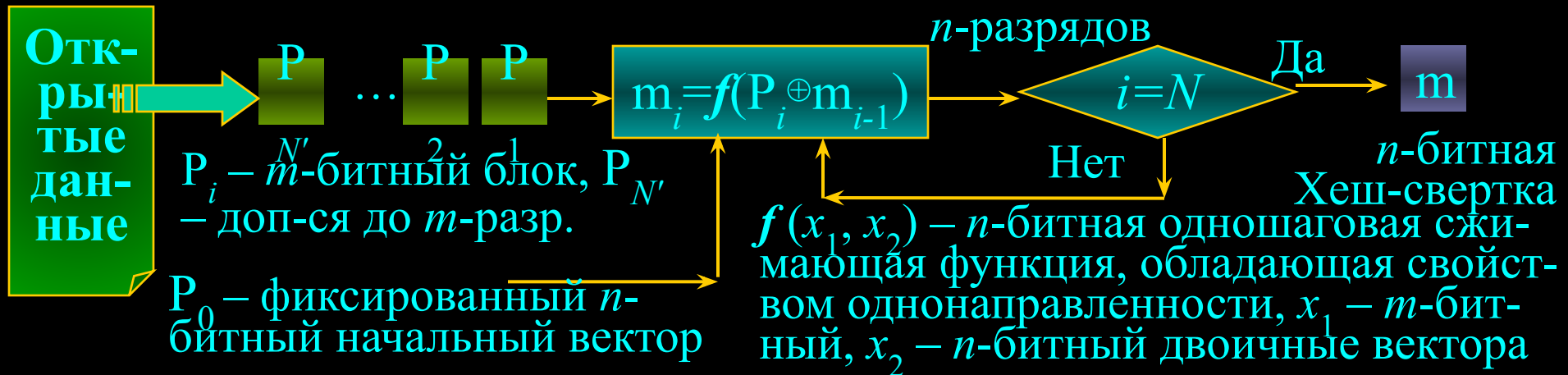
3. Криптографические технологии ЭЦП

Как правило, хеш-функции строят путем итерационных процедур на основе одношаговых сжимающих функций

Обобщенная схема ключевой хеш-функции



Обобщенная схема безключевой хеш-функции



3. Криптографические технологии ЭЦП

Подсистемы создания, хранения и распространения ключей – важнейший элемент криптосистем

Стандарт ANSI X9.17

Ключи

Для шифрования данных

Для шифрования ключей

Сеансовые ключи

Генерация ключей

Детерминированные методы

Путем формирования псевдослучай-ных последовательностей большой длины на основе ПСП малой длины с заданными (теми же) стат.св-ми

Сдвиг. регистры с лин. обр. связями

Недетерминированные методы

На основе случайных физических процессов (генераторы шума и т.п.)

На основе процессов физ. природы – движ. мыши, нажатие клавиш

Сеансовые ключи – на основе паролей пользователей

3. Криптографические технологии ЭЦП

Хранение ключей

Криптоустройства, имеющие спец. защищенную от НСД память для ключей	Хранение ключей в зашифрованном виде на ПЭВМ	Использование внешних устройств для хранения ключей (диски, магн. карты…)

Распределение ключей

Через фельдсвязь	Через спец. территориально-распределенную систему	Через передачу (в зашифрованном виде) или спец. режим формирования по открытым каналам связи на основе асимметричных криптопротоколов

для систем с открытым ключом

Через инфраструктуру открытых ключей посредством использования идеологии сертификатов ключей

Инфраструктура открытых ключей

абонент, получивший сообщение, должен быть уверен, что открытый ключ, с помощью которого расшифровывается сообщение или проверяется ЭЦП, действительно принадлежит объявленному отправителю

Сертификат ключа

- набор данных, заверенный ЭЦП центра сертификации (удостоверяющего центра) и включающий открытый ключ и список атрибутов, относящихся к абоненту ключа (имя абонента, название центра сертификации, номер сертификата, время действия сертификата, предназначение ключа (шифрование, ЭЦП))
- проверив ЭЦП сертификата по известному открытому ключу сертификационного центра, можно убедиться, что находящийся в нем открытый ключ действительно принадлежит обозначенному пользователю

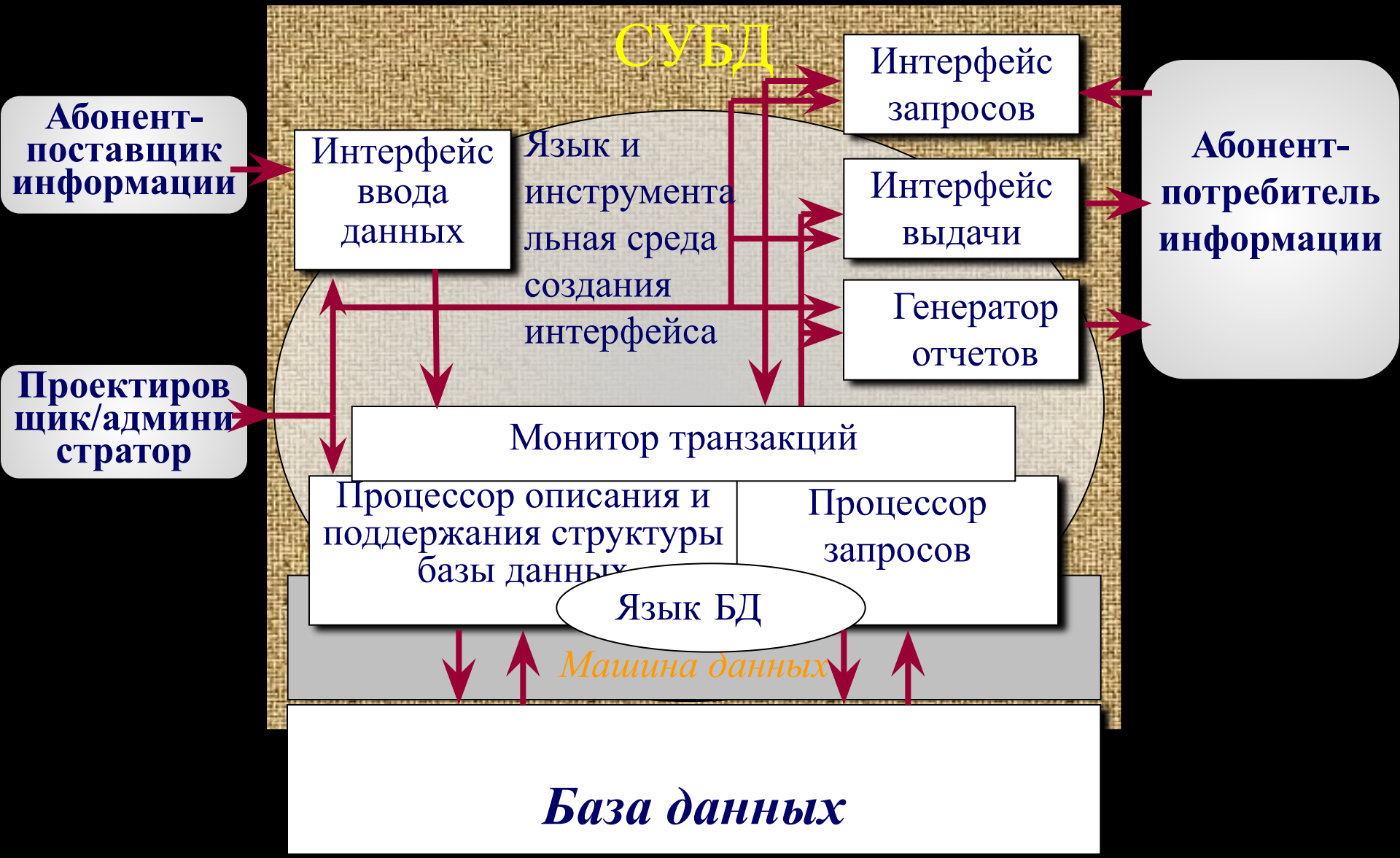
Сертификационный (удостоверяющий) центр

-доверенная третья сторона
- регистрирует абонентов открытых ключей
-изготавливает открытые и закрытые ключи и сертификаты открытых ключей
-обеспечивает доступ к сертификатам открытых ключей
-ведет справочник действующих и отозванных сертификатов

Иерархическая система сертификационных центров

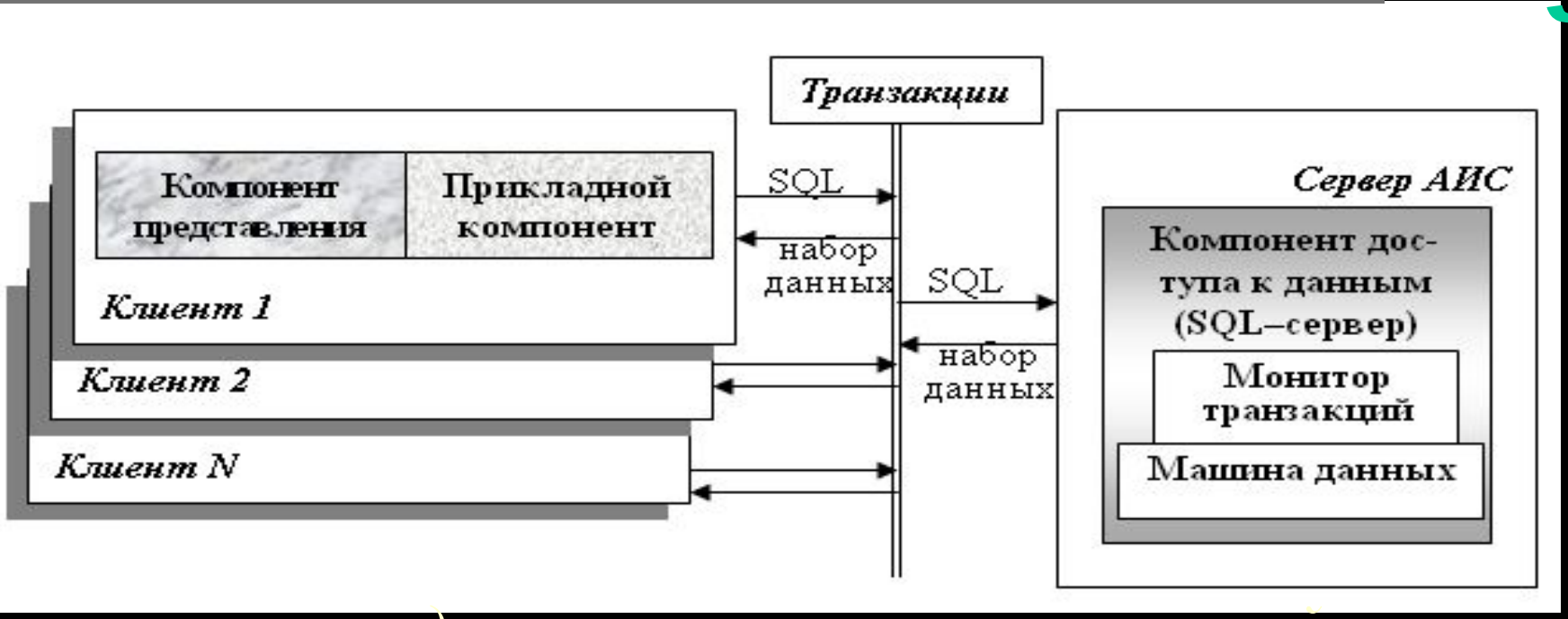
-сертификат открытого ключа самого сертификационного центра выдает сертификационный центр более высшей иерархии

Структура СУБД



4. Мониторы транзакций в СУБД «Клиент-сервер»

Клиент-серверные системы



Транзакция *- последовательная совокупность операций, имеющая отдельное смысловое значение по отношению к текущему состоянию базы данных*

Совокупность функций СУБД по организации и управлению транзакциями - ***монитор транзакций***

Транзакции играют важную роль в механизме обеспечения СУБД ограничений целостности базы данных. Ограничения целостности непосредственно проверяются по завершению очередной транзакции. Если условия ограничений целостности данных не выполняются, то происходит "откат" транзакции (выполняется SQL–инструкция ROLLBACK), в противном случае транзакция фиксируется (выполняется SQL–инструкция COMMIT).

Виды нарушений целостности (при параллельном выполнении транзакций)

Потерянные изменения - когда две транзакции одновременно изменяют один и тот же объект базы данных. В том случае, если в силу каких-либо причин, например, из–за нарушений целостности данных, происходит откат, скажем, второй транзакции, то вместе с этим отменяются и все изменения, внесенные в соответствующий период времени первой транзакцией. В результате первая еще не завершившаяся транзакция при повторном чтении объекта не "видит" своих ранее сделанных изменений данных.

"Грязные" данные - когда одна транзакция изменяет какой-либо объект данных, а другая транзакция в этот момент читает данные из того же объекта. Так как первая транзакция еще не завершена, и, следовательно, не проверена согласованность данных после проведенных, или вовсе еще только частично проведенных изменений, то вторая транзакция может "видеть" соответственно несогласованные, т.е. "грязные" данные.

Неповторяющиеся чтения - когда одна транзакция читает какой-либо объект базы данных, а другая до завершения первой его изменяет и успешно фиксируется. Если при этом первой, еще не завершенной, транзакции требуется повторно прочитать данный объект, то она "видит" его в другом состоянии, т.е. чтение не повторяется.

Механизмы изоляции транзакций и преодоления ситуаций несогласованной обработки данных

Синхронизационные захваты (блокировки) объектов базы данных

два основных режима захватов

совместный режим (*Shared*) - *захват по чтению*

монопольный режим (***eXclusive***) - *захват по записи*

Двухфазный протокол синхронизационных захватов (***блокировок***) ***объектов*** базы данных – 2PL (Two–Phase Locks)

1-*я фаза* - *транзакция запрашивает и накапливает захваты необходимых объектов в соответствующем режиме*

"гранулирование" *объектов захвата*

2-*я фаза* – *выполнение операций над захваченными объектами, фиксация изменений (или откат по соображениям целостности данных), освобождение захватов*

Возможность возникновения тупиковых ситуаций (Deadlock)

Автоматическое обнаружение (распознавание) тупиковых ситуаций на построении и анализе графа ожидания транзакций

Временные метки объектов базы данных

Механизмы изоляции транзакций и преодоления ситуаций несогласованной обработки данных

Временные метки объектов базы данных

Каждой транзакции приписывается временная метка, соответствующая моменту начала выполнения транзакции

При выполнении операции над объектом транзакция "помечает"его своей меткой и типом операции (чтение или изменение)

Если другой транзакции требуется операция над уже "помеченным" объектом, то выполняются действия по следующему алгоритму:

- *проверяется, не закончилась ли транзакция, первой "пометившая" объект;*
- *если первая транзакция закончилась, то вторая транзакция помечает его своей меткой и выполняет необходимые операции;*
- *если первая транзакция не закончилась, то проверяется конфликтность операции (конфликтно любое сочетание, кроме "чтение–чтение");*
- *если операции неконфликтны, то они выполняются для обеих транзакций, а объект до завершения операций помечается меткой более поздней, т.е. более молодой транзакции;*
- *если операции конфликтны, то далее происходит откат более поздней транзакции и выполняется операция более ранней (старшей) транзакции, а после ее завершения, объект помечается меткой более молодой транзакции и цикл действий повторяется.*

более частые откаты транзакций, но ***отсутствие тупиков***

Тема 2. **Модели безопасности компьютерных систем**

Лекция 2.7 **Лекция 2.7.**

Методы и технологии обеспечения доступности (сохранности) данных

Учебные вопросы:

1. **Резервирование архивирование и журнализация данных**
2. **Технологии и системы репликации данных**

Литература:

1. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: изд-во Урал. Ун- та, 2003. – 328 с.

2. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос-АРВ, 2007. – 352с.

3. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс: Учебное пособие. – М.: Гелиос-АРВ, 2002. – 308с.

1. Резервирование, архивирование и журнализации данных

Безопасность Информации в КС (составляющие защищенного состояния информации)

Обеспечение конфи-денциально-сти информа-ции	Обеспечение целостности информации	Обеспечение доступности информации

Обеспечение правомерной доступности информации

-отсутствие препятствий в правомерном доступе к данным (обеспечивается политикой и механизмами разграничения доступа)

-обеспечение сохранности файлов данных БД (профилактика носителей, организационные меры)

-восстановление данных в случае программно-аппаратных сбоев, ошибочных действий пользователей либо умышленных действий злоумышленников, приводящих у уничтожению (потере, разрушению) файлов данных БД (резервирование/архивирование, журнализация данных, репликация БД)

1. Резервирование, архивирование и журнализации данных

Резервирование

-организационно-технологическая система создания и обновления (поддержания актуальности) копий файлов БД

-установление и поддержания режима размещения, хранения и использования (доступа) копий БД для восстановления БД в случае сбоев и разрушений

-осуществляется либо средствами копирования файлов ОС, либо самой СУБД (специальными режимами работы СУБД или специальными утилитами СУБД)

«Горячее» резервирование

-постоянное и непрерывное функционирование 2-х или более равнозначных («зеркальных») копий БД в КС, относящихся к т.н. «системам реального времени»

-все изменения данных одновременно и параллельно фиксируются в зеркальных копиях БД

-при сбое одной копии функционирование КС обеспечивается другой «зеркальной» копией

Архивирование

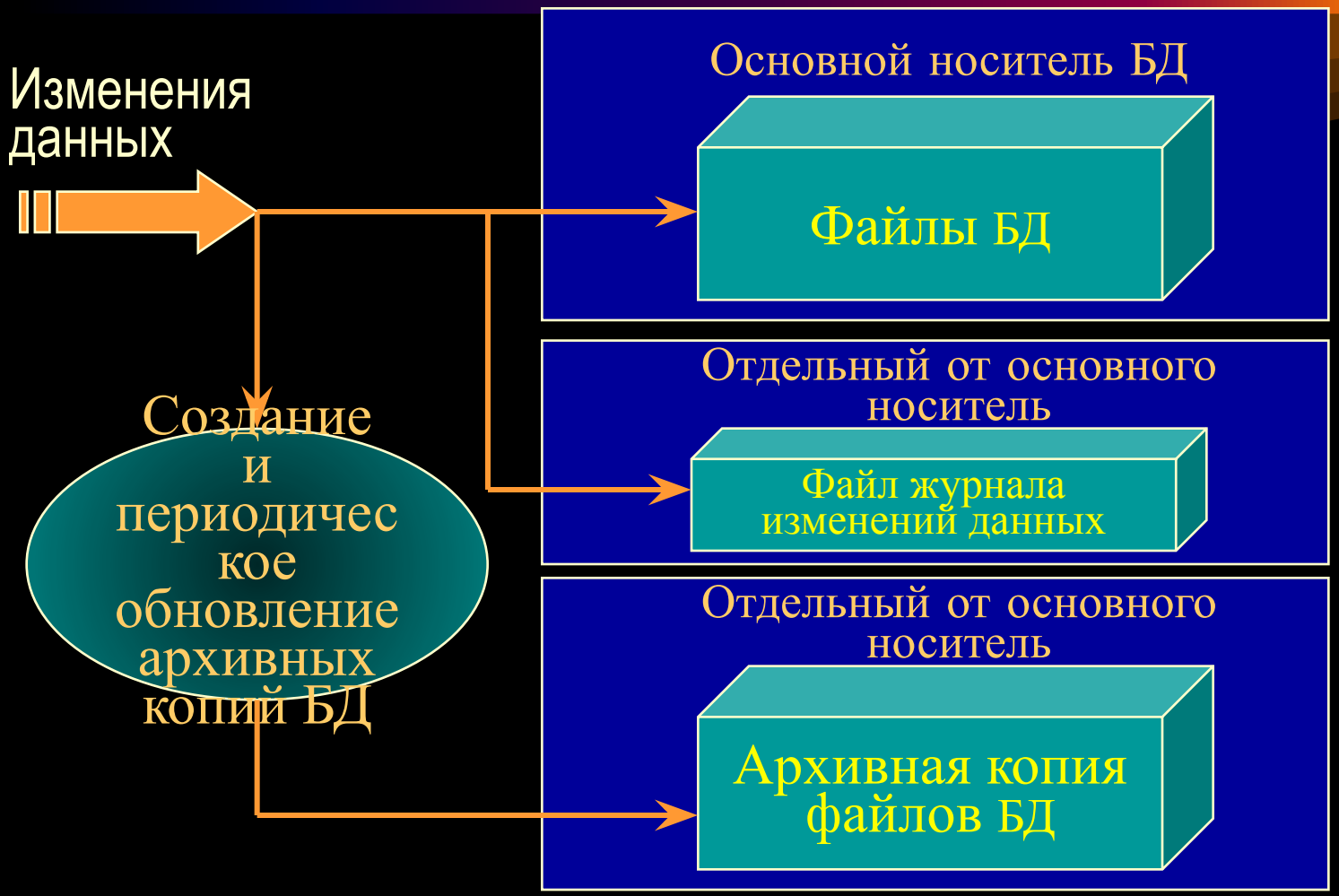
-по сути другое название системы резервирования данных, поскольку из-за большого размера файлов БД, создание резервных копий осуществляется с одновременным «сжатием» файлов данных

-сохраненная и «сжатая» копия БД называется «архивом» БД

1. Резервирование, архивирование и журнализации данных

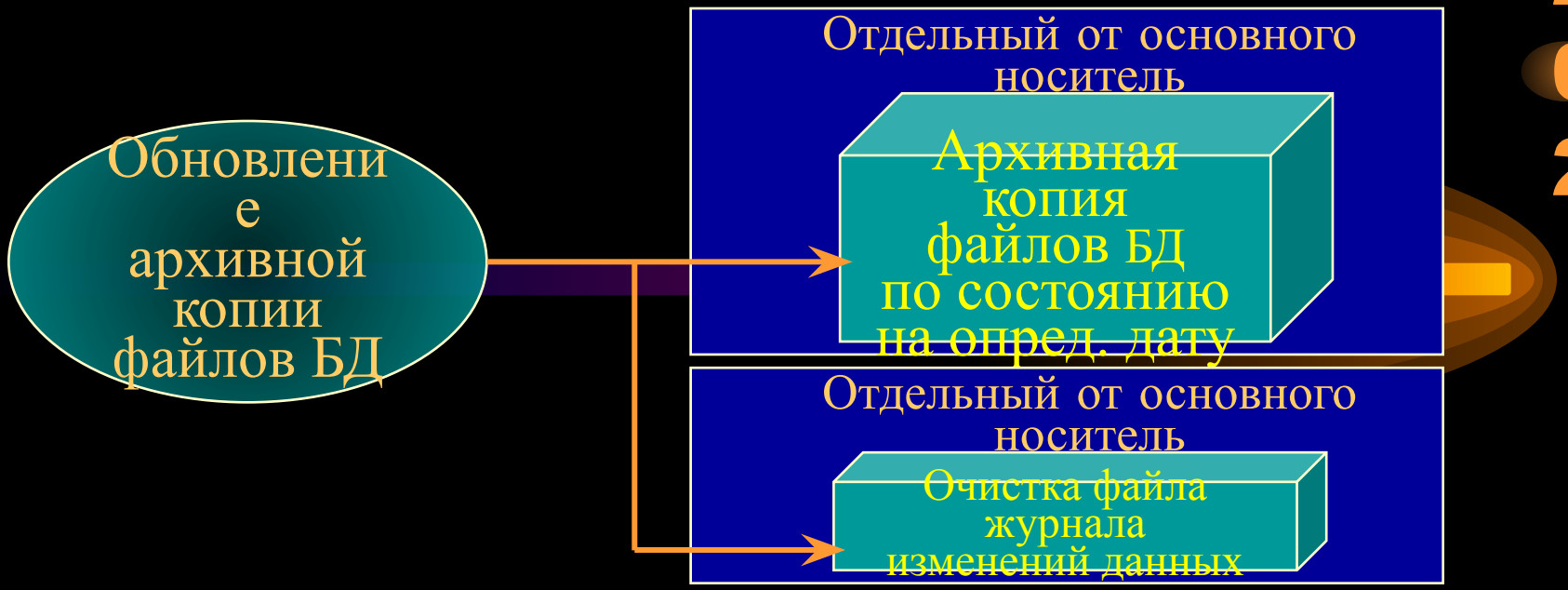
Журнализация данных

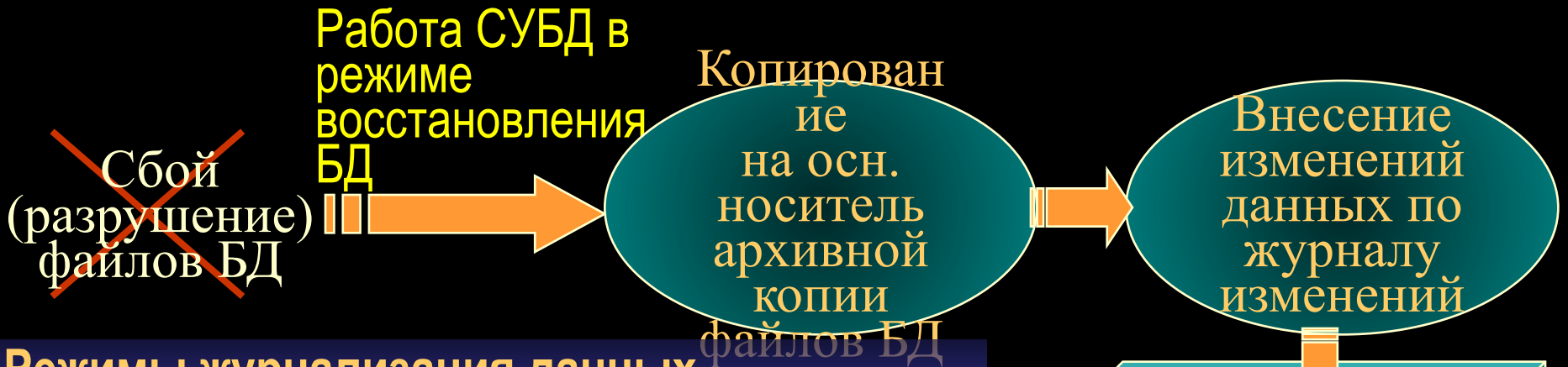
-система ведения специальных журналов текущих изменений данных для – а) аудита действий пользователей КС и б) для восстановления актуального состояния БД из существующего архива и произведенных с момента его создания изменений данных



1. Резервирование, архивирование и журнализации данных

2020





Режимы журнализация данных

-синхронный (изменения данных синхронно с БД вносятся в журнал изменений)

-асинхронный (изменения данных в журнале фиксируются в по определенному графику или отдельным командам

2. Технологии и системы репликации данных

Реплика БД

-особая копия БД для размещения на другом компьютере сети с целью автономной работы пользователей с одинаковыми (согласованными) данными общего пользования

Системы репликации данных

-разновидность технологий создания и функционирования распределенных КС

-разновидность технологий обеспечения сохранности и правомерной доступности информации

-пользователи КС работают на своих вычислительных установках с одинаковыми (общими) данными, растиражированными по локальным БД

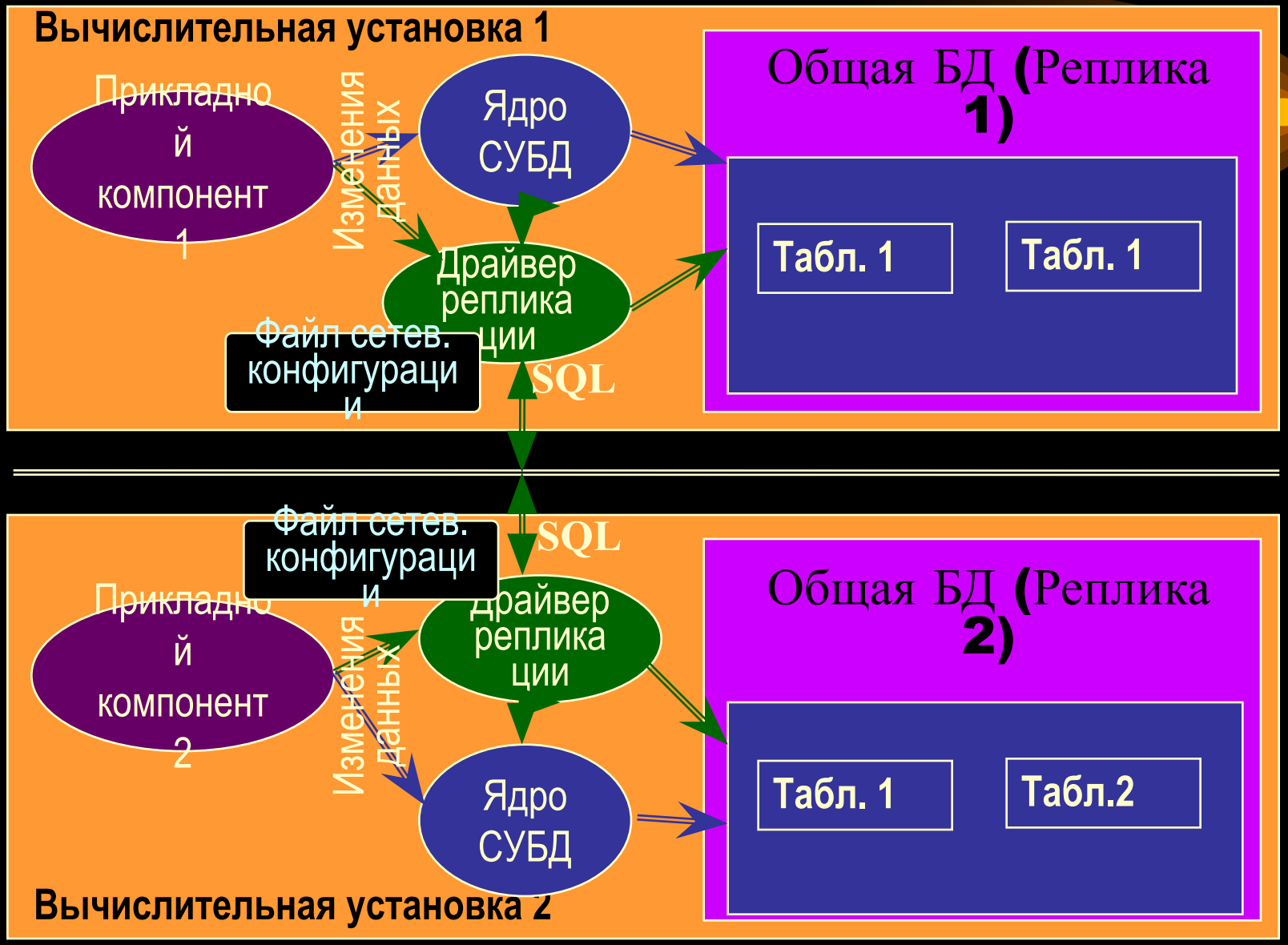
-снимается проблема быстродействия и ресурсоемкости сервера КС

Основные проблемы систем репликации

-обеспечение непрерывности согласованного состояния данных

-обеспечение непрерывности согласованного состояния структуры данных

Программно-техническая структура систем репликации



2. Технологии и системы репликации данных

Обеспечение непрерывности согласованного состояния данных

-системы синхронной репликации

-системы асинхронной репликации

Режим синхронной репликации изменений данных

-любая транзакция с любой рабочей станции сети осуществляется одновременно на всех репликах БД (фиксация транзакции производится только тогда, когда она успешно завершается одновременно на всех репликах системы)

-применяются аналогично клиент-серверным системам протоколы осуществления и фиксации транзакций

Проблемы и недостатки систем синхронной репликации

-снижение быстродействия обработки данных вследствие большого трафика данных в сети

-«тупики» при осуществлении транзакций (как в клиент-серверных системах)

2. Технологии и системы репликации данных

Обеспечение непрерывности согласованного состояния данных

Режим асинхронной репликации изменений данных

-транзакция на рабочих станциях осуществляются независимо друг от друга, в результате допускается текущая несогласованность состояния данных

-через определенные интервалы (по специальному графику, по специальным командам, в определенном, например во внерабочее, время и т.д.) осуществляется синхронизация реплик БД

-на рабочих станциях КС м. создаваться специальные хранилища данных репликации «накапливающие» изменения данных, поступающие с других рабочих станций

Проблемы и недостатки систем асинхронной репликации

-не могут применяться в КС, с высокой динамикой изменения данных

-в результате синхронизации реплик м. наблюдаться «потерянные изменения» при взаимном затирании изменений одних и тех объектов на разных репликах

2. Технологии и системы репликации данных

Обеспечение непрерывности согласованного состояния структуры данных

-системы с «главной» репликой

-системы с частичными репликами

Системы с «главной» репликой

-одна из реплик объявляется «главной» и только на ней допускается изменение структуры данных (добавление/удаление таблиц, изменение схемы таблиц)

-по принципу асинхронной репликации осуществляется тиражирование соответствующих изменений структуры данных по всем репликам системы

Системы с частичными репликами

-в каждой локальной БД определяются перечень реплицируемых объектов, в результате локальные БД «одинаковы» только в определенной части

-синхронизация реплик может осуществляется в синхронном и асинхронном (отложенном) режиме

-могут создаваться распределенные КС с функционально обоснованной схемой ввода и тиражирования данных, например данные в таблицу «Документы» вводятся в реплике секретариата и тиражируются по всем репликам, находящихся в др. подразделениях, данные в таблицу «Сотрудники» - в реплике кадрового подразделения и т.д.

Тема 2. Модели безопасности компьютерных систем

Лекция Лекция 2Лекция 2.Лекция 2.8.

Политика и модели безопасности в распределенных КС

Учебные вопросы:

2009

1. Общие положения о политике безопасности в распределенных КС
2. Зональная модель безопасности в распределенных КС

1. Общие положения о политике безопасности в распределенных КС

Три аспекта распределенности
(с т.зр. политики и субъектов обеспечения безопасности в КС)

- распределенность **защитных механизмов** по программным модулям ядра системы (модули, реализующие идентификацию/аутентификацию, управление доступом, криптозащита)
- рапределенность **информационного объекта, ассоциированного с МБО**, содержащего установки политики безопасности в КС
- распределенность **субъектов и объектов доступа КС по различным вычислительным установкам** (физическая распределенность)

1. Общие положения о политике безопасности в распределенных КС

Дополнительные аспекты политики безопасности в распределенных АИС

-нейтрализация угроз безопасности в процедурах идентификации/аутентификации с рабочих станций и при удаленном доступе пользователей АИС

-нейтрализация угроз безопасности в линиях связи и телекоммуникациях

-реализация политики привязки доступа пользователей с определенных рабочих станций, по определенному временному графику

-защита вывода информации из БД на внешние носители данных, в т.ч. на рабочих станциях АИС

-удаление остаточной информации на носителях при обработке данных на рабочих станциях

-отношения доверия между сегментами (зонами) сети АИС

-активный аудит действий пользователей

1. Общие положения о политике безопасности в распределенных КС

Распределенные компьютерные системы

В основе 7-ми Уровневая модель взаим-я откр. систем

распределенной архитектурой, разделяемые
ее обособленных компонента,
их локальными сегментами

Две разновидности

Система взаимодействующих лок. сегментов

Лок.сегмент (сеть) 1 — *Канал связи* — *Лок.сегмент (сеть) 2*

Распределенная КС как *единое целое с общей политикой безопасности*

Система- внешняя среда

Лок. сегмент (внутр. сеть) — *Канал связи* — **Не локализуемая внешняя среда (сеть)**

Внутренняя политика безопасности, включающая политику безопасности от внешней среды

Два направления

Создание защитных механизмов, устойчивых как по отношению к внутренним, так и внешним угрозам

Синтез защитных механизмов от внешних угроз

1. Общие положения о политике безопасности в распределенных КС

Синтез защитных механизмов от внешних угроз

- технологии межсетевого экранирования (анализ потока информации сетевого уровня – пакетов с уникальной информацией отправителя и получателя, и фильтрация по некоторым априорно-заданным критериям)

Создание защитных механизмов, устойчивых как по отношению к внутренним, так внешним угрозам

- политика и модель безопасности системы взаимодействующих локальных сегментов

Понятие локального сегмента

с т.зр. субъектно-объектной модели КС:

обособленная совокупность субъектов и объектов доступа

Обособление (идентификация) сегмента

два подхода – по критерию локализации (субъектов и объектов) в рамках некоторой технической компоненты

– по критерию порождения одним общим процессом (z.b. Монитор транзакций)

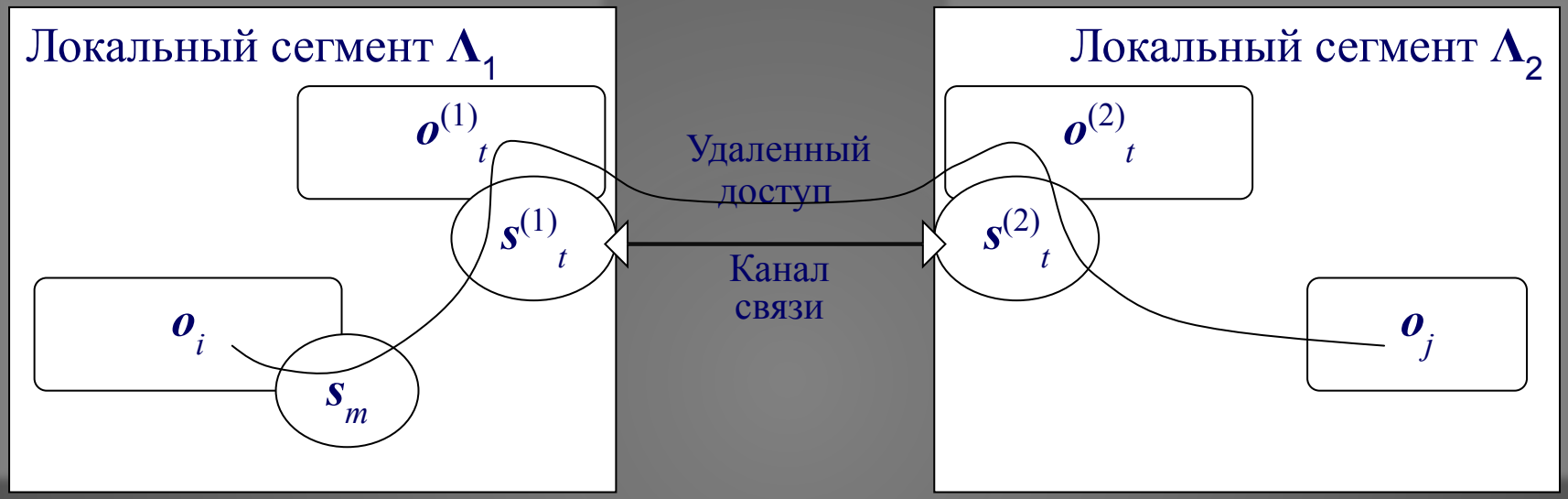
– на основе единого адресного пространства, в котором любой сущности (субъекту или объекту) присваивается уникальный глобальный идентификатор, и разделения адресного пространства на области, образующие (выделяющие) локальные сегменты КС

Понятие доступа в субъектно-объектной модели КС

5

– поток информации между объектами локализуемый через субъект (его ассоциированные объекты)

Удаленный доступ $p^{out} = Stream\ (s_m, o_i) \rightarrow o_j$



Обозначения: $s^{(1)}_t$ и $s^{(2)}_t$ – телекоммуникационные субъекты сегментов Λ_1 и Λ_2, соответственно;

$o^{(1)}_t$ и $o^{(2)}_t$ – ассоциированные с субъектами $s^{(1)}_t$ и $s^{(2)}_t$ информационные объекты (буферы оперативной памяти и т.п.);

o_i – объект, ассоциированный (но не обязательно) с субъектом s_m.

Доступ к объектам в две фазы

– вхождение в сегмент

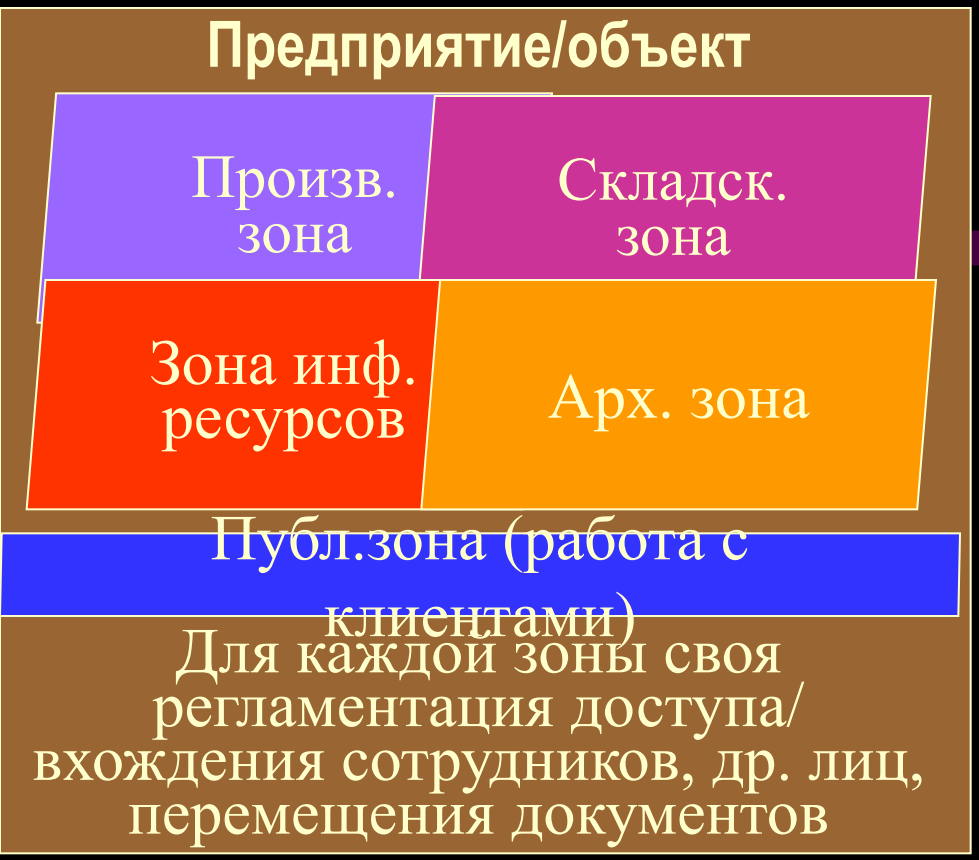
-- «в свой»

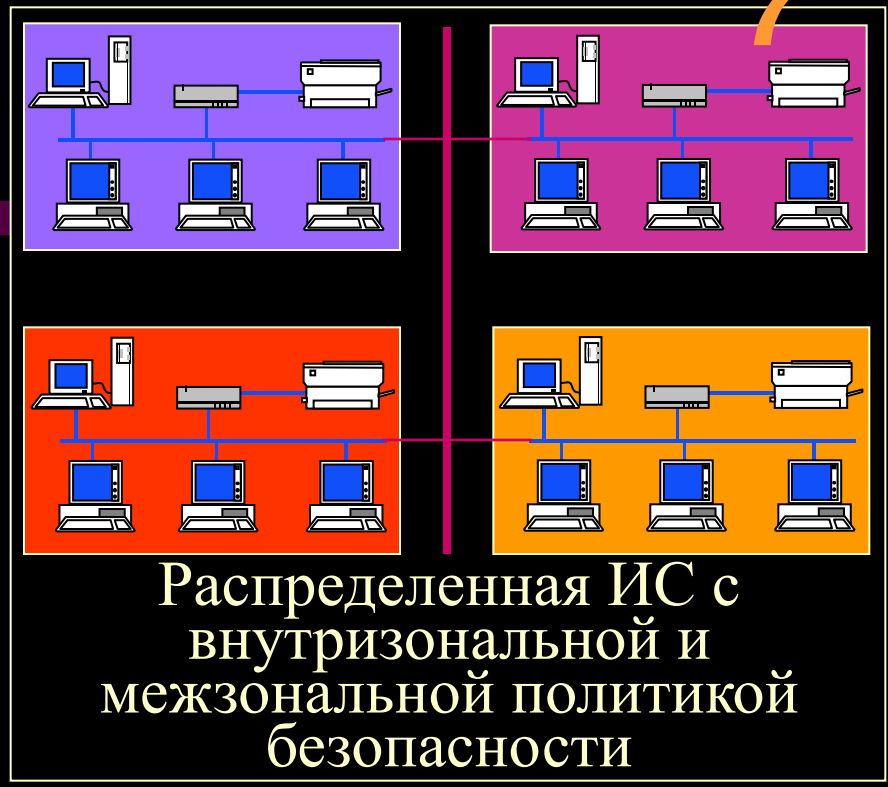
-- в доверяющий сегмент (удаленный доступ)

– запрос и получение доступа по внутризональной политике доверяющего сегмента

Дополнительная политика инициализации субъектов удаленных доступов

2. Зональная модель безопасности





Определение 1. *Зоной в распределенной ИВС называется совокупность подмножества пользователей* $U(u_1, u_2, \ldots, u_N)$, *подмножества объектов доступа* $O(o_1, o_2, \ldots, o_M)$ *и подмножества физических объектов* $V(v_1, v_2, \ldots, v_L)$, *обособленных в локальный сегмент* z_k *с отдельной (внутризональной) политикой безопасности*

Теоретико-множественная формализация зональной политики

$f_{phys} : V \to Z$ – значением функции $z = f_{phys}(v)$ является зона $z \in Z$, в которой находится (которой принадлежит) физический объект $v \in V$;

$f_{user} : U \to Z$ – значением функции $z = f_{user}(u)$ является зона $z \in Z$, в которой уполномочен (зарегистрирован) для работы пользователь $u \in U$;

$f_{fobject} : O \to V$ – значением функции $v = f_{fobject}(o)$ является физический объект $v \in V$, в котором находится (физически размещается) объект $o \in O$.

Частичный порядок доверия на множестве зон (возможность удаленных доступов)

Одностороннее

$$z_1 > z_2 \leftrightarrow P^{out}{}_L(z_1 \to z_2) \neq \varnothing \ \wedge \ P^{out}{}_L(z_1 \leftarrow z_2) = \varnothing$$

Двустороннее

$$z_1 = z_2 \leftrightarrow P^{out}{}_L(z_1 \to z_2) \neq \varnothing \ \wedge \ P^{out}{}_L(z_1 \leftarrow z_2) = \varnothing$$

Отсутствие

$$z_1 \neq z_2 \leftrightarrow P^{out}{}_L(z_1 \to z_2) = \varnothing \ \wedge \ P^{out}{}_L(z_1 \leftarrow z_2) = \varnothing$$

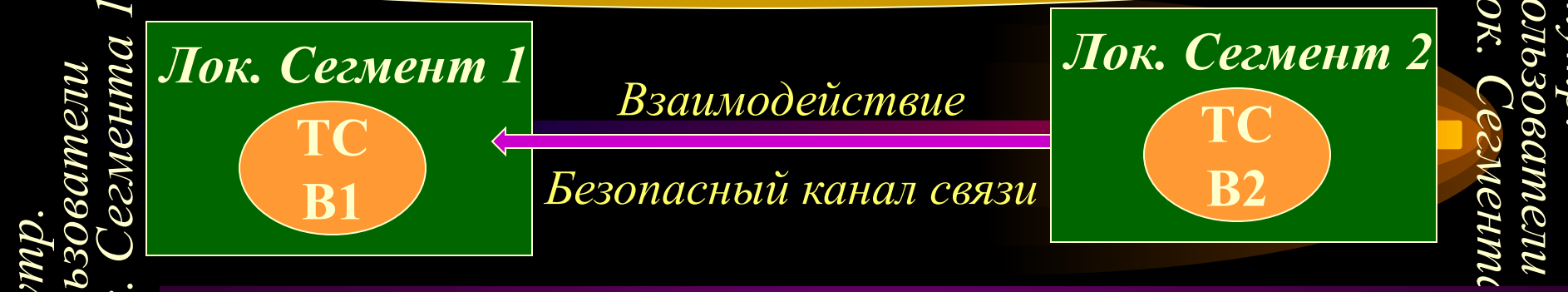
Политика безопасности в распределенных КС

Примеры реализации общесетевой политики политики безопасности в распределенных КС (сетях)

– модель безопасности Варадхараджана (Varadharadjan, 1990) для распределенной сети

– доменно-групповая политика безопасности в сетях на основе Windows NT

Политика безопасности в системе взаимодействующих сегментов



-Внутризональная политика безопасности

-Межзональная политика безопасности (политика взаимодействия)

Политика взаимодействия

Двустороннего доверия

– пользователи одного сегмента могут получать доступ к объектам другого сегмента и наоборот

Одностороннего доверия

– пользователи одного сегмента могут получать доступ к объектам другого сегмента, но наоборот нет

Тема 3. Методы анализа и оценки защищенности компьютерных систем

Лекция Лекция 3Лекция 3.1Лекция 3.1.

Методы, критерии и шкалы оценки защищенности (безопасности)

Учебные вопросы:

1. **Общая характеристика измерения (оценки) эмпирических объектов**
2. **Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации**
3. **Критерии оценки безопасности информационных технологий. Профили защиты СУБД**

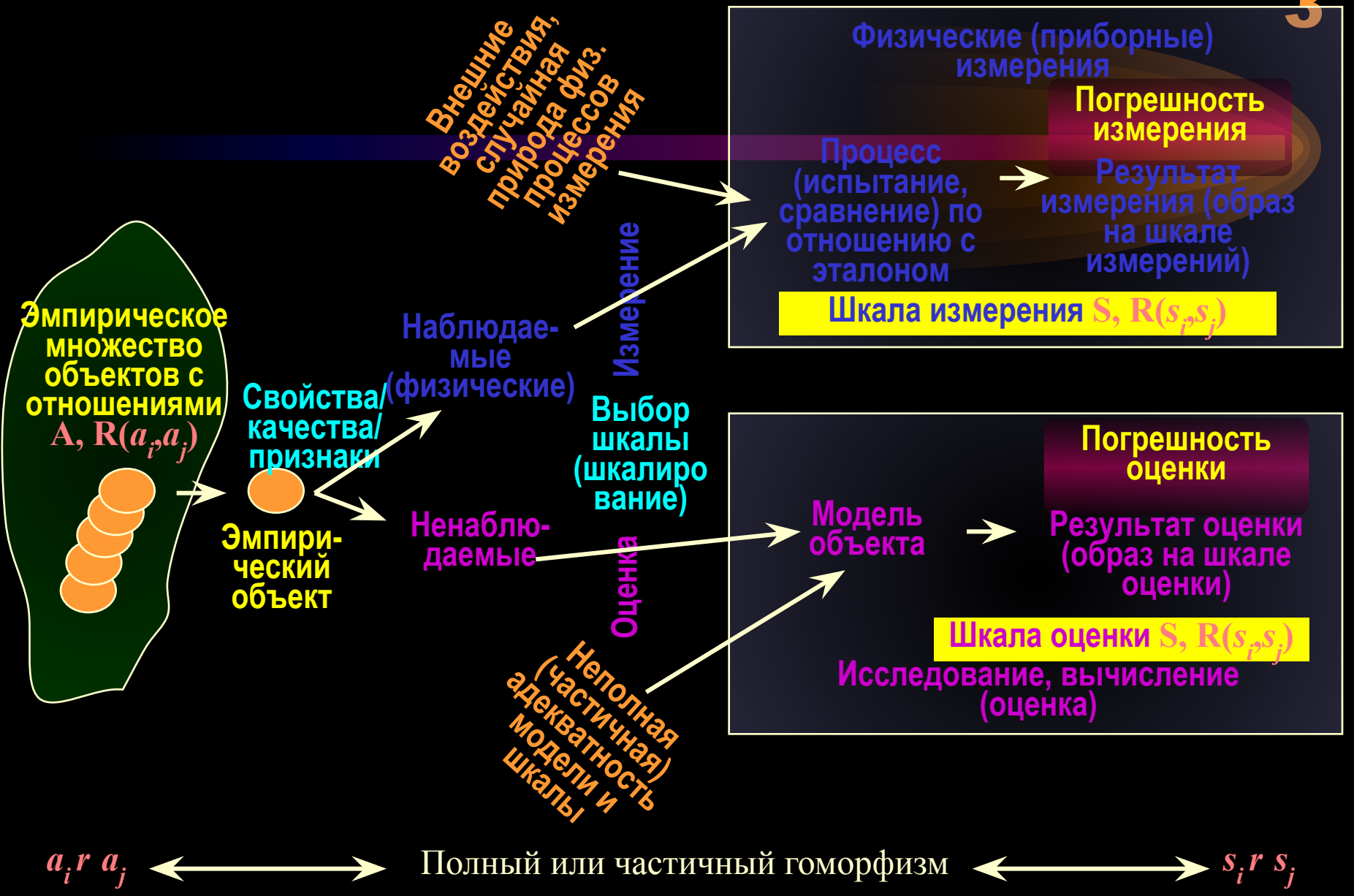
Литература:

1. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.

2. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос-АРВ, 2007. – 352с.

3. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс: Учебное пособие. – М.: Гелиос-АРВ, 2002. – 308с.

1. Общая характеристика измерения (оценки) эмпирических объектов



$a_i r\ a_j$ ⟷ Полный или частичный гоморфизм ⟷ $s_i r\ s_j$

1. Общая характеристика измерения (оценки) эмпирических объектов

Шкалы номинального (назывного) типа

-только для различения объектов (z.b. номера телефонов, автомобилей, коды городов, объектов и т.п.);

-не воспроизводят никаких отношений (порядка и т.д.) кроме отношений различия/эквивалентности (если $a_i \neq a_j$, то $s_i \neq s_j$; если $a_i \equiv a_j$, то $s_i \equiv s_j$);

-могут применяться для классификации объектов (номера/идентификаторы классов – результаты классификационного шкалирования объектов)

Шкалы порядкового (рангового) типа

-воспроизводят отношения порядка (строгого) и эквивалентности (если $a_i \leq a_j$, то $s_i \leq s_j$);

-обеспечивают упорядочение объектов по измеряемым (анализируемым/оцениваемым) свойствам (z.b. шкала твердости минералов Ф. Мооса, шкалы силы ветра, шкалы силы землетрясения, шкалы сортности товаров, шкалы оценки знаний);

-результаты измерений/оценок не являются числами в полном смысле – не могут складываться, умножаться и т.д.);

-из одной порядковой шкалы другая эквивалентная м.б. получена в результате монотонно-возрастающего преобразования

1. Общая характеристика измерения (оценки) эмпирических объектов

Шкалы интервалов

-воспроизводят кроме отношений эквивалентности и порядка (больше/меньше), еще и отношения интервалов (сколько между объектами);

-результаты измерений при линейных преобразованиях сохраняют неизменными интервалы между объектами измерения

$$\frac{s_1 - s_2}{s_3 - s_4} = \frac{f(s_1) - f(s_2)}{f(s_3) - f(s_4)} \quad \text{где } f(x)=ax+b,\ a>0$$

-соответственно одна шкала из другой м.б. получена путем линейного преобразования (z.b. шкалы температур Цельсия, Фаренгейта)

Шкалы отношений

-воспроизводят только отношения степени сравнения эмп. объектов (во сколько раз);

-результаты измерений при преобразованиях подобия $f(x)=ax$, $a>0$ сохраняют неизменными степени отношений объектов (примеры: шкалы измерения масс и длин предметов);

$$\frac{s_1}{s_2} = \frac{f(s_1)}{f(s_2)} \quad \text{где } f(x)=ax,\ a>0$$

-эквивалентные шкалы измерения отношений, получаемые одна из другой преобразованиям подобия имеют общую (нулевую) точку отсчета (примеры: шкалы измерения масс и длин предметов)

1. Общая характеристика измерения (оценки) эмпирических объектов

Шкалы разностей

-как и шкалы интервалов воспроизводят отношения интервалов и (на сколько один объект превосходит по измеряемому свойству другой объект), но не выражают отношения степеней сравнения;

-результаты измерений при преобразованиях сдвига $f(x)=x+b$ сохраняют неизменными разности измеряемых величин объектов (примеры: шкалы измерения масс и длин предметов);

-эквивалентные шкалы измерения отношений получаются одна из другой преобразованиям сдвига (примеры: шкалы прироста продукции, шкалы увеличения численности чего-либо, шкалы летоисчисления)

Абсолютные шкалы

-характеризуют единственность отображения измеряемых объектов в определенную (естественную, абсолютную шкалу);

-воспроизводят любые отношения между измеряемыми объектами (различия/эквивалентности, порядка, степени, интервалов, разности). Пример: - шкалы измерения количества объектов

1. Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС

Стандартизация – разработка и применение нормативно-технических и нормативно-методических документов в целях достижения упорядоченности в сферах разработки, производства и обращения *изделий*, *продукции*, *строений*, *сооружений*, *систем*, *процессов*, *процедур*, *работ* или *услуг*

Стандарт
- **нормативно-технический документ**, содержащий требования и характеристики к объекту стандартизации

Цели стандартизации

- повышение **уровня безопасности** жизни или здоровья граждан, имущества физических или юридических лиц, государственного или муниципального имущества, экологической безопасности, безопасности жизни или здоровья животных и растений;
- повышение уровня безопасности объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера;
- обеспечение научно-технического прогресса;
- повышение конкурентоспособности продукции, работ, услуг;
- рациональное использование ресурсов;
- обеспечение **технической и информационной совместимости**;
- обеспечение сопоставимости результатов исследований (испытаний) и измерений, технических и экономико-статистических данных;
- обеспечение взаимозаменяемости продукции.

1. Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС

Стандарты в сфере безопасности ИТ

По типу объекта стандартизации

- система (информационная, техническая, организационно-технологическая, аппаратная, криптографическая и т.д.)
- ИТ-продукт
- ИТ-технологии (в т.ч. **процессы**, **процедуры**)

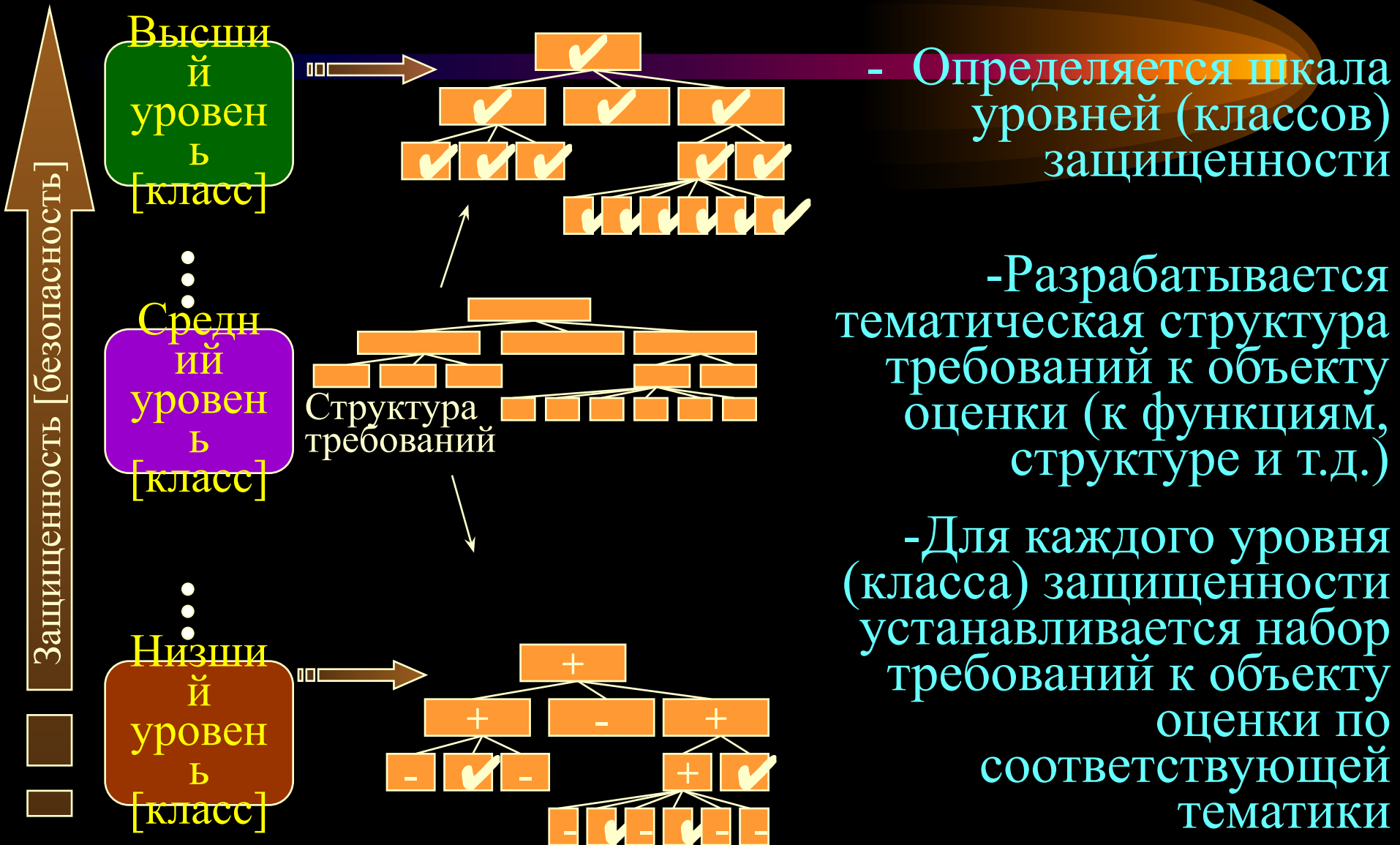
По типу шкалы оценки соответствия требованиям стандарта

- на основе номинальной шкалы (соответствует/несоответствует)
- на основе интервальной (количественной) шкалы (z.b. вероятность обнаружения атаки $\geq 0{,}99$)
- на основе ранговой (качественной) шкалы (реализация требований на «отлично», «хорошо», «удовлетворительно»; защищенность *высокая*, *средняя*, *низкая*, *незначительная*)

В большинстве Стандартов защищенности используются номинально-ранговые шкалы (оценки)

1. Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС

Общая схема стандартов и руководящих документов по функциональным требованиям к защищенным КС на основе номинально-ранговых оценок защищенности [безопасности]



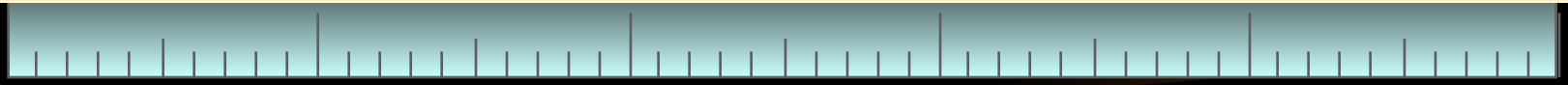
- Определяется шкала уровней (классов) защищенности

-Разрабатывается тематическая структура требований к объекту оценки (к функциям, структуре и т.д.)

-Для каждого уровня (класса) защищенности устанавливается набор требований к объекту оценки по соответствующей тематики

История создания стандартов информационной (компьютерной) безопасности

Единая шкала оценки безопасности для производителей, потребителей и экспертов



1. Критерии оценки надежных компьютерных систем (Оранжевая книга), NCSC МО США, 1983г. (по сетям - 1987, по СУБД - 91)
2. Европейские критерии безопасности информационных технологий 1986г. (Гармонизированные критерии, 1991г.) (Франция, Германия, Голландия, Англия)
3. Руководящие документы Гостехкомиссии при России по защите от НСД к информации, 1992г.
4. Федеральные критерии безопасности информационных технологий, ANSI и АНБ США (1992г.)
5. Канадские критерии безопасности компьютерных систем (1993г.)
6. Единые критерии безопасности информационных технологий, NCSC и АНБ США, 1996г.

1. Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС

Порядок использования и применения стандартов защищенности [стандартов ИБ]

Разработчики

1. Определение (получение) функциональных требований к объекту разработки
2. Определение (получение) требований по уровню (классу) защищенности
3. Составление на основе ГОСТ 34.201-89 и соотв. Стандарта защищенности ТЗ на разработку
4. Разработка (создание) объекта и реализация требований к объекту
5. Оценка соответствия разработанного объекта установленным требованиям и получение сертификата защищенности по соотв. классу (уровню)

Заказчики

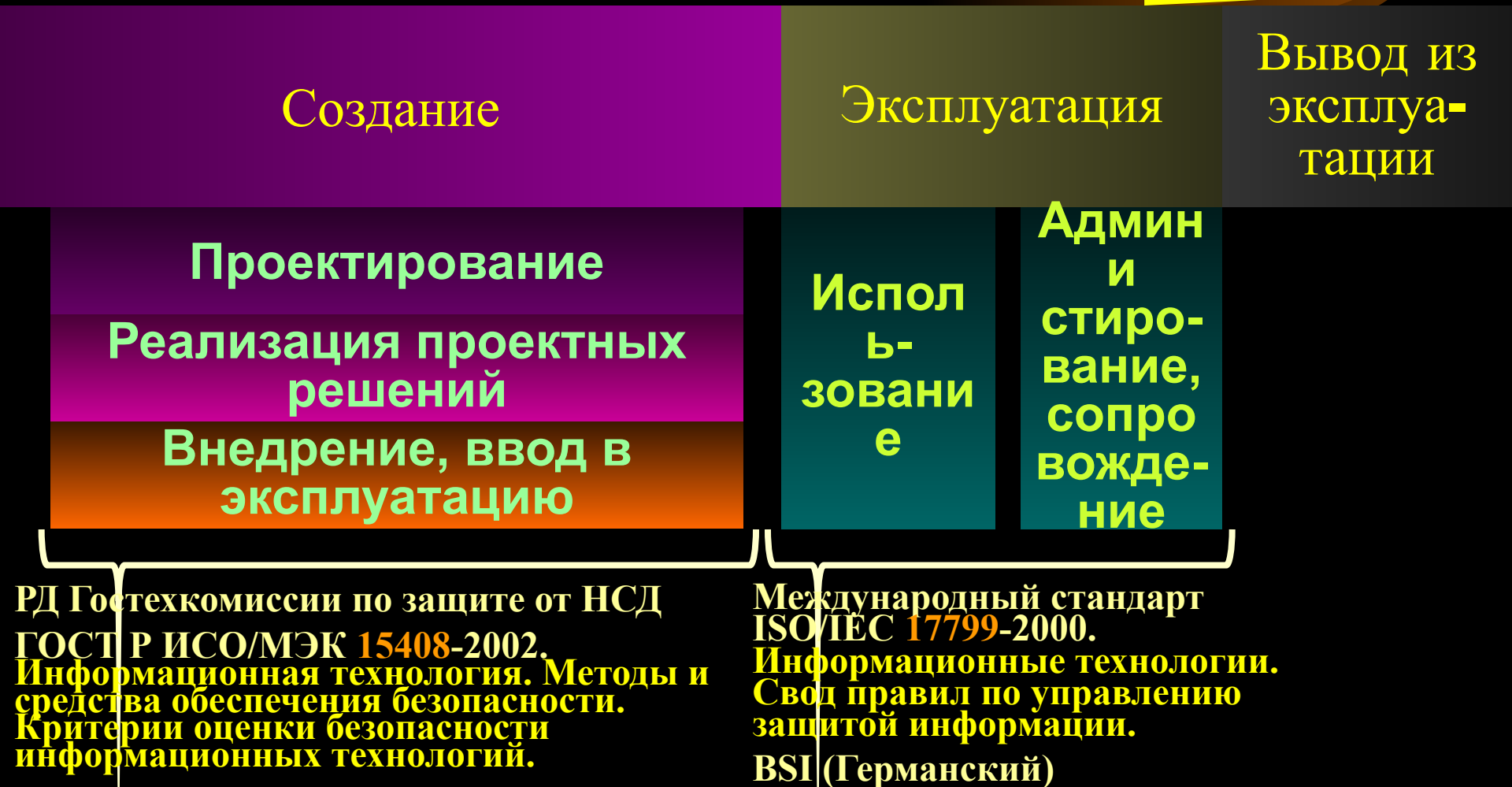
1. Потребность в объекте в защищенном исполнении (или в СЗИ)
2. Определение (по нормативным предписаниям или по решению руководителя) требуемого уровня (класса) защищенности
3. Заказ на разработку или приобретение готового объекта (продукта) с сертификатом безопасности по соответствующему классу (уровню)
4. Приемка объекта в эксплуатацию (при соотв. нормативных предписаниях аттестация объекта в защищенном исполнении)

Эксперты

1. Получение заявки на сертификацию по определенному классу защищенности
2. Определение по стандарту защищенности набора требований к объекту оценки
3. Разработка на основе ГОСТ 28195-89 и ГОСТ Р 51188-98 Программы испытаний (исследований)
4. Испытания (исследования) и вынесение решения о соответствии объекта заявленному уровню (классу) защищенности

1. Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС

Сфера действия стандартов ИБ (защищенности) АИС



РД Гостехкомиссии по защите от НСД

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

Международный стандарт ISO/IEC 17799-2000. Информационные технологии. Свод правил по управлению защитой информации.

BSI (Германский)

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

В основе РД от НСД – методология **TCSEC (**Оранжевая книга)

Уровень защищенности КС

Известные и апробированные требования по архитектуре КС, применяемым механизмам и средствам защиты

Ранговая шкала степени защищенности

- Самый высокий уровень защиты
- Средний уровень защиты
- Низкий уровень защиты
- Незащищенные системы

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

3

4

Схема РД ГосТехКомиссии России. СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации

СВТ

- совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем

в т.ч. общесистемные программные средства, СУБД и ОС с учетом архитектуры ЭВМ

7-классов защищенности в 4 группы по принципу разграничения доступа

4-я группа

Высший уровень защиты

1-й класс

Мандатная защита

3-я группа

2-й класс

3-й класс

4-й класс

Дискреционная защита

2-я группа

5-й класс

6-й класс

1-я группа

7-й класс

Верифицированная защита

*"Секретно", или собственность государства - **не ниже** 4-го класса*

Требования предъявля-лись, но оказались ниже 6-го класса

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

Структура функциональных требований по защите от НСД к СВТ

Система защиты от НСД к информации в СВТ
(подсистемы и функциональные требования)
ГОСТ Р 50739-95

Подсистема разграничения доступа

- Дискреционный принцип разграничения доступа
- Мандатный принцип разграничения доступа
- Идентификация и аутентификация
- Очистка памяти
- Изоляция модулей
- Защита ввода и вывода на отчуждаемый физический носитель информации
- Сопоставление пользователя с устройством

Подсистема учета (аудита)

- Регистрация (событий)
- Маркировка документов

Подсистема гарантированности защиты

- Гарантии проектирования
- Надежное восстановление
- Целостность КСЗ
- Контроль модификации
- Контроль дистрибуции
- Гарантии архитектуры
- Взаимодействие пользователя с КСЗ
- Тестирование

Конкретный набор требований задается в зависимости от класса (уровня) защиты СВТ

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

Структура требований по классам защищенности СВТ

Наименование показателя	Классы защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гаранитии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	-	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	=
Тестирование	+	+	+	+	+	=
Руководство пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская документация	+	+	+	+	+	=

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

Схема групп и классов защищенности АС от НСД

«Гостайна", или собственность государства - ***не ниже*** **3А, 2А, 1А (для 1А** с СВТ не ниже **2кл.), 1Б** (с СВТ не ниже **3 кл.), 1В** (с СВТ не ниже **4-го кл.)**

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

2 3 8

Система защиты от НСД к информации в АС

(подсистемы и функциональные требования)

ГОСТ Р 51583-2000, РД ГосТехКомиссии. АС. Защита от НСД к информации. Классификация АС и требования по защите информации

Подсистема управления доступом

- Идентификация, проверка подлинности, контроль доступа
- Управление потоками информации

Подсистема регистрации и учета

- Регистрация и учет
- Учет носителей информации
- Очистка освобождаемых областей памяти
- Сигнализация попыток нарушения защиты

Криптографическая подсистема

- Шифрование конфиденциальной информации
- Шифрование информации, принадлежащей различным субъектам доступа на разных ключах
- Использование сертифицированных криптографических средств

Подсистема обеспечения целостности

- Обеспечение целостности программных средств и обрабатываемой информации
- Физическая охрана СВТ и носителей информации
- Наличие администратора защиты информации
- Периодическое тестирование СЗИ от НСД
- Наличие средств восстановления СЗИ от НСД
- Использование сертифицированных средств защиты

Конкретный набор требований задается в зависимости от класса (уровня) защиты АС

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

2 3 9

Общая характеристика классов защищенности АС

Третья группа

Класс 3Б

- регламентируются требования обязательной парольной идентификации и аутентификации пользователя при входе в систему, регистрации входа/выхода пользователей, учета используемых внешних носителей, обеспечения целостности средств защиты информации (СЗИ), обрабатываемой информации и программной среды, а также наличие средств восстановления СЗИ.

Класс 3А

- + дополнительно устанавливаются требования по регистрации распечатки документов, физической очистке освобождаемых областей оперативной памяти и внешних носителей, усиливаются требования по обеспечению целостности СЗИ и программной среды через проверку целостности при каждой загрузке системы, периодическое тестирование функций СЗИ при изменении программной среды и персонала АС

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

2 4 0

Общая характеристика классов защищенности АС

Вторая группа

Класс 2Б

- в основном совпадают с требованиями класса 3Б с некоторым усилением требований по подсистеме обеспечения целостности (при загрузке системы)

Класс 2А

- + усиление требований по подсистеме управления доступом (идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств, а также программ, томов, каталогов, файлов, записей, полей записей, что обеспечивает избирательное управление доступом) и усилением требований по подсистеме регистрации и учета (регистрация не только входа/выхода субъектов, но загрузки и инициализации операционной системы, программных остановов, регистрация выдачи документов, запуска программ, обращений к файлам и другим защищаемым объектам, автоматический учет создаваемых файлов, что обеспечивает регистрацию всех потенциально опасных событий). Дополнительно регламентируется управление потоками информации с помощью меток конфиденциальности (*элементы полномочного управления доступом*), очистка освобождаемых участков оперативной и внешней памяти, а также *шифрование* всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа носители данных.

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

Общая характеристика классов защищенности АС

Первая группа

Класс 1Д

- требования, содержательно и идеологически совпадающие с требованиями классов 3Б и 2Б

Класс 1Г

- + требования содержательно и идеологически сходные с требованиями класса 2А (за исключением требований по шифрованию информации) с учетом различий в полномочиях пользователей – избирательное управление доступом в соответствии с матрицей доступа, регистрация потенциально опасных событий, очистку освобождаемых участков оперативной и внешней памяти

2. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации

Общая характеристика классов защищенности АС

Первая группа

Класс 1В

- + Дополнительно регламентируется полномочное управление доступом (метки конфиденциальности объектов и полномочия субъектов доступа), усиливаются требования к подсистеме регистрации опасных событий, вводится требование наличия администратора защиты и его интерактивного оповещения о попытках несанкционированного доступа.

Класс 1Б

- + дополнительно требования по шифрованию информации (аналогично классу 2А).

Класс 1А

- + дополнительные требования использования разных ключей шифрования различными субъектами доступа

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

История создания «Общих критериев»

1. 1990г. начало разработки Раб.гр. 3 Подкомитета 27 Первого технического комитета (JTCI|SC27|WG3) Международной организации по стандартизации (ISO) «Критериев оценки безопасности информационных технологий» (Eva-luation Criteria for IT Security, ECITS) в качестве международного стандарта
2. 1993г. начало совместной разработки правительственными организациями Канады, США, Великобритании, Германии, Нидерландов и Франции межгосударственного стандарта «Общие критерии оценки безопасности информационных технологий» (Common Criteria for IT Security Evaluation), т. н. «Общие критерии», иди ОК (Common Criteria)
3. 1998г. опубликование и широкое открытое обсуждение версии 2.0 ОК и ее принятие в августе 1999г.
4. Принятие и введение в действие с 1 декабря 1999г. Международного стандарта ISO/IEC 15408 Information technology – Security techniques – Evaluation Criteria for IT Security в 3-х частях:
   - Part 1: Introduction and general model. – ISO/IEC 15408-1.1999
   - Part 2: Security functional requirements. – ISO/IEC 15408-2.1999
   - Part 3: Security assurance requirements. – ISO/IEC 15408-3/1999
5. Принятие в 2002г. ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий» на основе идентичного перевода ISO/IEC 15408-1999 с датой введения с 1 января 2004г.
6. 2002г. Принятие Руководящего документа ГосТехКомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» на основе идентичного текста ГОСТ Р ИСО/МЭК 15408-2002

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Общая характеристика «Общих критериев»

4

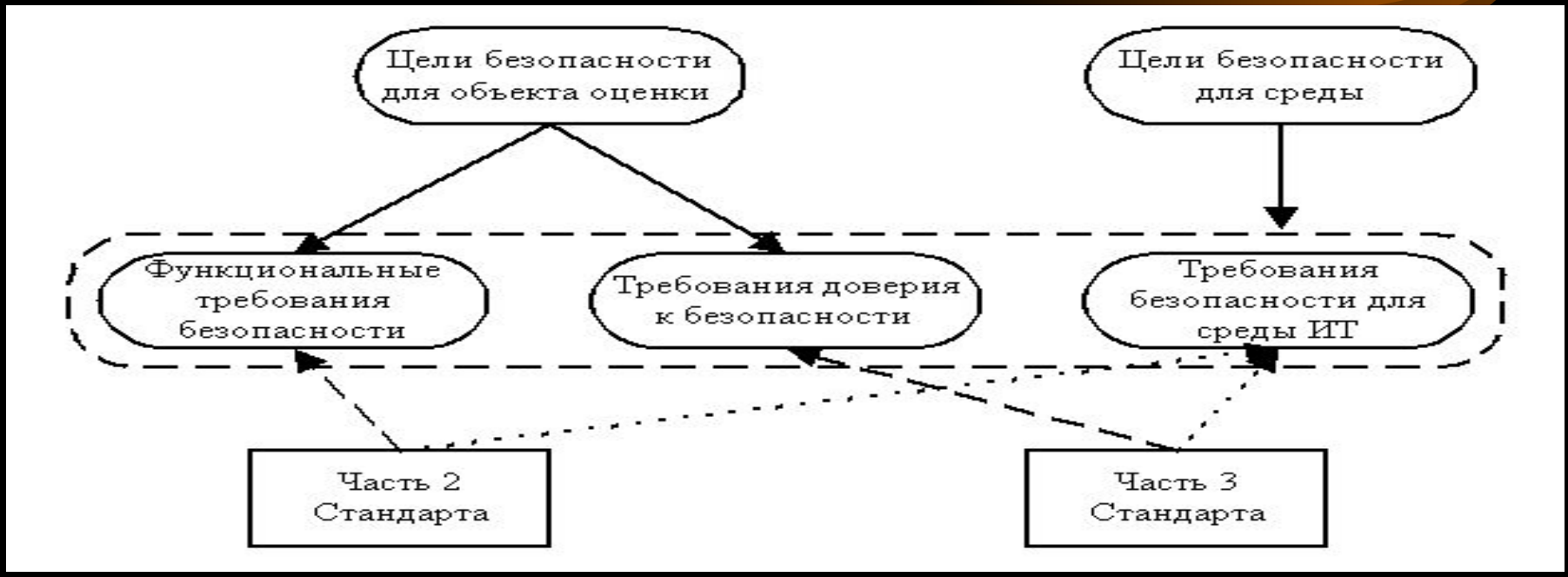
1. Регламентирует процессы создания и оценки (сертификации) изделий ИТ по требованиям безопасности
2. **Объектом оценки (ОО)** является **продукт ИТ** (*совокупность средств ИТ, предоставляющих определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы*) или **система ИТ** (*специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации*)
3. Рассматривает **ОО** в контексте всех аспектов **среды безопасности**, которая в идеологии ОК включает:
   - **законодательную среду** (затрагивающую **ОО**)
   - **административную среду** (положения политик и программ безопасности, затрагивающие **ОО**)
   - **процедурно-технологическую среду** (физ.среда, в т.ч. меры физической защиты, персонал и его свойства, эксплуатационные и иные процедуры, связанные с **ОО**)
   - **программно-техническую среду** (в которой функционирует **ОО** и его защищаемые активы)
4. Устанавливает следующую **структуру описания аспектов среды безопасности** при задании требований безопасности к объекту ОО и его оценки:
   - **предположения безопасности** (выделяют ОО из общего контекста, задают границы рассмотрения)
   - **угрозы безопасности** (те, ущерб от которых нуждается в уменьшении, по схеме: источник, метод воздействия, используемые уязвимости, ресурсы-активы на которые направлены)
   - **положения политики безопасности** (в совокупности с предположениями безопасности устанавливают точно для системы ИТ или в общих чертах для продукта ИТ все другие аспекты среды безопасности)

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Общая характеристика «Общих критериев»

5. Регламентирует виды и порядок **установления требований безопасности** к изделиям ИТ, порядок и структуру требований к оценки реализации установленных требований

Виды требований безопасности к продуктам и системам ИТ



Порядок установления требований безопасности к продуктам и системам ИТ

Каталог (библиотека) требований ко всем возможным видам продуктов или систем ИТ (ч.2 ОК)

Профили защиты для конкретных видов изделий ИТ- ОС, СУБД, МЭ и т.д (подлежат сертификации)

Задание по безопасности при создании изделия ИТ (является ОО наряду с самим ОО при сертификации ОО)

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Общая характеристика «Общих критериев»

6. Регламентирует структуру и виды **установления требований безопасности** к изделиям ИТ, порядок и структуру требований к оценки реализации установленных требований в **идеологии степени доверия** на основе **ранговой шкалы** оценки к реализации требований по безопасности

Устанавливается **7 уровней доверия** (7-й – наивысший). Сертификаты с 1-го по 4-й признаются всеми странами-участниками «**Клуба ИСО 15408**». Сертификаты 5-го-7-го уровней требуют **подтверждения в национальных системах сертификации**.

7. На основе утвержденных **ПЗ** разрабатываются (создаются) **продукты ИТ** и **оцениваются** на соответствие требованиям безопасности.

Оценка производится на основе применения т.н. **оценочных уровней доверия** (**ОУД – ОУД1, ОУД2,…,ОУД7**)), представленных в стандарте.

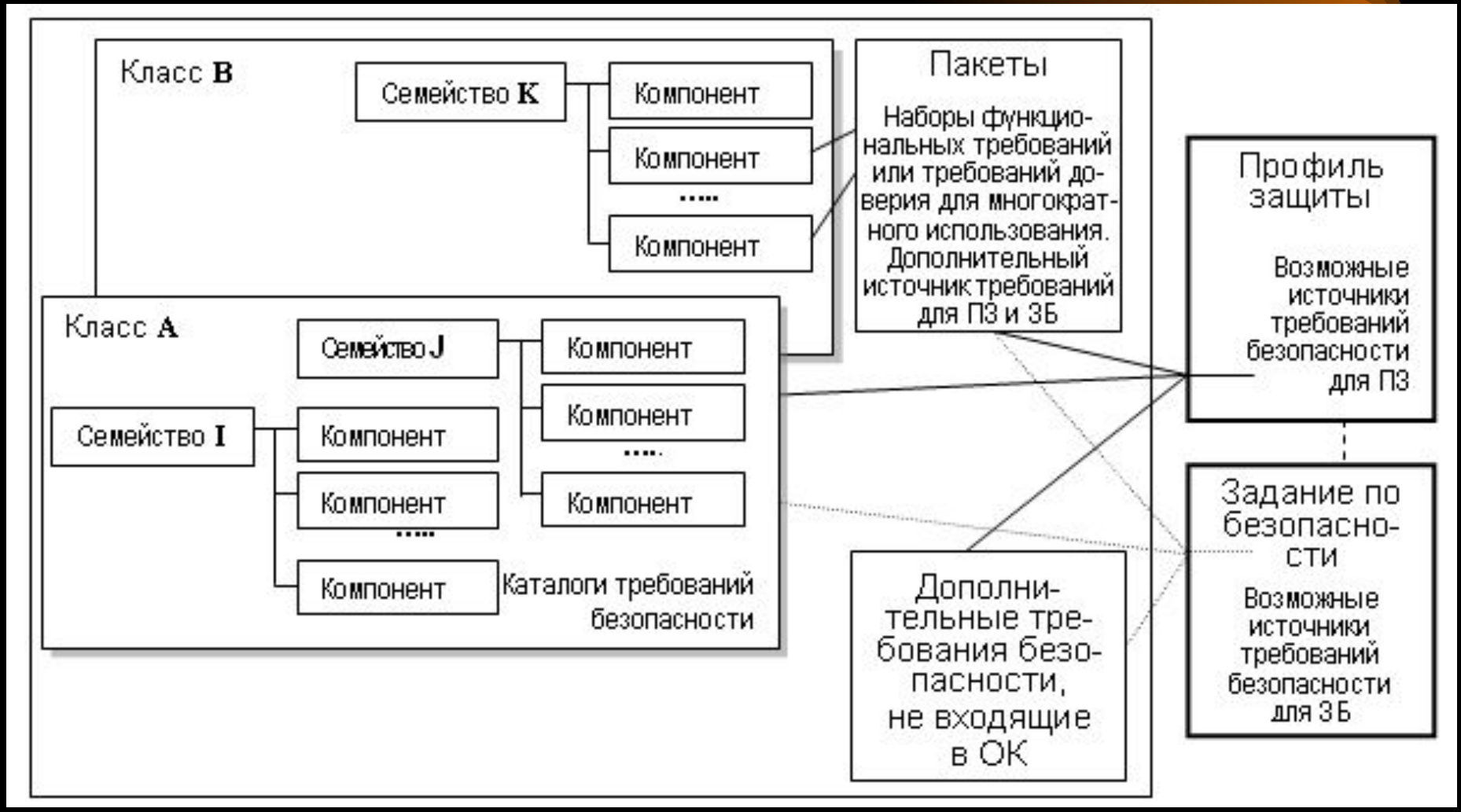
ОУД включают методы и содержание процедур по оценки объектов:

ОУД1 – предусматривает функциональное тестирование
ОУД2 – предусматривает структурное тестирование
ОУД3 – предусматривает методическое тестирование и проверку
ОУД4 – предусматривает методическое проектирование, тестирование и просмотр
ОУД5 – предусматривает полуформальное проектирование и тестирование
ОУД6 – предусматривает полуформальную верификацию проекта и тестирование
ОУД7 – предусматривает формальную верификацию проекта и тестирование

Содержание требований по **ОУД** основывается на совокупности т.н. **компонент доверия**, объединяемых в **4 семейства гарантированности**, из которых, в свою очередь, складываются **7 классов гарантированности** (*гарантированность по управлению конфигурацией, по поставкам и эксплуатации, по разработке, по руководствам, по поддержке жизненного цикла, по тестированию, по оценке уязвимостей*)

Иерархическая структура функциональных требований безопасности ИТ (ГОСТ Р ИСО/МЭК 15408-2002. Ч.2)

11 классов, в каждом классе от 2-х до 16-ти семейств



3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Класс FAU. АУДИТ БЕЗОПАСНОСТИ
1 Автоматическая реакция аудита безопасности (FAU_ARP)
2 Генерация данных аудита безопасности (FAU_GEN)
3 Анализ аудита безопасности (FAU_SAA)
4 Просмотр аудита безопасности (FAU_SAR)
5 Выбор событий аудита безопасности (FAU_SEL)
6 Хранение данных аудита безопасности (FAU_STG)

Класс FCO. СВЯЗЬ
1 Неотказуемость отправления (FCO_NRO)
2 Неотказуемость получения (FCO_NRR)

Класс FCS. КРИПТОГРАФИЧЕСКАЯ ПОДДЕРЖКА
1 Управление криптографическими ключами (FCS_CKM)
2 Криптографические операции (FCS_COP)

Класс FDP. Защита данных пользователя
1 Политика управления доступом (FDP_ACC)
2 Функции управления доступом (FDP_ACF)
3 Аутентификация данных (FDP_DAU)
4 Экспорт данных за пределы действия ФБО (FDP_ETC)
5 Политика управления информационными потоками (FDP_IFC)
6 Функции управления информационными потоками (FDP_IFF)
7 Импорт данных из-за пределов действия ФБО (FDP_ITC)
8 Передача в пределах ОО (FDP_ITT)
9 Защита остаточной информации (FDP_RIP)
10 Откат (FDP_ROL)
11 Целостность хранимых данных (FDP_SDI)
12 Защита конфиденциальности данных пользователя при передаче между ФБО (FDP_UCT)
13 Защита целостности данных пользователя при передаче между ФБО (FDP_UIT)

Класс FIA. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ
1 Отказы аутентификации (FIA_AFL)
2 Определение атрибутов пользователя (FIA_ATD)
3 Спецификация секретов (FIA_SOS)
4 Аутентификация пользователя (FIA_UAU)
5 Идентификация пользователя (FIA_UID)
6 Связывание пользователь-субъект (FIA_USB)

Класс FMT. УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ
1 Управление отдельными функциями ФБО (FMT_MOF)
2 Управление атрибутами безопасности (FMT_MSA)
3 Управление данными ФБО (FMT_MTD)
4 Отмена (FMT_REV)
5 Срок действия атрибута безопасности (FMT_SAE)
6 Роли управления безопасностью (FMT_SMR)

Класс FPR. ПРИВАТНОСТЬ
1 Анонимность (FPR_ANO)
2 Псевдонимность (FPR_PSE)
3 Невозможность ассоциации (FPR_UNL)
4 Скрытность (FPR_UNO)

Класс FPT. ЗАЩИТА ФБО (функций безопасности объекта)
1 Тестирование базовой абстрактной машины (FPT_AMT)
2 Безопасность при сбое (FPT_FLS)
3 Доступность экспортируемых данных ФБО (FPT_ITA)
4 Конфиденциальность экспортируемых данных ФБО (FPT_ITC)
5 Целостность экспортируемых данных ФБО (FPT_ITI)
6 Передача данных ФБО в пределах ОО (FPT_ITT)
7 Физическая защита ФБО (FPT_PHP)
8 Надежное восстановление (FPT_RCV)
9 Обнаружение повторного использования (FPT_RPL)
10 Посредничество при обращениях (FPT_RVM)
11 Разделение домена (FPT_SEP)
12 Протокол синхронизации состояний (FPT_SSP)
13 Метки времени (FPT_STM)
14 Согласованность данных ФБО между ФБО (FPT_TDC)
15 Согласованность данных ФБО при дублировании в пределах ОО (FPT_TRC)
16 Самотестирование ФБО (FPT_TST)

Класс FRU. ИСПОЛЬЗОВАНИЕ РЕСУРСОВ
1 Отказоустойчивость (FRU_FLT)
2 Приоритет обслуживания (FRU_PRS)
3 Распределение ресурсов (FRU_RSA)

Класс FTA. ДОСТУП К ОО
1 Ограничение области выбираемых атрибутов (FTA_LSA)
2 Ограничение на параллельные сеансы (FTA_MCS)
3 Блокирование сеанса (FTA_SSL)
4 Предупреждения перед предоставлением доступа к ОО (FTA_TAB)
5 История доступа к ОО (FTA_TAH)
6 Открытие сеанса с ОО (FTA_TSE)

Класс FTP. ДОВЕРЕННЫЙ МАРШРУТ / КАНАЛ
1 Доверенный канал передачи между ФБО (FTP_ITC)
2 Доверенный маршрут (FTP_TRP)

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Иерархическая структура функциональных требований безопасности ИТ (ГОСТ Р ИСО/МЭК 15408-2002. Ч.2)

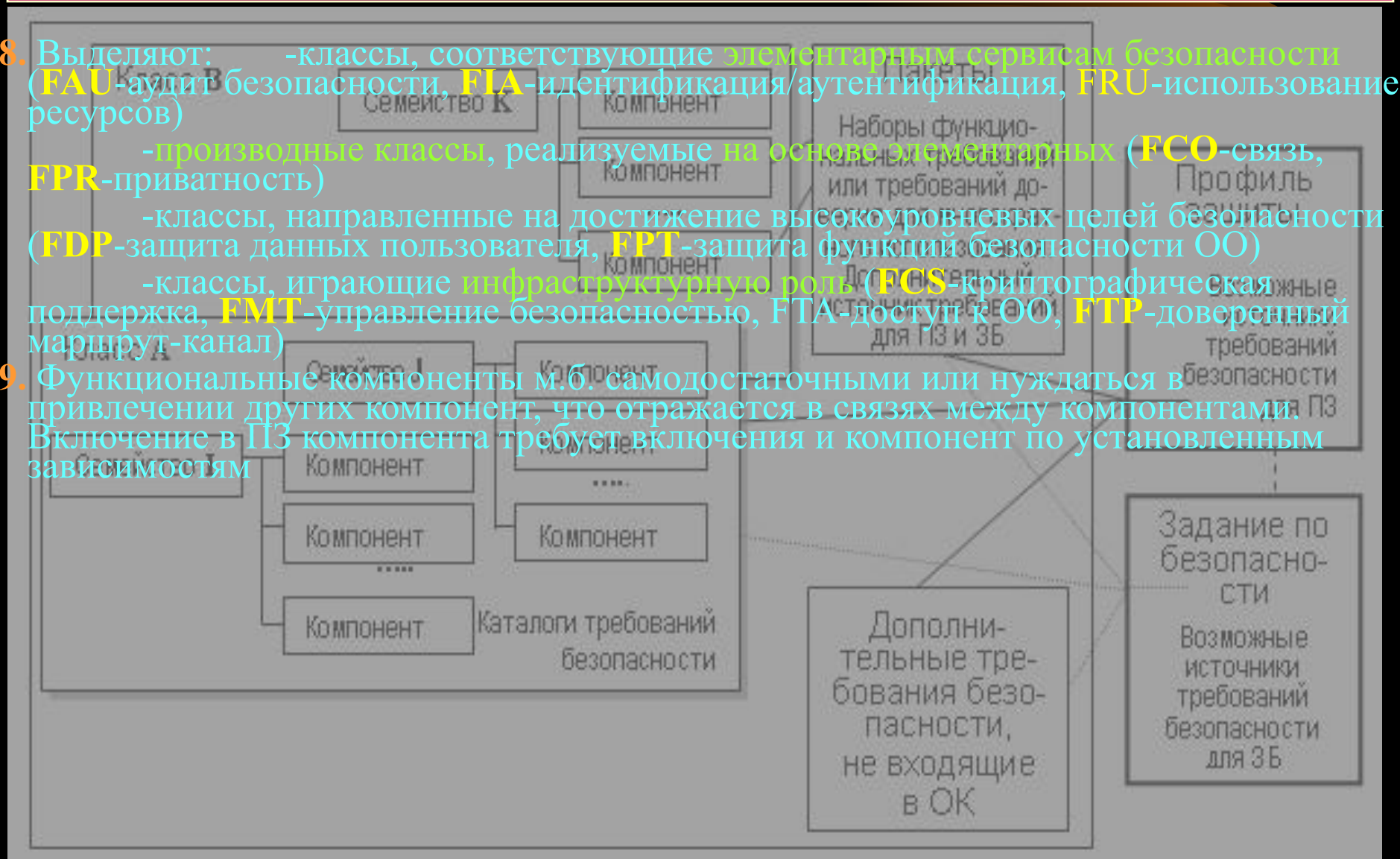
8. Выделяют: -классы, соответствующие элементарным сервисам безопасности (**FAU**-аудит безопасности, **FIA**-идентификация/аутентификация, FRU-использование ресурсов)

-производные классы, реализуемые на основе элементарных (**FCO**-связь, **FPR**-приватность)

-классы, направленные на достижение высокоуровневых целей безопасности (**FDP**-защита данных пользователя, **FPT**-защита функций безопасности ОО)

-классы, играющие инфраструктурную роль (**FCS**-криптографическая поддержка, **FMT**-управление безопасностью, FTA-доступ к ОО, **FTP**-доверенный маршрут-канал)

9. Функциональные компоненты м.б. самодостаточными или нуждаться в привлечении других компонент, что отражается в связях между компонентами. Включение в ПЗ компонента требует включения и компонент по установленным зависимостям



3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Классы функциональных требований безопасности ИТ (ГОСТ Р ИСО/МЭК 15408-2002, ч.2)

1. Тестирование базовой абстрактной машины (FPT_AMT)
2. Безопасность при сбое (FPT_FLS)
3. Доступность экспортируемых данных ФБО (FPT_ITA)
4. Конфиденциальность экспортируемых данных ФБО (FPT_ITC)
5. Целостность экспортируемых данных ФБО (FPT_ITI)
6. Передача данных ФБО в пределах ОО (FPT_ITT)
7. Физическая защита ФБО (FPT_PHP)
8. Надежное восстановление (FPT_RCV)
9. Обнаружение повторного использования (FPT_RPL)
10. Посредничество при обращениях (FPT_RVM)
11. Разделение домена (FPT_SEP)
12. Протокол синхронизации состояний (FPT_SSP)
13. Метки времени (FPT_STM)
14. [illegible]

11. Ограничение области выбираемых атрибутов (FTA_LSA)
12. Ограничение на параллельные сеансы (FTA_MCS)
3. Блокирование сеанса (FTA_SSL)
4. Предупреждения перед предоставлением доступа к ОО (FTA_TAB)
5. История доступа к ОО (FTA_TAH)
6. Открытие сеанса с ОО (FTA_TSE)

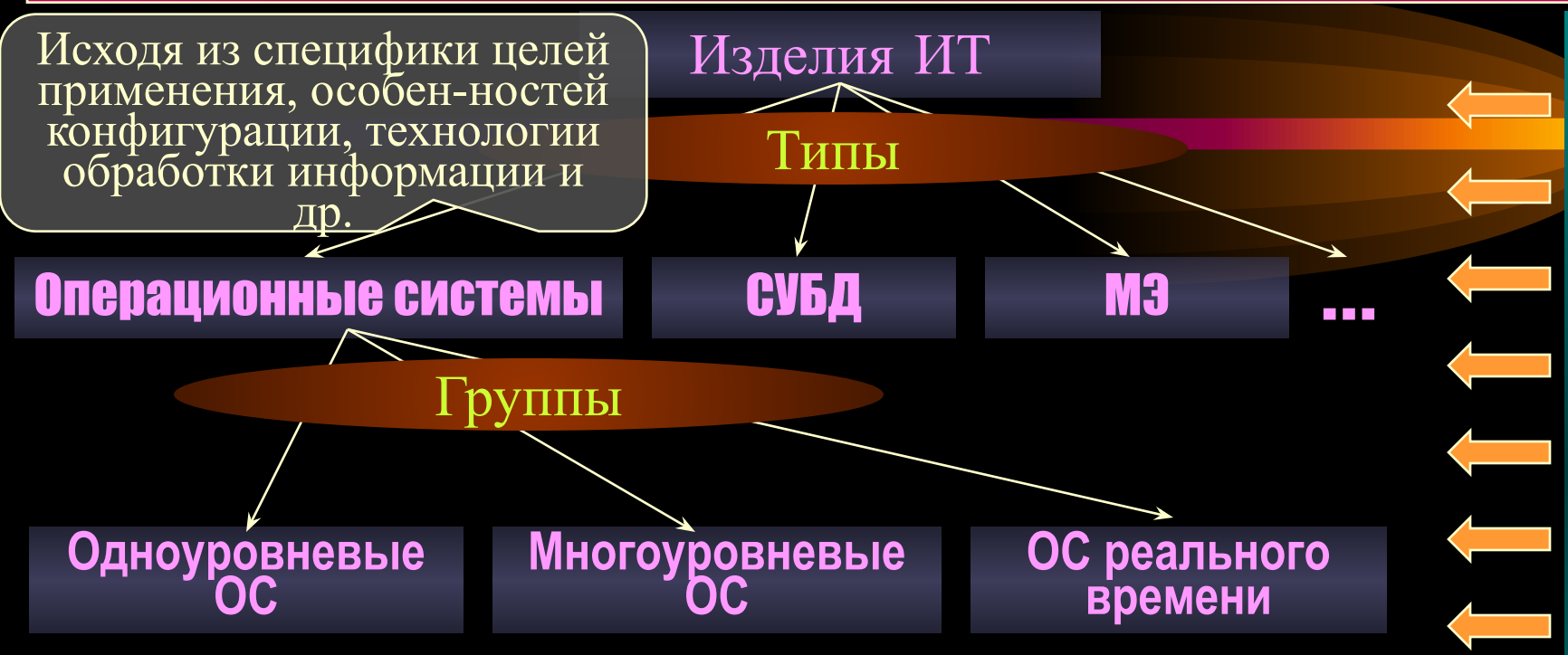
1. Доверенный канал передачи между ФБО (FTP_ITC)
2. Доверенный маршрут (FTP_TRP)

10. [illegible]
11. [illegible]
12. [illegible]
13. Защита целостности данных пользователя при передаче между ФБО (FDP_UIT)

Класс **FTP**. **Доверенный маршрут / канал** (2 семейства)

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Классификация изделий ИТ, функциональные пакеты ТБ



Каталог функциональных Требований безопасности ГОСТ Р ИСО/МЭК 15408-2002. Ч.2

- для каждого **типа** изделий ИТ формируется **семейство профилей защиты**
- для каждого типа (семейства профилей защиты) из всего полного каталога ФТБ (ч.2 ОК) формируется базовый функциональный пакет требований безопасности (**БФПТБ** семейства)
- для каждой **группы** из **БФПТБ семейства** с дополнением ФТБ из общего каталога ФТБ (ч.2 ОК) формируется функциональный пакет требований безопасности группы (**ФПТБ группы**) - БФПТБ семейства $\subseteq$ ФПТБ группы

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Классы защищенности и пакеты требований доверия без-ти

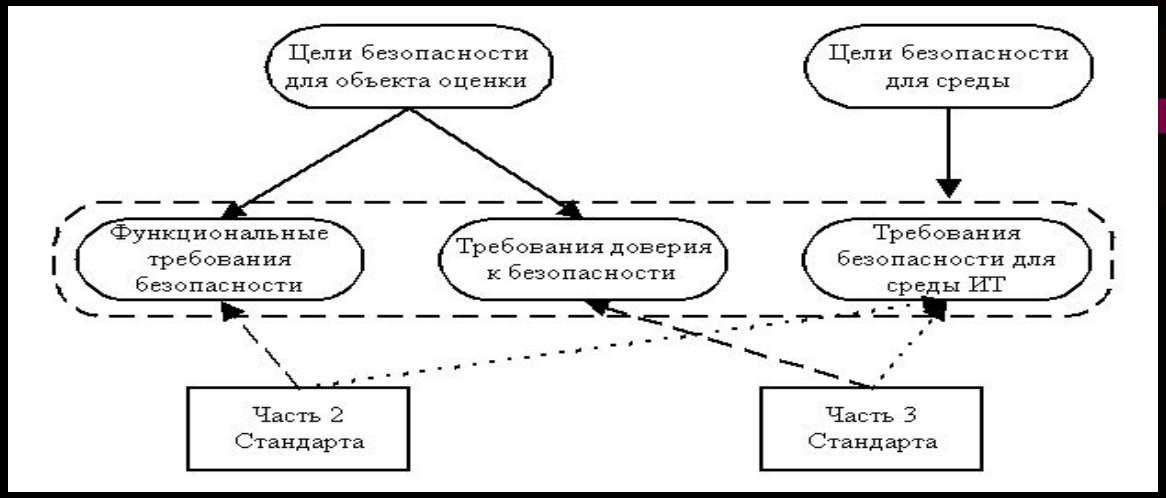
Каталог требований доверия безопасности ГОСТ Р ИСО/МЭК 15408-2002. Ч.3

Соответствие классов защищенности изделий ИТ, базовых пакетов доверия и минимального уровня стойкости функций безопасности

Класс защищенности изделий ИТ	Базовый (минимальный) пакет доверия		Минимальный уровень стойкости функций безопасности
	Оценочный уровень доверия	Дополнительные требования доверия к безопасности ИТ(из РД «Критерии оценки безопасности информационных технологий»)	
1 (первый)	ОУД6	ALC_FLR.3 «Систематическое устранение недостатков» AVA_CCA.3 «Исчерпывающий анализ скрытых каналов»	Высокая СФБ
2 (второй)	ОУД5	ALC_FLR.3 «Систематическое устранение недостатков» AVA_CCA.2 «Систематический анализ скрытых каналов» AVA_VLA.4 «Высоко стойкий»	Высокая СФБ
3 (третий)	ОУД4	ADV_IMP.2 «Реализация ФБО» ADV_INT.1 «Модульность» ALC_FLR.2 «Процедуры сообщений о недостатках» ATE_DPT.2 «Тестирование: проект нижнего уровня» AVA_CCA.1 «Анализ скрытых каналов» AVA_VLA.3 «Умеренно стойкий»	Средняя СФБ
4 (четвертый)	ОУД1		Базовая СФБ

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Общая схема формирования требований безопасности к изделиям и системам ИТ



Формирование функциональных требований безопасности и требований доверия к безопасности при разработке Профиля защиты

Класс защищенности L

↓

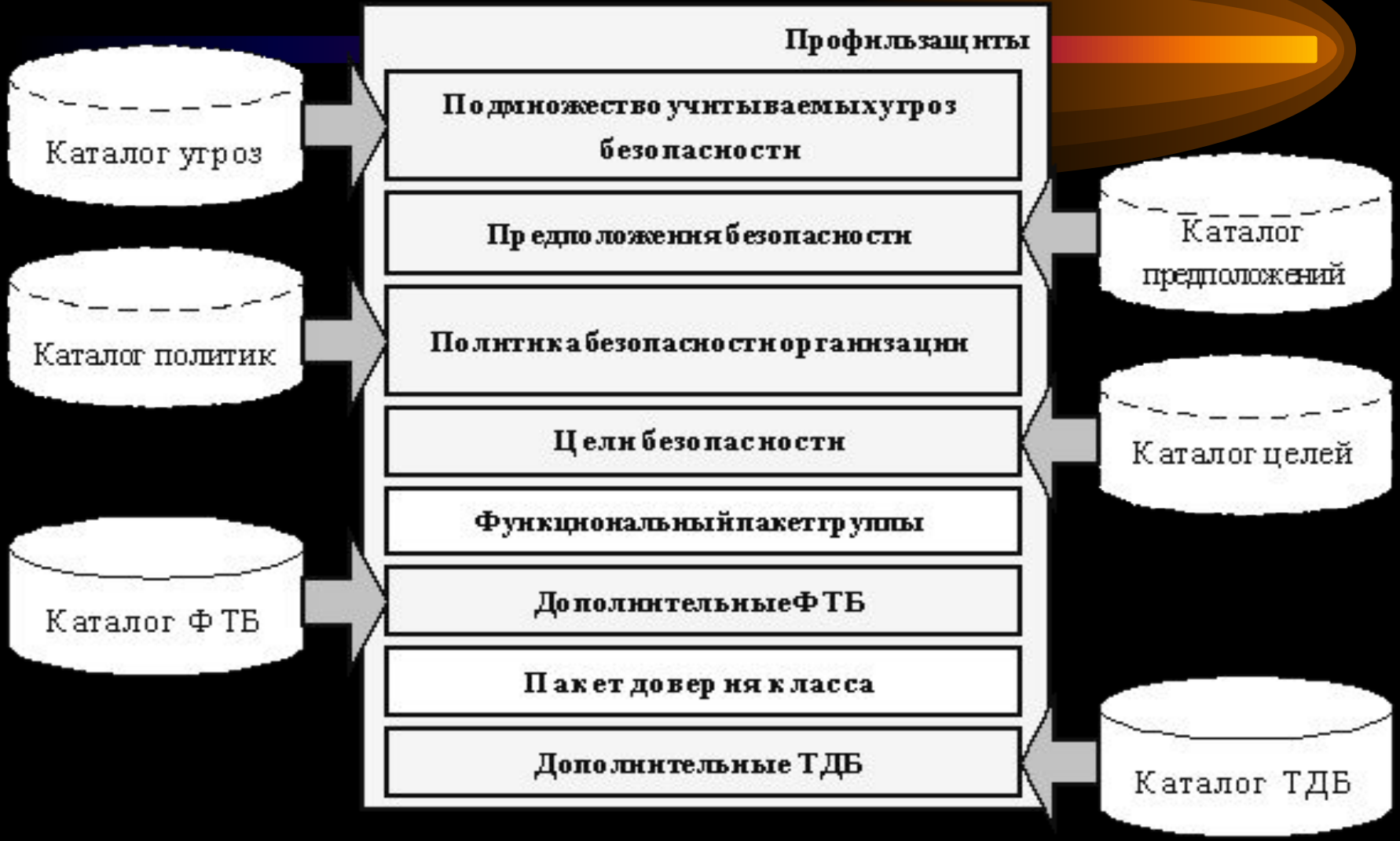
Базовый пакет доверия класса L

↓

Группа К → Функциональный пакет группы К → Профиль защиты

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Общая схема формирования Профиля защиты



3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Организационный порядок разработки профиля защиты

1) -среди зарегистрированных профилей защиты нет соответствующего семейства, или группы, или особенности изделия ИТ, среды безопасности, специфика угроз, политика безопасности организации и класс защищенности не соответствуют зарегистрированным ПЗ
   - принимается **решение о разработке** ПЗ (любым юридическим или физическим лицом по заказу или инициативно)

2) -осуществляется разработка ПЗ в соответствии с *Руководством по формирования семейств ПЗ*, *Положением о разработке ПЗ и ЗБ*, *Руководством по разработке ПЗ и ЗБ*

3) -после завершения разработки проекта ПЗ подается **заявка** на его оценку и сертификацию в испытательную лабораторию на предмет его *полноты, непротиворечивости, технической правильности и возможности использования* при изложении требований к безопасности изделий ИТ;
   -при соответствии результатов испытаний требованиям нормативных документов орган сертификации оформляет отчет о сертификации и выдает **сертификат соответствия ПЗ**

4) -после завершения разработки проекта ПЗ подается **заявка** на его регистрацию в орган регистрации ПЗ в соотв. с *Руководством по регистрации ПЗ*
   -о разработке зарегистрированного проекта ПЗ д.б. **опубликовано уведомление** в информационной системе общего пользования по адресу WWW.GOSTEXKOM.RU (по установленной форме, в т.ч. с указанием срока публичного обсуждения проекта)

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Структура и содержание Профиля защиты

1. Введение
   - 1.1. Идентификация ПЗ
   - 1.2. Аннотация ПЗ
2. Описание изделия ИТ
3. Среда безопасности изделия ИТ
   - 3.1. Предположения безопасности
   - 3.2. Угрозы
   - 3.3. Политика безопасности организации
4. Цели безопасности
   - 4.1. Цели безопасности для изделия ИТ
   - 4.2. Цели безопасности для среды изделия ИТ
5. Требования безопасности изделия ИТ
   - 5.1. Функциональные требования безопасности изделия ИТ
   - 5.2. Требования доверия к безопасности изделия ИТ
   - 5.3. Требования безопасности для среды изделия ИТ
6. Замечания по применению (необязательный)
7. Обоснование
   - 7.1. Обоснование целей безопасности
   - 7.2. Обоснование требований безопасности

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Структура и содержание профиля защиты

1. Введение

1.1.Идентификация ПЗ

а) ключевые слова;
б) оценочный уровень доверия (ОУД), если он применяется в ПЗ;
в) утверждение о соответствии версии ОК;
г) состояние оценки ПЗ.

1.2.Анотация ПЗ

резюме по высокоуровневому обзору проблемы безопасности, которая подлежит решению в ПЗ, и краткий обзор ее решения в ПЗ

Профили защиты, с которыми связан рассматриваемый профиль, и другие документы, на которые ссылается (необязательный подраздел)

Структура и организация профиля защиты (необязательный подраздел)

2. Описание изделия ИТ

а) тип продукта ИТ;
б) основные функциональные возможности ОО;
в) границы ОО (необязательная информация);
г) среда функционирования ОО (необязательная информация).

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Структура и содержание профиля защиты

3. Среда безопасности изделия ИТ

3.1. Предположения безопасности

а) предположения относительно предопределенного *использования* изделия ИТ;

б) предположения, связанные с защитой любой части изделия ИТ *со стороны среды* (например, физическая защита);

в) предположения *связности* (например, межсетевой экран должен быть единственным сетевым соединением между частной (защищаемой) и внешней (потенциально враждебной) сетью);

г) предположения, имеющие отношение *к персоналу* (например, предполагаемые пользовательские роли, основные обязанности (ответственность пользователей и степень доверия этим пользователям).

Каждое предположение, угроза, правило ПБОр д. иметь уникальную метку

3.2. Угрозы

идентификация угроз (идентификация защищаемых активов, источников угроз, методов нападения)

спецификация угроз по соответствующим идентифицированным аспектам

3.3. Политика безопасности организации

совокупность правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности

а) идентификация применяемых *правил управления информационными потоками*;

б) идентификация применяемых *правил управления доступом*;

в) определение *правил* ПБОр для *аудита безопасности*;

г) решения, предписанные организацией, например, использование определенных *криптографических алгоритмов* или *следование определенным стандартам*.

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Структура и содержание профиля защиты

4. Цели безопасности

4.1. Цели безопасности для изделия ИТ

(ответственность за противостояние угрозам и следование ПБОр, промежуточный этап формирования требований безопасности ИТ)

Три типа целей безопасности для ОО:

а) цели **предупредительного** характера, направленные либо на предотвращение реализации угроз, либо на перекрытие возможных путей реализации данных угроз;

б) цели **обнаружения**, определяющие способы обнаружения и постоянного мониторинга событий, оказывающих влияние на безопасное функционирование ОО;

в) цели **реагирования**, определяющие необходимость каких-либо действий ОО в ответ на потенциальные нарушения безопасности или другие нежелательные события, с целью сохранения или возврата ОО в безопасное состояние и/или ограничения размера причиненного ущерба.

Требования:

а) учет каждой идентифицированной угрозы, направленной против изделия ИТ, по *крайней мере, одной целью* безопасности для изделия ИТ;

б) учет каждого правила идентифицированной ПБОр, которому должно удовлетворять изделие ИТ, по крайней мере, одной целью безопасности для изделия ИТ

4.2. Цели безопасности для среды изделия ИТ

(ответст-ть за достиж-е которых возлаг-ся на ИТ-среду, а также связанные с реализацией в пределах среды функцион-я изделия ИТ организационных и других нетехнических мер)

а) противостояние угрозам (или отд-м аспектам угроз), которым *изд-е ИТ не против-т*;

б) поддержку реализации правил ПБОр, которые не удовлетворены или не полностью удовлетворены изделием ИТ;

в) поддержку идентифицированных целей безопасности для изделия ИТ в плане противостояния угрозам и реализации соответствующих правил ПБОр;

г) поддержку идентифицированных предположений о среде.

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Структура и содержание профиля защиты

5. Требования безопасности изделия ИТ

5.1. Функциональные требования безопасности изделия ИТ

Определяют *требования для функций безопасности*, обеспечивающих достижение целей безопасности для изделия ИТ

Выбирают из ч.2 ОК, при наличии из ФПТБ группы

Различают (необязательно) следующие два типа ФТБ:

а) *основные* ФТБ, непосредственно удовлетворяющие конкретные цели безопасности для изделия ИТ;

б) *поддерживающие* ФТБ, не предназначенные для непосредственного удовлетворения целей безопасности для изделия ИТ, но способствующие выполнению основных ФТБ и, тем самым, косвенным образом способствующие удовлетворению целей безопасности для изделия ИТ.

5.2. Требования доверия к безопасности изделия ИТ

Определяют *требуемый уровень уверенности в надлежащей реализации ФТБ*. Выбираются из ч.3 ОК, БПДК в зависимости от:

а) *ценности активов*, подлежащих защите, и осознаваемого риска их компрометации; б) *технической реализуемости*; в) *стоимости разработки* и *оценки*; г) *требуемого времени* для разработки и оценки изделия ИТ; д) *требований рынка* (для продуктов ИТ); е) *зависимостей* функциональных компонентов и компонентов доверия к безопасности.

5.3. Требования безопасности для среды изделия ИТ

определяют *функциональные требования* и *требования доверия* к безопасности, выполнение которых возлагается на *ИТ-среду* (то есть, на внешние по отношению к изделию ИТ аппаратные, программные или программно-аппаратные средства) с тем, чтобы обеспечить достижение целей безопасности для изделия ИТ

Структура и содержание профиля защиты

7. Обоснование

7.1. Обоснование целей безопасности

Демонстрация соответствия целей безопасности идентифицированным угрозам может быть выполнена следующим образом:

а) ***в виде таблицы***, показывающей, какие цели безопасности каким угрозам соответствуют (например, угрозе Т3 соответствует цель О3); при этом необходимо обеспечить соответствие каждой цели безопасности, по крайней мере, одной угрозе;

б) ***логическим обоснованием*** того, что цели безопасности противостоят угрозам

7.2. Обоснование требований безопасности

Демонстрацию соответствия ФТБ целям безопасности для ОО можно представить следующим образом:

а) ***в виде таблицы***, показывающей, какие ФТБ какие цели безопасности удовлетворяют (например, компоненты FRU_RSA.1 и FTP_MCS.1 соответствуют цели безопасности О3), при этом необходимо обеспечить соответствие каждого ФТБ, по крайней мере, одной цели безопасности;

б) ***логическим обоснованием*** соответствия ФТБ целям безопасности.

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Пример разделов ПЗ СУБД

3.2.2 Угрозы, предотвращаемые ОО (СУБД)

Нарушители могут инициировать следующие типы угроз СУБД (или СУБД должна противостоять следующим угрозам).

T.ACCESS *Несанкционированный доступ к базе данных.* Посторонний или пользователь системы, который в настоящее время не является уполномоченным пол
телем базы данных, обращается к СУБД. Эта угроза включает *исполнение роли* лица, которое может или не может быть уполномоченным пользовател
зы данных, а также которое обращается к СУБД, исполняя роль уполномоченного пользователя базы данных (включая уполномоченного пользовател
полняющего роль другого пользователя, который имеет другой, возможно более привилегированный, доступ).

T.DATA *Несанкционированный доступ к информации.* Уполномоченный пользователь базы данных обращается к информации, содержащейся в пределах СУБ
разрешения пользователя базы данных, который является собственником данных или который отвечает за защиту данных.

Эта угроза включает несанкционированный доступ к информации СУБД, остаточной информации, хранящейся в памяти или в ресурсах хранения,
ляемых ОО, или к данным управления БД.

T.RESOURCE *Чрезмерное использование ресурсов.* Аутентифицированный пользователь базы данных использует глобальные ресурсы базы данных путем, который
под угрозу возможность других пользователей базы данных получить доступ к СУБД.

Эта угроза относится к доступности информации в пределах СУБД. Например, пользователь базы данных мог выполнять действия, связанные с исп
ванием чрезмерных ресурсов, периодически препятствуя законному доступу других пользователей базы данных к данным, ресурсам и сервисам. Так
падения могут быть злонамеренными, происходить в результате невнимательности или небрежности, или в случае, когда пользователь базы данных
просто не сознавать потенциальные последствия своих действий. Воздействие таких нападений на готовность и надежность системы может быть ус
многими пользователями, действующими одновременно.

T.ATTACK *Необнаруженное нападение.* Необнаруженная компрометация СУБД происходит в результате действий нарушителя (уполномоченного или неупол
ченного пользователя базы данных), пытающегося выполнить действия, которые он не уполномочен выполнять.

Эта угроза включена, потому что независимо от обеспечения контрмер, адресованным другим угрозам, все же имеется еще остаточная угроза нарушен
литики безопасности нарушителями, пытающимися противостоять этим контрмерам.

T.ABUSE.USER *Неправильное использование привилегий.* Необнаруженная компрометация СУБД происходит в результате действий пользователя базы данных (пред
ренных или нет), связанных с выполнением операций индивидуума, уполномоченного на их выполнение.

Эта угроза включена, потому что независимо от обеспеченных контрмер, адресованных другим угрозам, все же имеется еще остаточная угроза нару
политики безопасности или базы данных, размещенной в опасном месте, в результате действий, предпринятых уполномоченными пользователями
данных. Например, пользователь базы данных может предоставить доступ к объекту БД, ответственным за который он является, другому пользовател
данных, способному использовать эту информацию для мошеннических целей.

Отметим, что эта угроза не распространяется на пользователей базы данных с высоким уровнем доверия: см. предположение A.MANAGE ниже.

3. Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Пример разделов ПЗ СУБД

3.2.3 Угрозы, предотвращаемые средой

T.OPERATE *Опасная операция.* Компрометация базы данных может произойти из-за неправильной конфигурации, администрирования и/или функционирования ной системы.

T.CRASH *Внезапные прерывания.* Внезапные прерывания функционирования ОО могут приводить к потере или разрушению данных, связанных с безопасн таких как данные управления БД и данные аудита. Такие прерывания могут являться результатом ошибки оператора (см. также T.OPERATE) или сбо граммного обеспечения, аппаратных средств, источников питания или носителей данных.

T.PHYSICAL *Физическое нападение.* Критичные к безопасности части ОО или базовой операционной системы и/или сетевых сервисов могут быть подвергнуты ф скому нападению, которое может нарушить безопасность.

3.3 Политики безопасности организации

P.ACCESS Доступ к объектам БД определяется:

а) владельцем объекта БД; и

б) идентификатором субъекта базы данных, пытающегося получить доступ; и

в) привилегиями доступа к объекту БД, которыми владеет субъект базы данных; и

г) административными привилегиями субъекта базы данных; и

д) ресурсами, выделенными субъекту.

Заметим, что эта политика включает следующее:

а) *владение* – владельцы объектов БД ответственны за свои объекты; и

б) *дискреционное управление доступом* – владельцы объектов БД могут предоставлять другим пользователям базы данных доступ или управлени ми объектами БД на основе дискреционного управления доступом; и

с) *ресурсы* - пользователи базы данных уполномочены использовать только те ресурсы, которые распределены им.

P.ACCOUNT Пользователи базы данных ответственны за:

а) операции на объектах, которые определены владельцем объекта; и

б) действия, определенные администраторами базы данных.

Пример разделов ПЗ СУБД

3.4 Предположения

ОО зависит как от технических аспектов ИТ, так и от функциональных аспектов ее среды.

3.4.1 Предположения по ОО

A.TOE.CONFIG ОО инсталлирован, сконфигурирован и управляется в соответствии со своей оцененной конфигурацией.

3.4.2 Основные системные предположения

3.4.2.1 Физические предположения

A.PHYSICAL Ресурсы функционирования ОО и базовой системы расположены в пределах управления средствами доступа, которые предотвращают несанкционированный физический доступ посторонних, пользователей системы и пользователей базы данных.

3.4.2.2 Предположения конфигурации

A.SYS.CONFIG Базовая система (операционная система и/или сервисы безопасности сети, и/или специальное программное обеспечение) инсталлированы, сконфигурированы и управляются в соответствии со своей безопасной конфигурацией.

A.ACCESS Базовая система конфигурирована так, что только санкционированная группа лиц может получить доступ к системе.

A.MANAGE Будут назначены одно или более компетентных доверенных лиц для того, чтобы управлять ОО, базовой системой и безопасностью информации.

3.4.2.3 Предположения связности

A.PEER Предполагается, что любые другие компоненты ИТ, с которыми взаимодействует ОО, будут под тем же самым управлением и функционируют под самой политикой безопасности.

A.NETWORK Предполагается, что когда требуется для ОО, в распределенной среде базовые сервисы сети будут основаны на безопасных протоколах взаимодействия, которые обеспечат аутентичность пользователей.

Пример разделов ПЗ СУБД

4 Цели безопасности

Этот раздел описывает цели безопасности ИТ ОО, а также угрозы и политики, которым они адресованы. В нем далее представлены требования к среде функционирования, необходимые для поддержки целей ИТ ОО.

4.1 Цели безопасности ИТ

Этот подраздел определяет цели безопасности ИТ, которые должны быть удовлетворены с помощью ОО в комбинации со средой безопасности ИТ. В таблице 1 представлено отношение целей безопасности ОО к каждой из угроз и политик безопасности и показано, что всякой угрозе соответствует, по крайней мере, одна цель безопасности ИТ, и что всякая политика безопасности удовлетворена, по крайней мере, одной целью безопасности ИТ. В таблице слово «ДА» указывает, что указанная цель безопасности ИТ уместна для определенной угрозы или политики безопасности.

Таблица 1

Взаимосвязь угроз и политик с целями безопасности ОО

Угрозы\Политики	O.I&A.TOE	O.ACCESS	O.AUDIT	O.RESOURCE	O.ADMIN.TOE
T.ACCESS	ДА	ДА		ДА	ДА
T.DATA	ДА	ДА			ДА
T.RESOURCE	ДА	ДА		ДА	ДА
T.ATTACK	ДА	ДА	ДА		ДА
T.ABUSE.USER	ДА	ДА	ДА		ДА
P.ACCESS		ДА		ДА	
P.ACCOUNT		ДА	ДА		

В разделе 6 представлено логическое обоснование покрытия идентифицированными целями безопасности определенных угроз.

O.ACCESS — ОО должен обеспечить конечных пользователей и администраторов возможностью управления доступом к их собственным данным или ресурсам или к тем, за которые они отвечают в соответствии с политикой безопасности P.ACCESS. Для этого ОО имеет следующие более конкретные цели:

- O.ACCESS.OBJECTS — ОО должен предотвратить несанкционированное или непредусмотренное раскрытие, ввод, модификацию или уничтожение данных и объектов базы данных, а также просмотр базы данных, управление данными и аудит данных базы данных.
- O.ACCESS.CONTROL — ОО должен предоставить возможность пользователям базы данных, которые являются собственниками или ответственными за данные, управлять доступом к этим данным других уполномоченных пользователей базы данных.
- O.ACCESS.RESIDUAL — ОО должен предотвратить несанкционированный доступ к остаточным данным, остающимся в объектах и ресурсах после использования этих объектов и ресурсов.

O.RESOURCE — ОО должен предоставить средства управления использованием ресурсов базы данных уполномоченными пользователями ОО.

O.I&A.TOE — ОО с поддержкой или без поддержки базовой системы должен предоставить средства идентификации и аутентификации пользователей ОО.

O.AUDIT — ОО должен предоставить средства подробной регистрации значимых для безопасности событий для того, чтобы в достаточной мере помочь админ-ру ОО:

а) обнаруживать предпринятые нарушения безопасности или потенциальную ошибку в конфигурации средств безопасности ОО, которые оставили бы базу данных незащищенной от компрометации; и

б) обязать индивидуальных пользователей базы данных быть ответственными за любые выполняемые ими действия, которые являются значимыми для безопасности базы данных в соответствии с политикой P.ACCOUNT.

O.ADMIN.TOE — Там, где необходимо, ОО вместе с базовой системой должен предоставить функции, позволяющие уполномоченному администратору эффективно управлять ОО и его функциями безопасности, обеспечивая, чтобы только уполномоченные администраторы могли получать доступ к такой функциональности.

Пример разделов ПЗ СУБД

4.2 Цели безопасности для среды

Следующие цели безопасности ИТ должны быть удовлетворены средой, в которой ОО используется.

O.ADMIN.ENV Там где необходимо, ОО вместе с базовой системой должен предоставить функц-ные возможности, позволяющие уполномоченному администратору эффективно управлять ОО и его ми без-ти, обеспечивая, чтобы только уполномоченные администраторы могли получать доступ к такой функциональности.

O.FILES Базовая система должна обеспечить механизмы управления доступом, которые позволят защитить от несанкционированного доступа все связанные с СУБД файлы и каталоги (включ полняемые программы, библиотеки рабочих программ, файлы базы данных, экспортируемые файлы, файлы повторной регистрации, управляемые файлы, файлы с трассировкой и ф дампом).

O.I&A.ENV Базовая операционная система должна предоставить средства идентификации и аутентификации пользователей, когда требуется с помощью ОО надежно подтвердить подлинность пол телей.

O.SEP Базовая операционная система должна предоставить средства для изоляции функций безопасности ОО и уверенность в том, что компоненты ФБО не будут искажаться. Составляющим лизующие ФБО, являются: 1) файлы, используемые СУБД для того, чтобы хранить базу данных и 2) процессы ОО, управляющие базой данных.

Следующие, не связанные с ИТ, цели безопасности должны быть удовлетворены процедурными и другими мерами, предпринятыми в пределах среды ОО.

O.INSTALL Ответственные за ОО должны обеспечить, чтобы:

а) ОО был поставлен, инсталлирован, управлялся и использовался в соответствии с эксплуатационной документацией ОО, и

б) Базовая система была инсталлирована и использовалась в соответствии с ее эксплуатационной документацией. Если элементы системы сертифицированы, то они должны быть и лированы и использоваться в соответствии с необходимой документацией сертификации.

O.PHYSICAL Ответственный за ОО должен обеспечить, чтобы те части ОО, которые являются критичными к политике без-ти, были защищены от физич-го нападения.

O.AUDITLOG Администраторы базы данных должны обеспечить, чтобы средства аудита использовались и управлялись эффективно. Эти процедуры должны применяться в журнале аудита базы д и/или журнале аудита для базовой операционной системы, и/или для сетевых сервисов безопасности. В особенности:

а) должны быть предприняты необходимые действия для того, чтобы обеспечить продолжительное функционирование аудита, например, для того, чтобы обеспечить достаточную св ную память, необходимую для регулярной архивации журнала аудита;

б) журналы регистрации событий аудита должны регулярно просматриваться и необходимо определить действия или события, которые могут привести к нарушению безопасности в щем.

в) системные часы д.б. защищены от несанкционированной модификации (так, чтобы целостность меток времени аудита не была скомпрометирована).

O.RECOVERY Ответственный за ОО должен предоставить возможность для процедур и/или механизмов восстановления функционирования на месте после системного сбоя или другого прерыван компромисса с защитой.

O.QUOTA Администраторы базы данных должны обеспечивать, чтобы каждый пользователь ОО имел необходимые квоты, которые:

а) достаточны для выполнения операций, к которым пользователь имеет доступ;

б) достаточно ограничены, чтобы пользователь не мог нарушить режим эксплуатации, доступ к ресурсам и монополизировать ресурсы.

O.TRUST Ответственный за ОО должен обеспечить, чтобы только у пользователей с высоким уровнем доверия была привилегия, которая позволяет им:

а) устанавливать или изменять конфигурацию журнала аудита для базы данных;

б) изменять или удалять любую запись аудита в журнале аудита базы данных;

в) создавать любые учетные данные пользователя или изменять любые атрибуты безопасности пользователя;

г) предоставлять полномочия на использование административных привилегий.

O.AUTHDATA Ответственный за ОО должен обеспечить, чтобы данные аутентификации для любых учетных данных пользователя ОО, так же как и для базовой системы, надежно поддерживалась и н крывались лицам, которые не уполномочены использовать эту учетную запись. В особенности:

а) носители, на которых хранятся данные аутентификации для базовой операционной системы и/или сетевых сервисов безопасности, не должны быть физически устранимы из ба платформы несанкционированными пользователями;

б) пользователи не должны раскрывать свои пароли другим лицам;

в) пароли, сгенерированные администратором системы, должны быть распределены безопасным способом.

O.MEDIA

Пример разделов ПЗ СУБД

Отображение целей безопасности среды на угрозы, цели безопасности ОО, политику и предположения о безопасном использовании

Цели безопасности среды	Противостоящая угроза	Поддерживаемая цель ОО	Поддерживаемая политика	Отображение в предположении о безопасном использовании
O.INSTALL	T.OPERATE			A.TOE.CONFIG, A.SYS.CONFIG, A.MANAGE
O.PHYSICAL	T.PHYSICAL			A.ACCESS, A.PEER, A.PHYSICAL
O.AUDITLOG		O.AUDIT	P.ACCOUNT	A.MANAGE
O.RECOVERY	T.CRASH			A.MANAGE
O.QUOTA		O.RESOURCE		A.MANAGE
O.TRUST			P.ACCESS	A.MANAGE
O.AUTHDATA		O.I&A.TOE	P.ACCESS	A.MANAGE, A.PEER, A.NETWORK
O.MEDIA	T.CRASH			A.MANAGE
O.ADMIN.ENV		O.ADMIN.TOE		A.MANAGE
O.FILES	T.ACCESS		P.ACCESS	A.MANAGE
O.I&A.ENV	T.ACCESS	O.I&A.TOE	P.ACCESS	A.MANAGE
O.SEP	T.ACCESS		P.ACCESS	A.MANAGE

Пример разделов ПЗ СУБД

5.1 Функциональные требования безопасности – основные требования

В приведенной ниже таблице перечисляются функциональные компоненты, включенные в этот ПЗ.

Таблица 3

Список функциональных компонентов

Компонент	Наименование
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
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
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_RIP.2	Полная защита остаточной информации
FIA_ATD.1	Определение атрибутов пользователя
FIA_UID.1	Выбор момента идентификации
FIA_USB.1	Связывание пользователь-субъект
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_REV.1	Отмена
FMT_SMR.1	Роли безопасности
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FRU_RSA.1	Максимальные квоты
FTA_MCS.1	Базовое ограничение на параллельные сеансы
FTA_TSE.1	

Тема 3. **Методы анализа и оценки защищенности компьютерных систем**

Лекция 3.2.

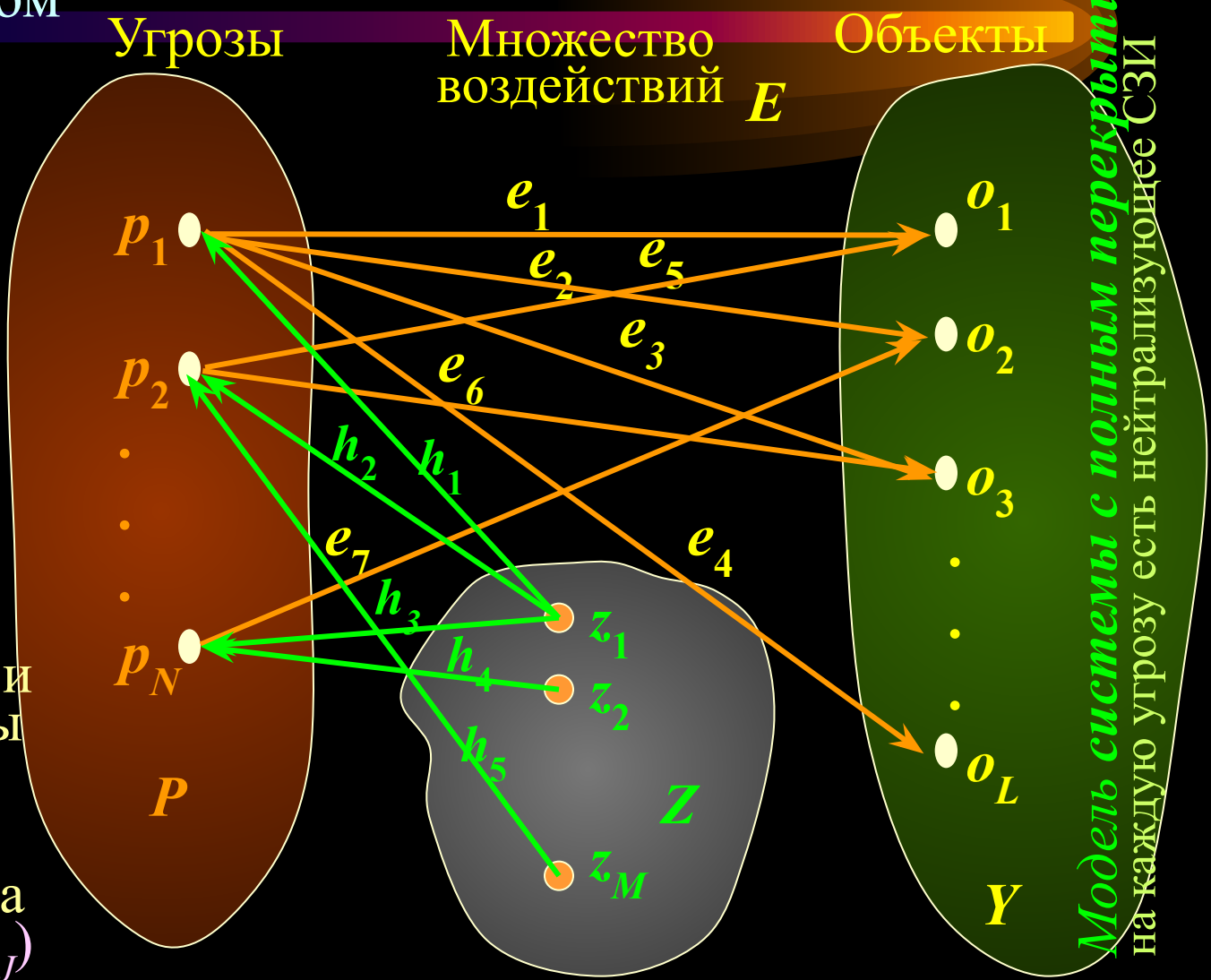
Теоретико-графовые модели комплексной оценки защищенности КС

1. *Модели комплексной оценки защищенности КС*

Специфицируют политику комплексного использования и применения защитных механизмов и анализа защищенности КС на основе теоретико-графового подхода

КС представляется трехдольным графом ***G(P,O,Z,E,H)***:

- множество угроз $P(p_1,p_2,\ldots,p_N)$
- множество объектов защиты $O(o_1,o_2,\ldots,o_L)$
- множество воздействий угроз на объекты $E(e_1,e_2,\ldots,e_K)$
- множество средств и механизмов защиты $Z(z_1,z_2,\ldots,z_M)$
- множество воздействий СЗИ на угрозы $H(h_1,h_2,\ldots,z_J)$



1. *Модели комплексной оценки защищенности КС*

•Каждое ребро графа ***G(P,O,Z,E,H)*** специфицирует воздействие конкретной угрозы на конкретный объект

•От каждой угрозы м.б. несколько воздействий на различные объекты и каждый объект м.б. подвергнут нескольким угрозам (связь "многие-ко-многим")

•Граф ***G(P,O,Z,E,H)*** взвешенный.

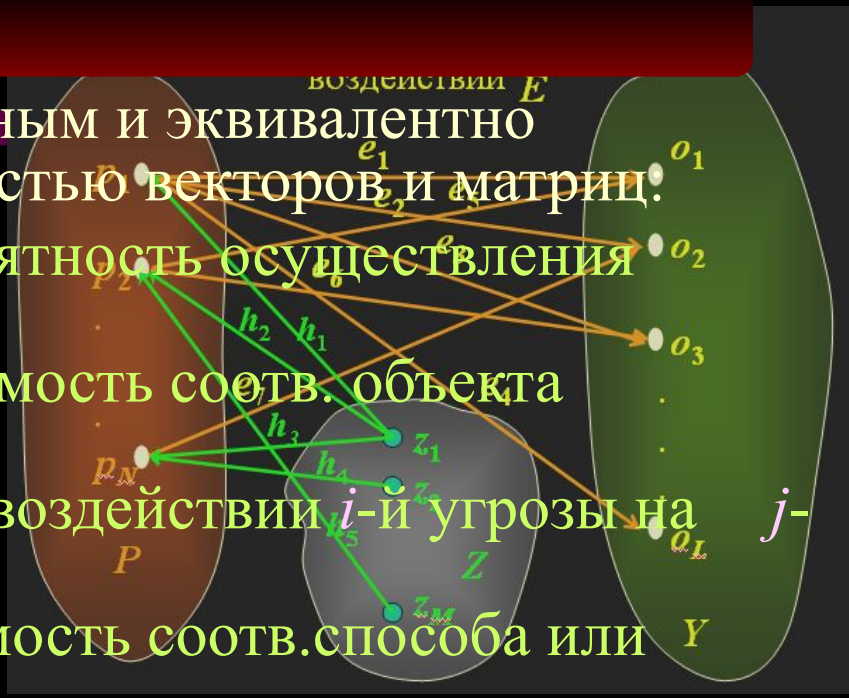
Веса вершин и ребер м. определять:
- величину ущерба от реализации угроз
- или вероятность осуществления угроз

Выбор защитных механизмов осуществляется так, чтобы:
- редуцируя граф, устранить наиболее опасные угрозы
- или изменить веса e_i с тем, чтобы минимизировать поток угроз на основе тех или иных критериев

1. *Модели комплексной оценки защищенности КС*

Области применения теоретико-графовых моделей

Технико-экономическое обоснование систем обеспечения безопасности



Граф ***G(P,O,Z,E,H)*** является взвешенным и эквивалентно представляется следующей совокупностью векторов и матриц:

вектор $\boldsymbol{P}(p_1, p_2, \ldots p_N)$, где p_i – вероятность осуществления соотв.угрозы;

вектор $\boldsymbol{O}(o_1, o_2, \ldots o_L)$, где o_i – стоимость соотв. объекта защиты;

NxL матрица $\boldsymbol{E}\{e_{i,j}\}$, где $e_{i,j}$ =1 при воздействии i-й угрозы на j-й объект, и = 0 в противном случае;

вектор $\boldsymbol{Z}(z_1, z_2, \ldots z_M)$, где z_i – стоимость соотв.способа или средства защиты;

NxM матрица $\boldsymbol{H}\{h_{i,j}\}$, где $h_{i,j}$ – вероятность устранения (или степень снижения ущерба) i-й угрозы от применения j-го средства защиты

Ущерб безопасности без использования СЗИ

Ущерб безопасности при использования СЗИ

Тактико-техническое обоснование систем обеспечения безопасности

Вероятность реализации угроз без СЗИ

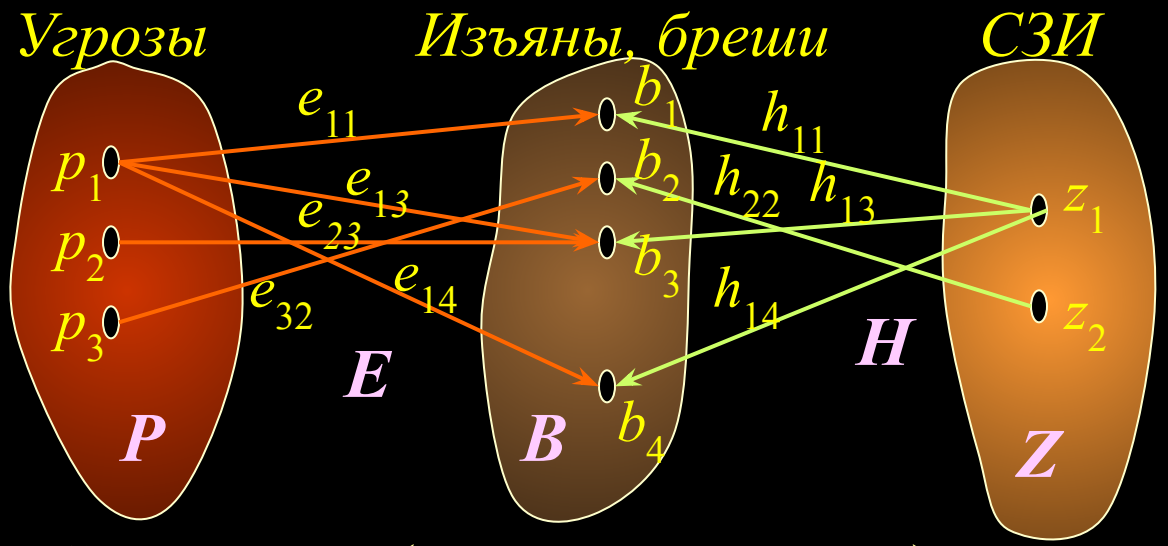
Вероятность преодоления СЗИ

$$M$$

Другие задачи

Система – взвешенный трехдольный граф

G(P,B,Z,E,H)



E – матрица вероятностей осуществления угроз по брешам в системе безопасности

H – матрица вероятностей нейтрализации (степени устранения) с помощью СЗИ брешей или изъянов в системе безопасности

Оценка рисков нарушения ИБ

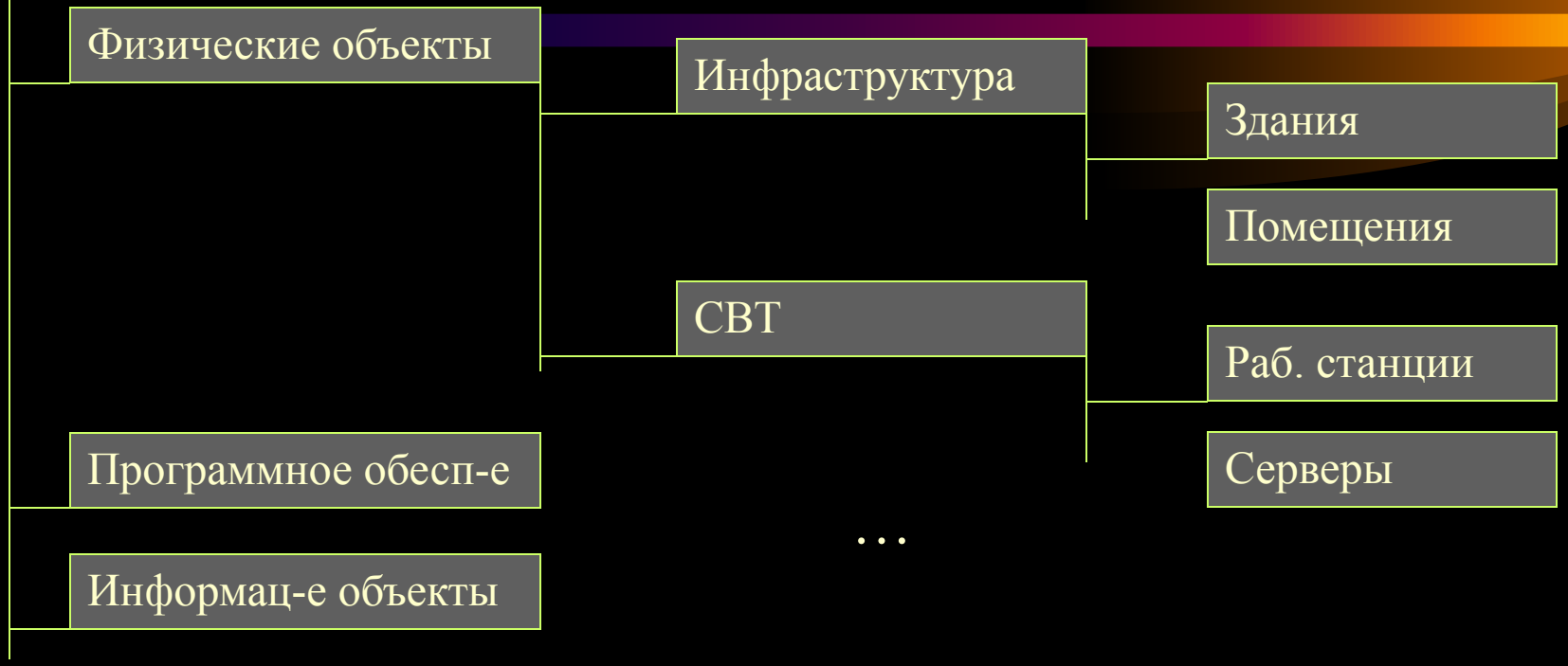
4

Этапы:

1. **Идентификация и оценка ценности объектов защиты**
2. **Формирование перечня угроз и оценка их опасностей (вероятностей)**
3. **Формирование перечня СЗИ – базового уровня защиты с учетом имеющихся нормативных требований**
4. **Вычисление ущерба с учетом применения СЗИ и оценка остаточного риска, как правило, в ранговой шкале:**
   - **остаточный риск незначительный**
   - **остаточный риск приемлемый**
   - **остаточный риск высокий**
   - **остаточный риск неприемлемый**
5. **Формирование дополнительных мер защиты и СЗИ для достижения приемлемого риска**

1.Идентификация и оценка ценности объектов защиты

1.1.Формирование ***полного перечня объектов защиты***- на основе видового дерева

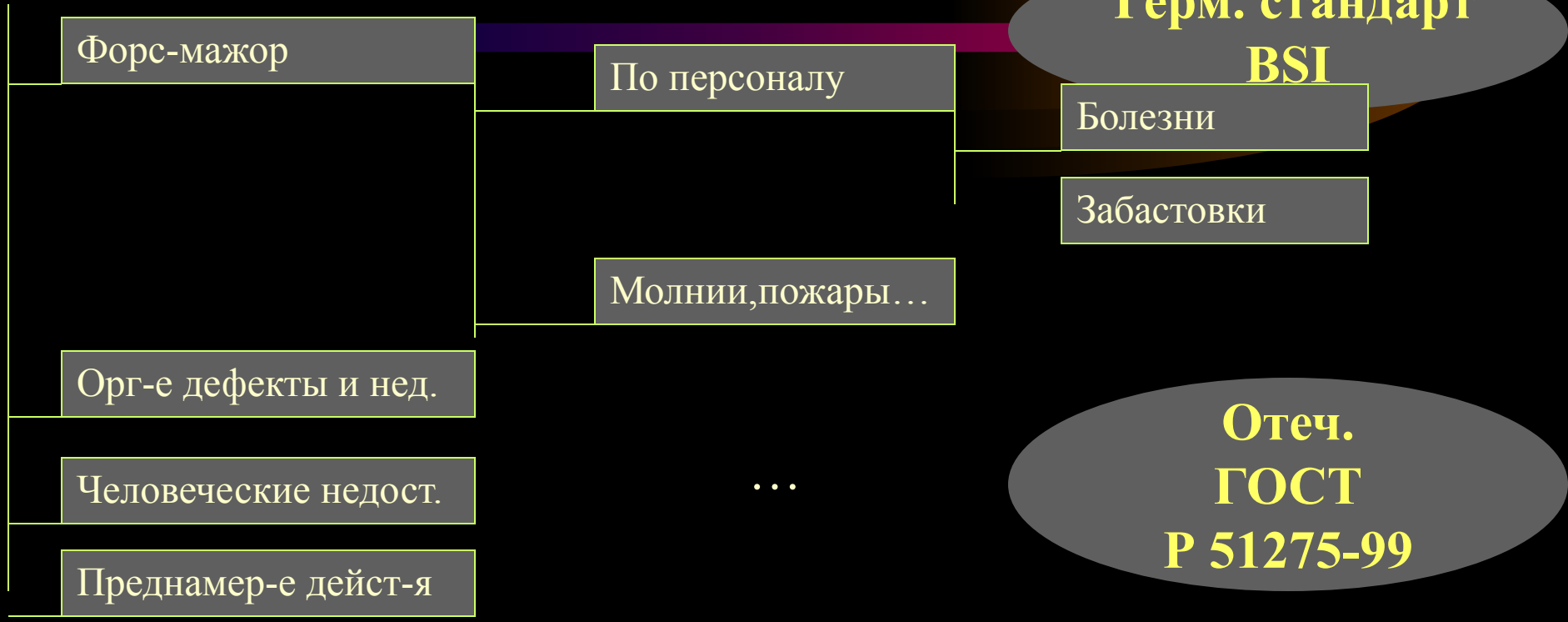


1.2.Определение ценности объектов защиты

в большинстве методик на основе материальной стоимости и ущерба от их разрушения, НСД и т.д.

2.Идентификация угроз и оценка их вероятности

2.1. **Формирование перечня угроз и оценка их опасностей –** также на основе видового дерева



2.2.Определение опасности или вероятностей угроз

в большинстве методик на основе экспертных оценок и анализа имеющейся статистики

3. Формирование перечня и системы СЗИ

3.1. На основе стандартов и РД по защищенности КС

7

- Орган-нно-режимные
- Физической защиты
- Технической защиты
- Аппаратно-прогр-е
  - Подсистема упр-я доступом
    - Идент-я,аутентификация
    - Упр-е потоками
    - . . .
  - Подсистема аудита
    - Регистрация и учет соб-й
    - Регистрация и учет нос-й
    - Системы активн. аудита
    - Сканеры уязвимостей
    - . . .
  - Криптографич. подсистема
  - Подсист. обесп. целостности
    - Системного ПО
    - . . .

Стандарты комплексной оценки защищенности КС

В развитие методологии данного подхода в 80-х годах за рубежом были разработаны подходы к комплексной оценки защищенности КС, закрепленные в соответствующих национальных стандартах:

- британском стандарте BS 7799 (ISO 17799) – Великобритания;
- ведомственном стандарте NASA США "Безопасность информационных технологий" (http://esdis.dsfo.nasa.gov);
- германском стандарте "BSI" (http://www.bsi.bund.de/.

CASE-средства комплексной оценки защищенности

- COBRA, разработчик C&A Systems Security Ltd (http://www.securityauditor.net);
- RiskPAC, разработчик CSCI (http://www.csciweb.com);
- CRAMM, разработчик Logica (Великобритания);
- MARION, разработчик CLUSIF (Франция);
- RiskWatch (http://www.riskwatch.com);
- АванГард (Россия)
- Гриф (Россия)

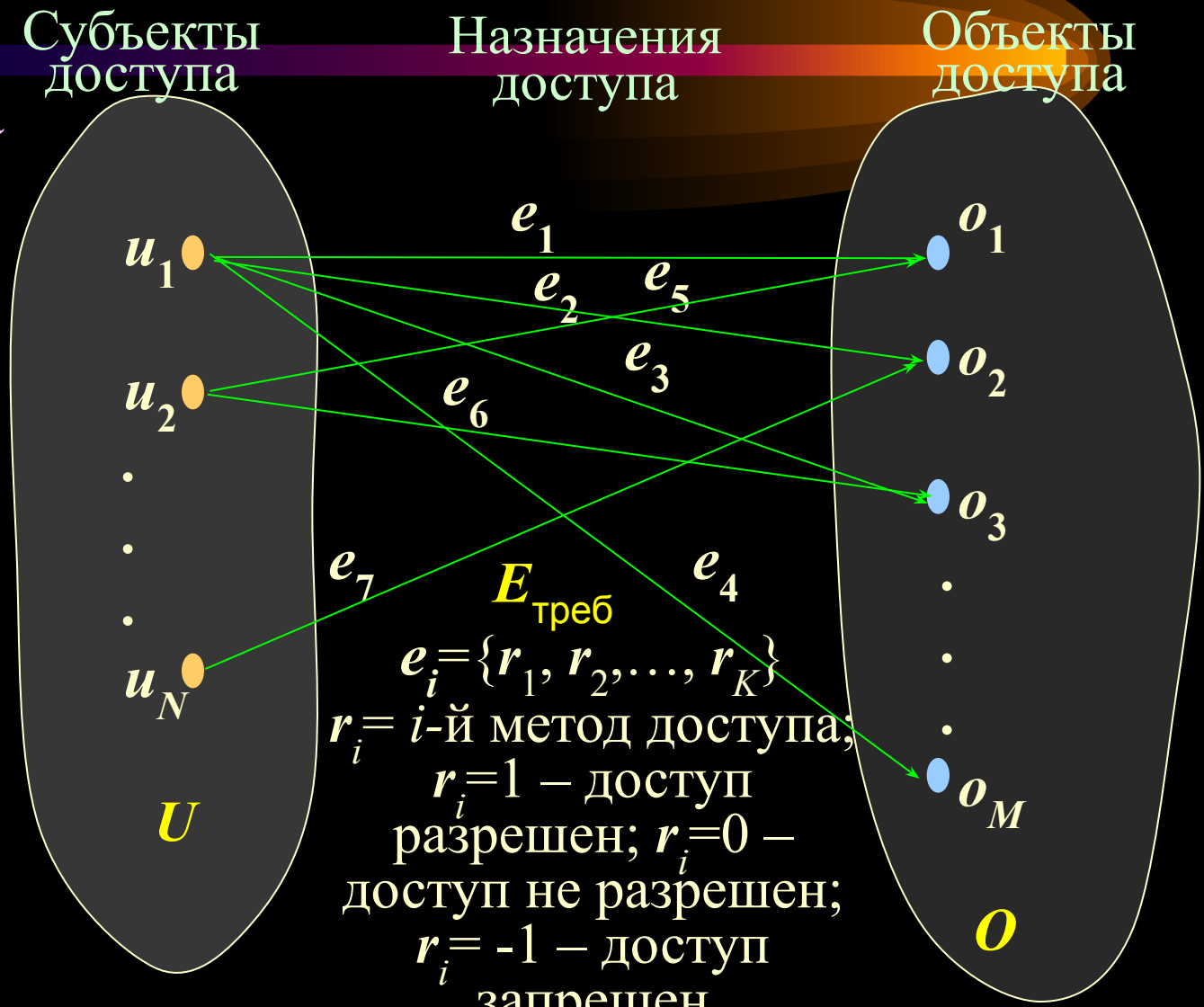
Тема 3. Методы анализа и оценки защищенности компьютерных систем

Лекция 3.3. Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

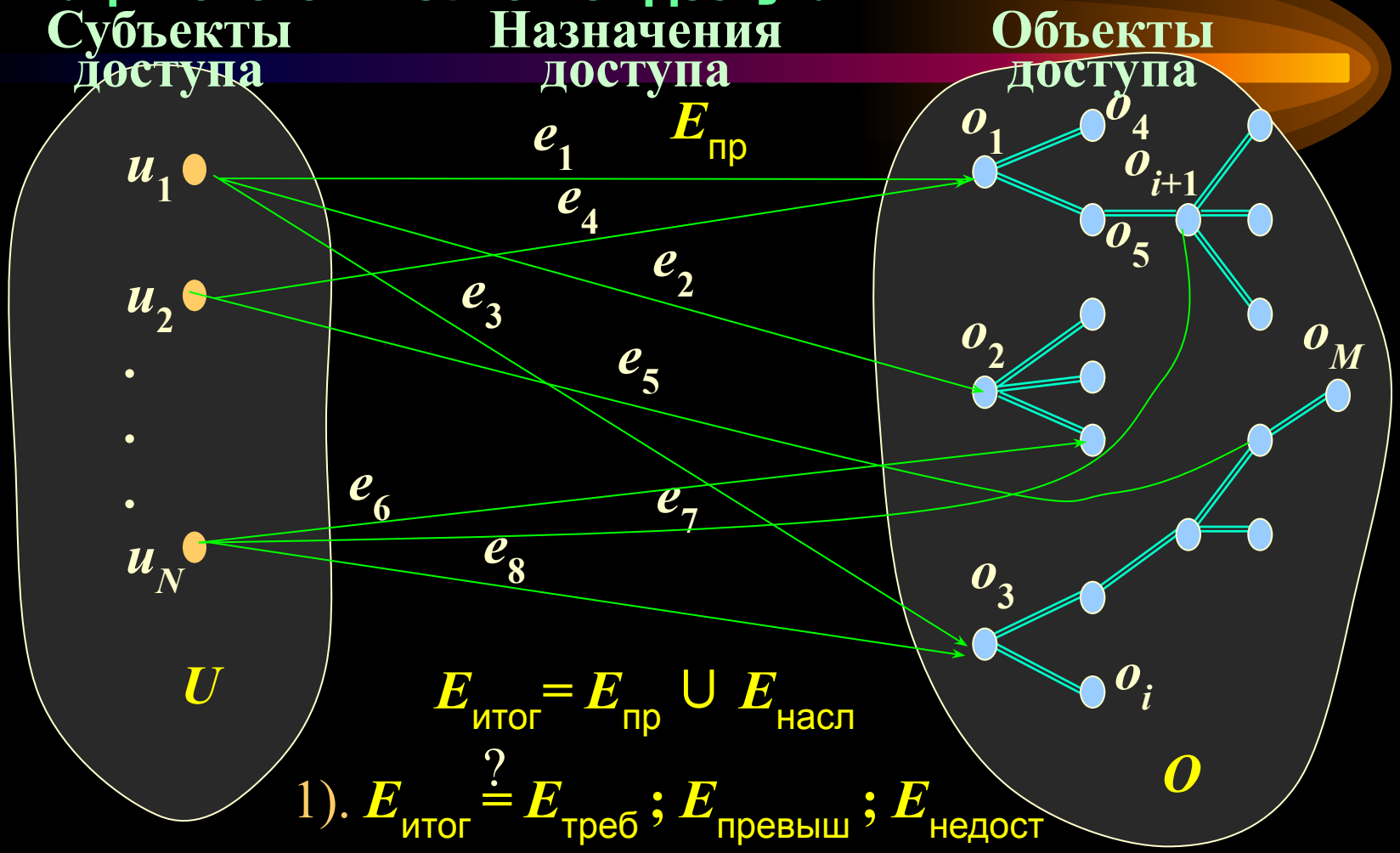
Двудольный граф требуемых назначений доступа $\Gamma(U,O,E)$

- Множество вершин U одной доли графа — субъекты доступа
- Множество вершин O другой доли графа — объекты доступа
- Множество ребер (дуг) $E_{треб}$ — требуемые назначения доступа субъектов к объектам



1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Граф назначений доступа $\Gamma(U,O,E)$ при иерархической организации системы объектов доступа



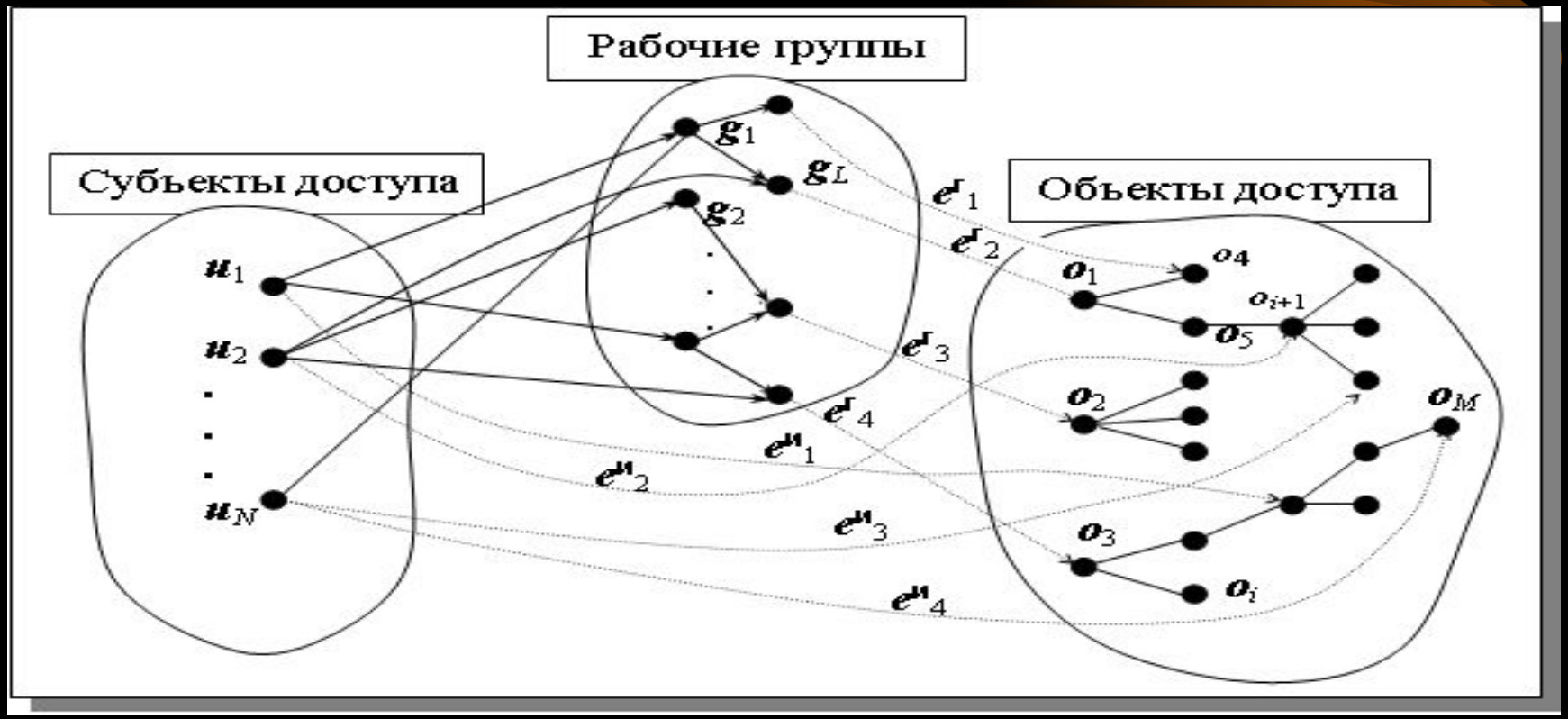
$$E_{итог} = E_{пр} \cup E_{насл}$$

1). $E_{итог} \stackrel{?}{=} E_{треб}$; $E_{превыш}$; $E_{недост}$

2). **Вариативность** наделения субъектов доступа $E_{треб}$ за счет различного сочетания $E_{пр}$ и $E_{насл}$

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Граф индивидуально-групповых назначений доступа $\Gamma(U,G,O,E)$ при иерархической организации системы объектов доступа



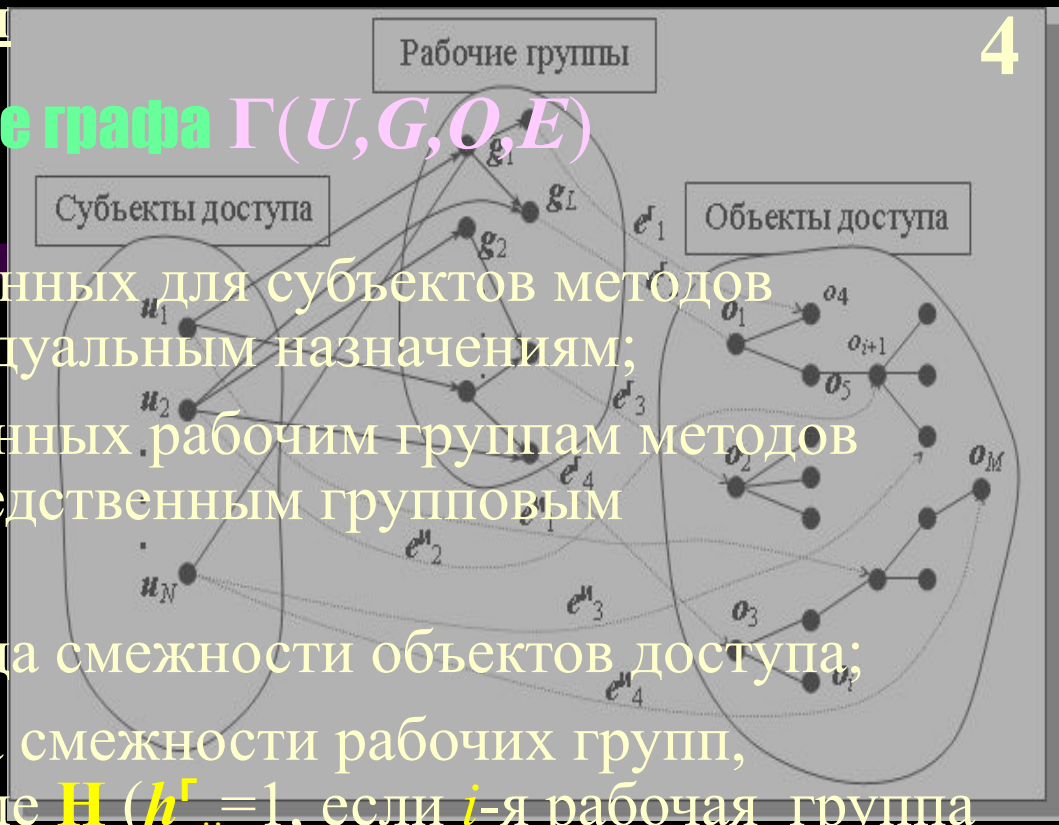
$$E_{итог} = E^{и} \cup E^{г} = (E^{и}_{пр} \cup E^{и}_{насл}) \cup ((E^{г}_{пр} \cup E^{гг}) \cup E^{г}_{насл})$$

1). $E_{итог} \stackrel{?}{=} E_{треб}$; $E_{превыш}$; $E_{недост}$

2). Дополнительная **вариативность** наделения субъектов доступа $E_{треб}$ за счет различного сочетания $E^{и}$ и $E^{г}$

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Матричное представление графа $\Gamma(U,G,O,E)$



$R^и$ – (NxMxK)-массив разрешенных для субъектов методов доступа к объектам по индивидуальным назначениям;

$R^г$ – (LxMxK)-массив разрешенных рабочим группам методов доступа к объектам по непосредственным групповым назначениям;

H – квадратная (MxM) матрица смежности объектов доступа;

$H^г$ – квадратная (LxL) матрица смежности рабочих групп, аналогичная по смыслу матрице **H** ($h^г_{ij}$=1, если i-я рабочая группа содержит j-ю рабочую групп, $h^г_{ij}$=0, если не содержит);

W – прямоугольная (NxL) матрица вхождения пользователей в рабочие группы (w_{ij}=1, если i-й пользователь входит в состав j-й рабочей группы; w_{ij}=0, в противном случае)

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Сочетание прав доступа по прямым назначениям и прав доступа по иерархическому наследованию

- политика простой суперпозиции (дизъюнкции) прав по прямым и наследственным назначениям:

$$\boldsymbol{R}_{ij} = \{\boldsymbol{r}_{ij1|\text{пр}} \cup \boldsymbol{r}_{ij1|\text{насл}}, \boldsymbol{r}_{ij2|\text{пр}} \cup \boldsymbol{r}_{ij2|\text{насл}}, \ldots, \boldsymbol{r}_{ijK|\text{пр}} \cup \boldsymbol{r}_{ijK|\text{насл}}\}$$

- политика приоритетной суперпозиции (дизъюнкции) прав по прямым и наследственным назначениям с приоритетом прямых назначений

$$\boldsymbol{R}_{ij} = \{\boldsymbol{r}_{ij1|\text{пр}} \vee \boldsymbol{r}_{ij1|\text{насл}}, \boldsymbol{r}_{ij2|\text{пр}} \vee \boldsymbol{r}_{ij2|\text{насл}}, \ldots, \boldsymbol{r}_{ijK|\text{пр}} \vee \boldsymbol{r}_{ijK|\text{насл}}\}$$

$r_{ijk\|\text{насл}}$	$r_{ijk\|\text{пр}}$	$r_{ijk\|\text{насл}} \vee r_{ijk\|\text{пр}}$
1	0	1
1	1	1
1	-1	-1
0	0	0
0	1	1
0	-1	-1
-1	0	-1
-1	1	1
-1	-1	-1

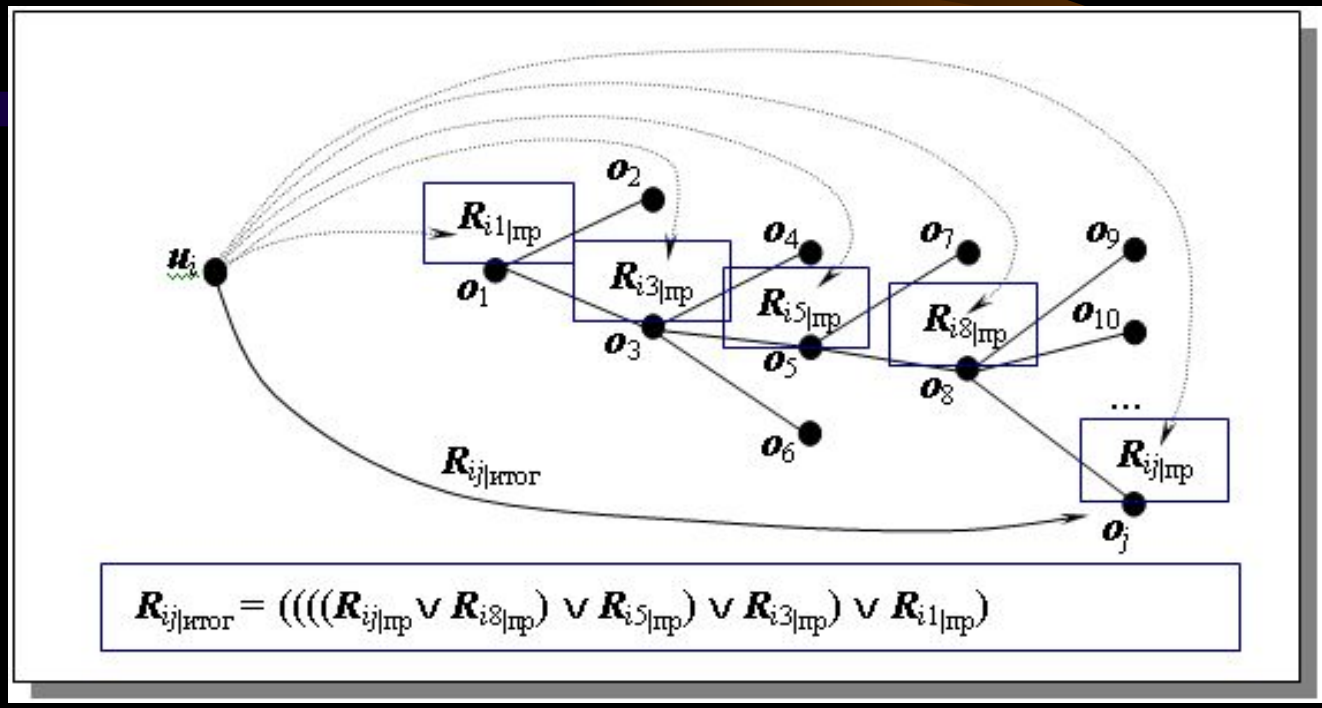
- политика фильтрационной суперпозиции прав доступа к вложенным объектам

$$\boldsymbol{R}_{ij} = \{\boldsymbol{r}_{ij1|\text{пр}} \cup (\boldsymbol{r}_{ij1|\text{насл}} \cdot \boldsymbol{\delta}^{\Phi}_{ij1}), \boldsymbol{r}_{ij2|\text{пр}} \cup (\boldsymbol{r}_{ij2|\text{насл}} \cdot \boldsymbol{\delta}^{\Phi}_{ij2}), \ldots, \boldsymbol{r}_{ijK|\text{пр}} \cup (\boldsymbol{r}_{ijK|\text{насл}} \cdot \boldsymbol{\delta}^{\Phi}_{ijK})\}$$

δ^{Φ}_{ijk}	
1	передача прав на вложенные объекты в j-й объект по k-му методу доступа для i-го пользователя разрешена
0	запрещена

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Определение итоговых прав доступа при приоритетной суперпозиции с учетом структурной вложенности объектов



- по спискам доступа

- через матрицу смежности объектов доступа **H**

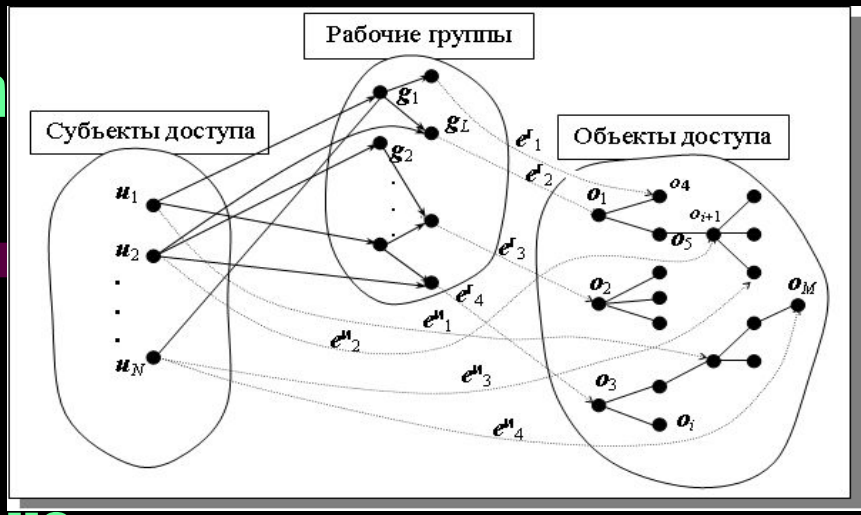
$\mathbf{R}_{\mathbf{k}|итог} = \mathbf{R}_{\mathbf{k}|пр} \otimes (\mathbf{H}^S + \mathbf{I})$, где $\mathbf{H}^S = \mathbf{H} + \mathbf{H}^2 + \ldots + \mathbf{H}^n$,

$\otimes$ - модифицированная операция матричного умножения на основе ассиметричной дизъюнкции:

$(\mathbf{R}_{\mathbf{k}|итог})_{ij} = r_{i1\mathbf{k}}(h^S_{1j\mathbf{k}} + \delta_{1j}) \vee r_{i2\mathbf{k}}(h^S_{2j\mathbf{k}} + \delta_{2j}) \vee \ldots \vee r_{iM\mathbf{k}}(h^S_{Mj\mathbf{k}} + \delta_{Mj})$,

I – единичная матрица; δ_{ij} – символ Кронекера

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам



Определение итоговых прав доступа рабочих групп при приоритетной суперпозиции с учетом структурной вложенности рабочих групп и объектов

$$\mathbf{R}^{\Gamma}_{k|итог}=W\otimes(((\mathbf{H}^{\Gamma S}+I)^{T}\otimes\mathbf{R}^{\Gamma}_{k})\otimes(\mathbf{H}^{S}+I))$$

Определение итоговых индивидуально-групповых прав доступа с приоритетом индивидуальных назначений

$$\mathbf{R}^{И\Gamma}_{k|итог}=\mathbf{R}^{И}_{k|итог}\oplus\mathbf{R}^{\Gamma}_{k|итог}=$$

$$=(\mathbf{R}_{k|пр}\otimes(\mathbf{H}^{S}+I))\oplus(W\otimes(((\mathbf{H}^{\Gamma S}+I)^{T}\otimes\mathbf{R}^{\Gamma}_{k})\otimes(\mathbf{H}^{S}+I)))$$

$r^{И}$	r^{Γ}	$r^{И}\oplus r^{\Gamma}$
1	0	1
1	1	1
1	-1	1
0	0	0
0	1	1
0	-1	-1
-1	0	-1
-1	1	-1
-1	-1	-1

Коэффициент дублирования прав доступа

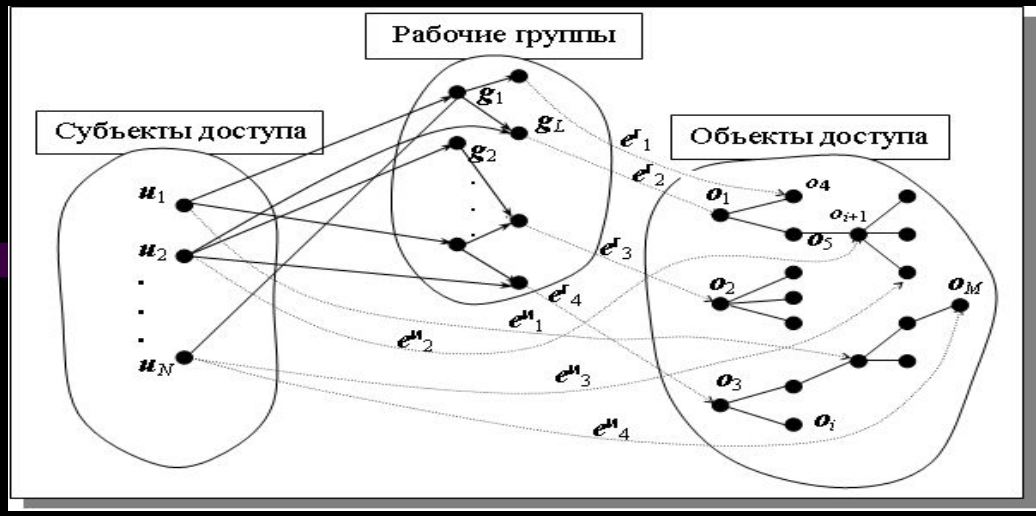
$$K_{дубл}=\sum_{k}\sum_{i}\sum_{j}k_{ijk},$$

$$k^{И}_{ijk}=(\mathbf{R}^{И}_{k|пр}\cdot(\mathbf{H}^{S}+I))_{ij}$$

$$K^{\Gamma}_{k}=W\cdot(((\mathbf{H}^{\Gamma S}+I)^{T}\cdot\mathbf{R}^{\Gamma}_{k})\cdot(\mathbf{H}^{S}+I))$$

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Количественные параметры превышения и недостатка прав доступа



$$R^{+}_{\Delta} = R^{иг}_{итог} \ominus^{+} R_{треб}$$

$$R^{-}_{\Delta} = R^{иг}_{итог} \ominus^{-} R_{треб}$$

$r^{иг}_{итог}$	$r_{треб}$	$r^{иг}_{итог} \ominus^{+} r_{треб}$	$r^{иг}_{итог} \ominus^{-} r_{треб}$
1	0	1	0
1	1	0	0
1	-1	1	0
0	0	0	0
0	1	0	1
0	-1	0	0
-1	0	0	0
-1	1	0	1
-1	-1	0	0

$$К_{превыш} =$$

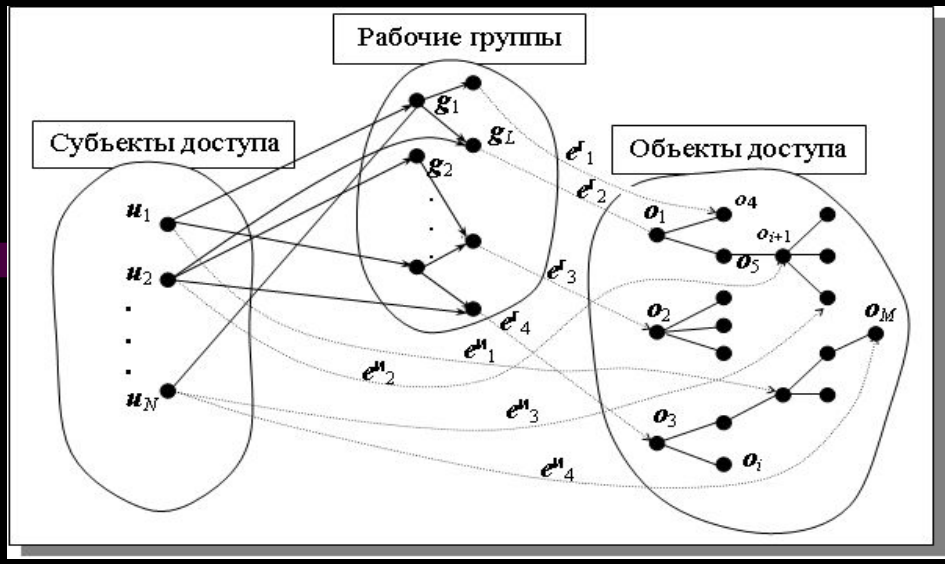
$$k_{превыш i} =$$

$$k_{превыш ij} =$$

$$К_{недост} =$$

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Количественные характеристики системы рабочих групп



$$\Omega^{\Gamma} = \begin{pmatrix} \sigma^{\Gamma}_{11} & \sigma^{\Gamma}_{12} & \dots & \sigma^{\Gamma}_{1L} \end{pmatrix}$$

$$\sigma^{\Gamma}_{ij} =$$

Количественные характеристики близости пользователей по потребностям в доступе

$$\sigma^{U}_{ij} =$$

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Пример количественного анализа системы индивидуально-группового доступа

Главный бухгалтер (u_1) – общее руководство подразделением, планирование, контроль деятельности.

Старший бухгалтер (u_2) – ведение обобщенного (сводного) финансово-экономического учета и анализа, замещение в случае необходимости гл.бухгалтера (отпуск, болезнь, командировка).

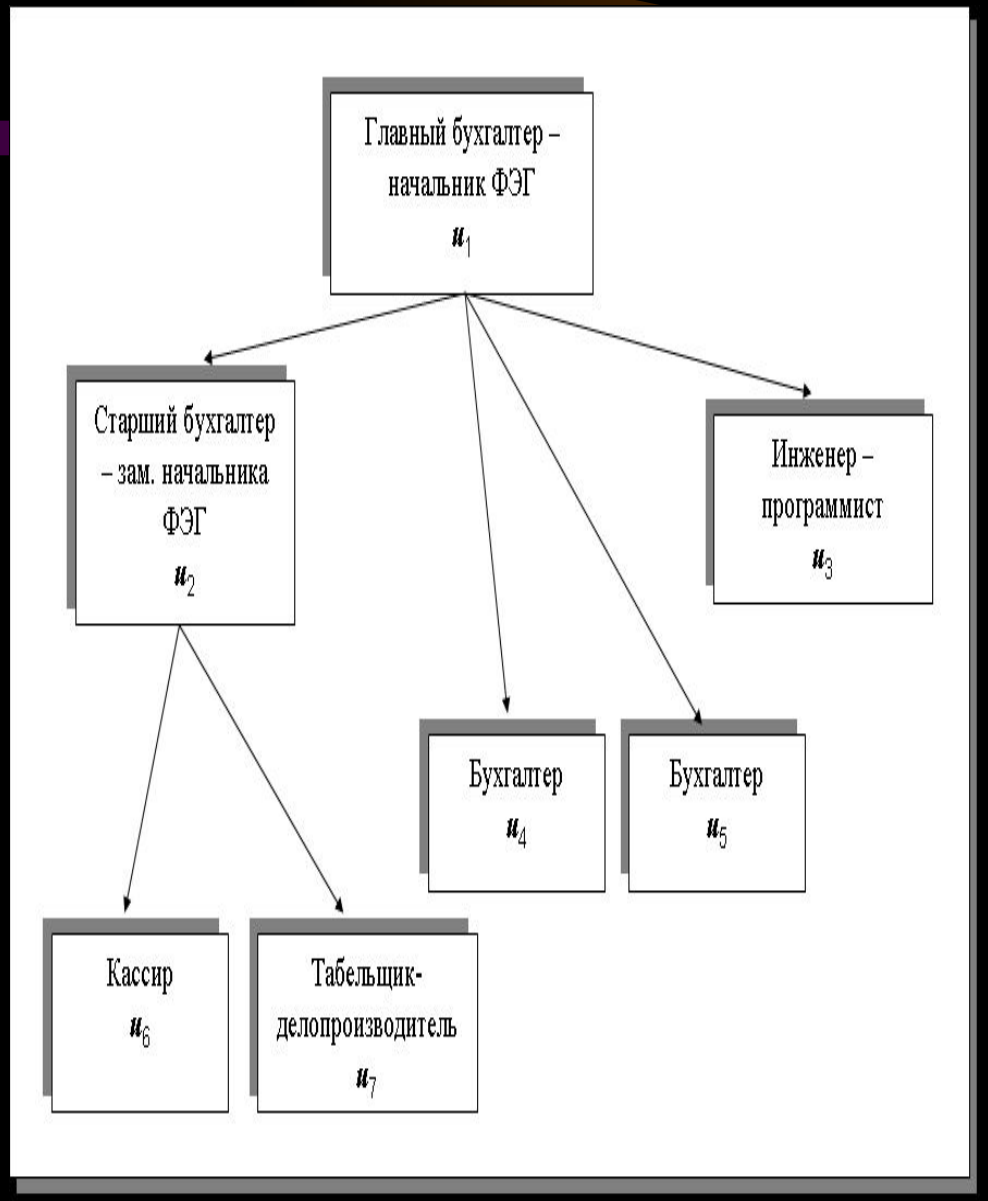
Бухгалтер (первый) (u_4) – бухгалтер-экономист, подменяет ст. бухгалтера.

Бухгалтер (второй) (u_5) – бухгалтер по заработной плате, подменяет (первого) бухгалтера и кассира.

Кассир (u_6) – проводки по кассе, выдача зарплаты, подменяет табельщика-делопроизводителя и (второго) бухгалтера.

Табельщик-делопроизводитель (u_7) – ведение Табеля рабочего времени сотрудников организации, а также ведение делопроизводства подразделения.

Инженер-программист (u_3) – организация работы локальной информационной сети подразделения



1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Пример количественного анализа системы индивидуально-группового доступа

Система рабочих групп

Группа "*Администраторы*" (g_1) – включает $\{u_1, u_3\}$.

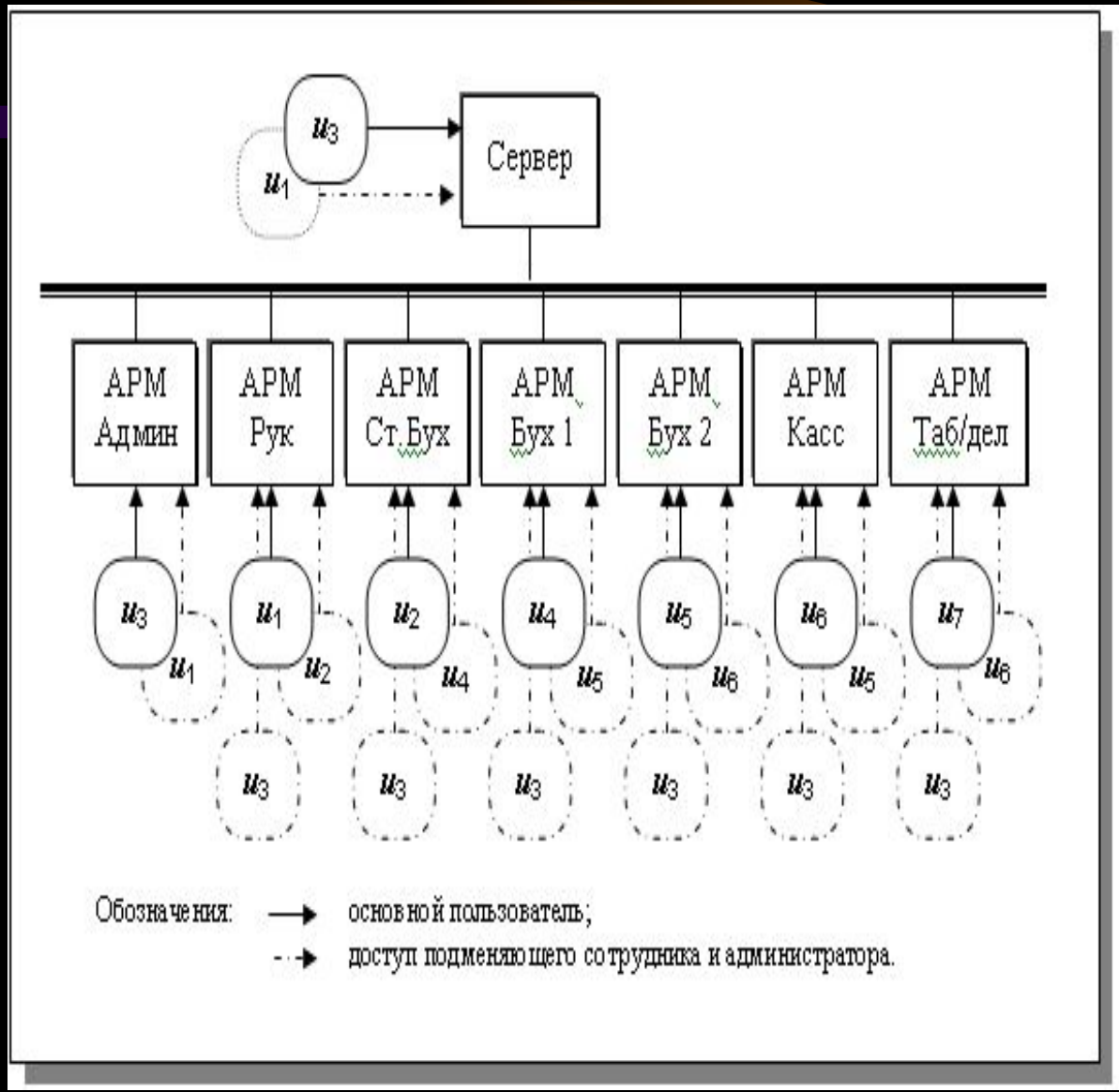
Группа "*Бухгалтеры*" (g_2) – включает $\{u_1, u_2, u_4, u_5, u_6\}$.

Группа "*Исполнители документов*" (g_3) , включает $\{u_1, u_2, u_3, u_4, u_5, u_6, u_7\}$.

Группа "*Users*" (g_4) – включает $\{u_1, u_2, u_3, u_4, u_5, u_6, u_7, g_2, g_3\}$.

Права доступа

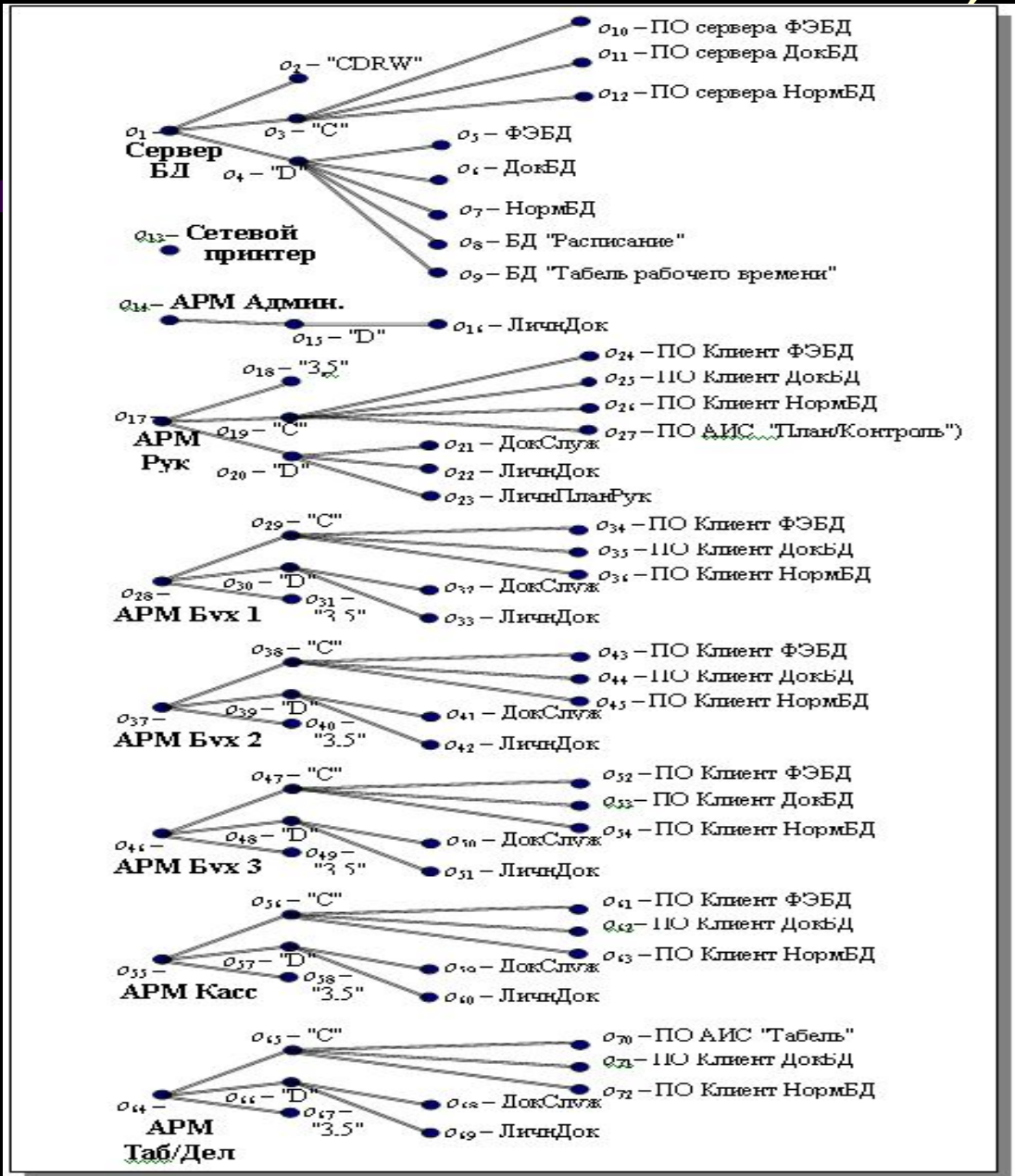
определяются разрешениями по четырем методам доступа – r_1 (чтение), r_2 (чтение/запись), r_3 (выполнение) и r_4 (полный доступ). Функция $f_{корр}$ обеспечивает в векторах обнуление r_1, если $r_2=1$; обнуление r_1, r_2, r_3, если $r_4=1$; требует $r_1=1$ в $_{|насл}$, если $r_3=1$.



1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Пример количественного анализа системы индивидуально-группового доступа

- Клиент-серверная финансово-экономическая АИС (ФЭБД)
- Клиент-серверная АИС делопроизводства/докум ентооборота (ДокБД)
- Клиент-серверная информационно-правовая система (НормБД)
- Локальная АИС "Табель рабочего времени" (БД "Табель")
- Локальная АИС "Планирование и контроль" (БД "Расписание")



1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Пример количественного анализа системы индивидуально-группового доступа

Групповые назначения

g_1 – полный доступ к объектам сети с запретом доступа к личным папкам сотрудников.

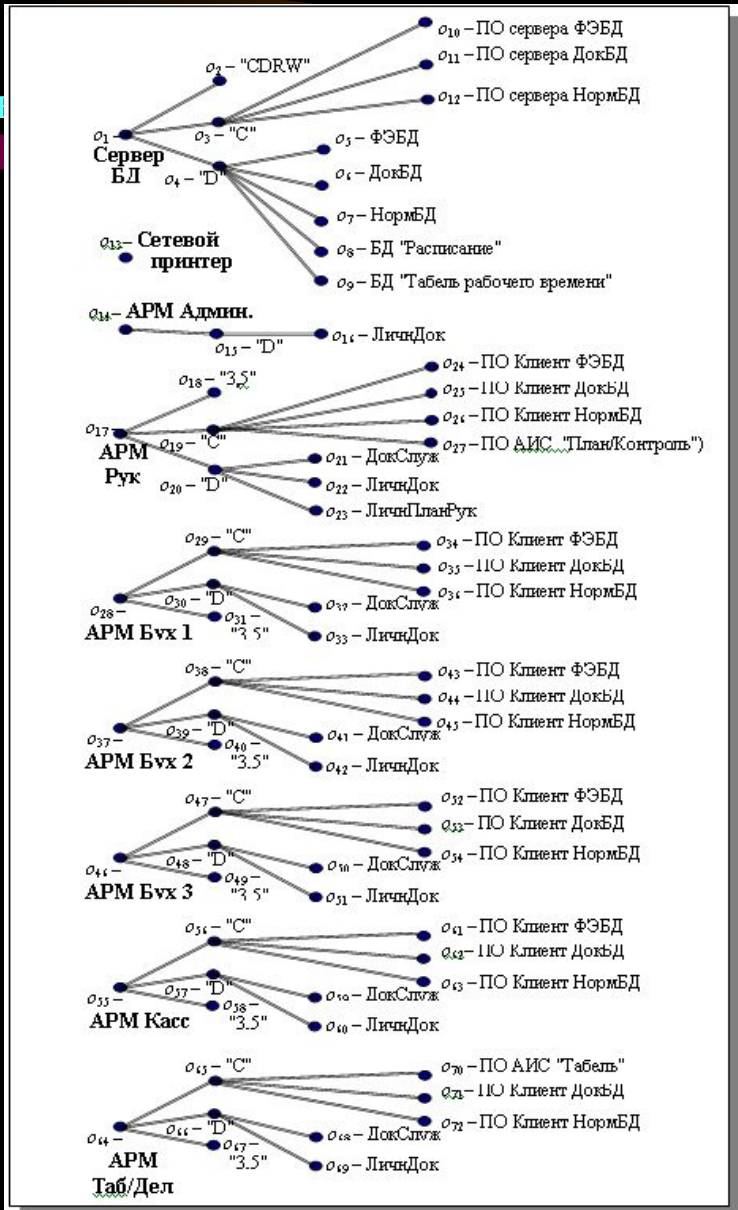
g_2 – работа в АИС "ФЭБД", доступ к бухгалтерским АРМ (для подмены работников или выполнения своих функций на других АРМ, в случае выхода из строя своего), запрет доступа к личным папкам на "не своем" АРМ, запрет доступа к CDRW на сервере.

g_3 – работа в АИС "ДокБД", доступ "чтение/запись" к сетевому принтеру, запрет доступа к CDRW на сервере.

g_4 – работа в АИС "НормБД", доступ "чтение" к расписанию на сервере, запрет доступа к сетевому принтеру, запрет доступа к CDRW на сервере

Индивидуальные назначения

права на полный доступ пользователей к "своим" АРМ, доступ к АРМ подменяемых сотрудников с запретом доступа к их личным папкам и дисководам "3,5", права выполнения локальных АИС на АРМ замещаемых сотрудников (работа в АИС "Планирование и контроль" на АРМ руководителя для u_2, работа в АИС "Табель рабочего времени" для u_6 на АРМ табельщика-делопроизводителя).



1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Пример количественного анализа системы индивидуально-группового доступа

Расчет величин $K_{дубл}$, $K_{превыщ}$ и $\sigma^{г}_{jj}$ по пяти вариантам системы индивидуально-группового доступа:

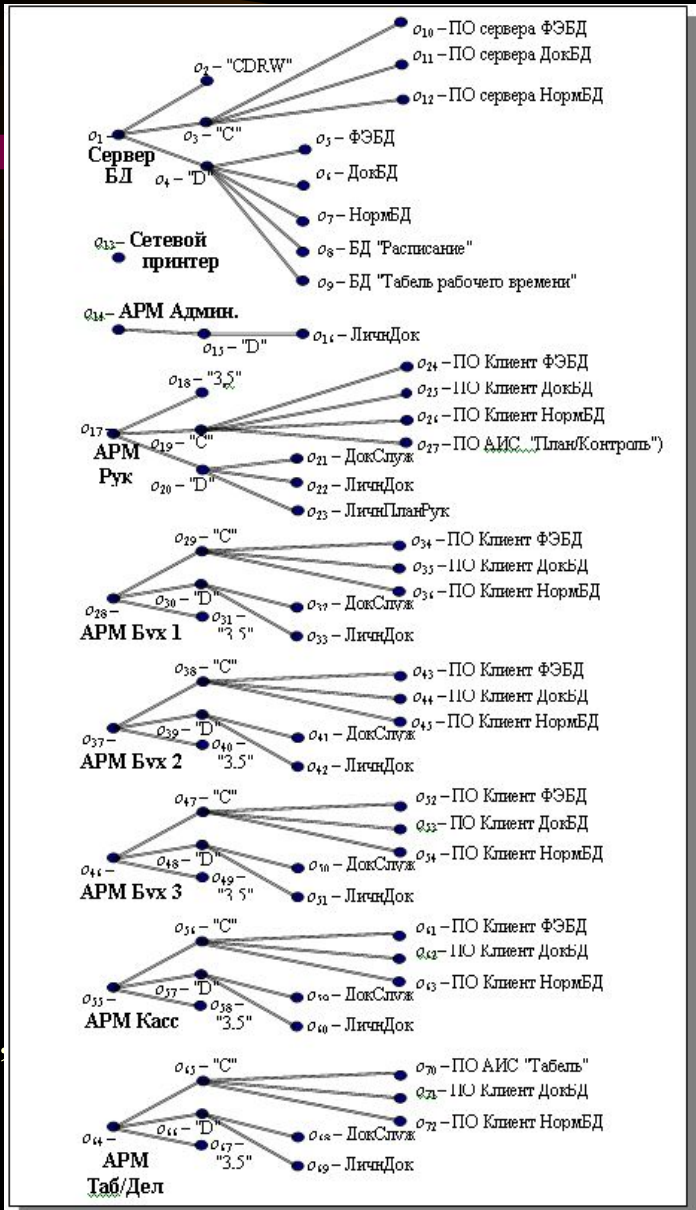
1-й вариант – исходный;

2-й вариант – исключение пользователя u_3 (инженера-программиста) из групп g_3 и g_4 (в силу того, что у группы g_1, в которую он входит, имеются полные права доступа ко всей системе за исключением доступа к личным папкам пользователей);

3-й вариант – исключение из группы g_4 групп g_2 и g_3 и, кроме того, добавление группе g_3 прав доступа к АИС НормБД;

4-й вариант – исключение из группы g_4 всех пользователей и других групп (группа g_4 "гостевая" для временной регистрации и работы в сети сторонних пользователей), и аналогично добавление группе g_3 прав доступа к АИС НормБД;

5-й вариант – аналогичный 4-му с дополнительным исключением по индивидуальным назначениям разрешений на доступ к АРМ подменяемых работников, так как необходимый доступ имеется в разрешениях группы g_2 (кроме прав доступа к локальным АИС)



1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Пример количественного анализа системы индивидуально-группового доступа

	Варианты					
	1	2	3	4	5	6
Избыточность (дублирование) прав доступа						
$K_{дубл}$	0,42619	0,40516	0,32817	0,28928	0,26627	0,21865
$K_{дубл}{}_{u_1}$	0,56388	0,56388	0,45833	0,41944	0,41667	0,22778
$K_{дубл}{}_{u_2}$	0,41111	0,41111	0,30556	0,26667	0,26389	0,23611
$K_{дубл}{}_{u_3}$	0,35833	0,21111	0,30556	0,26667	0,21111	0,21111
$K_{дубл}{}_{u_4}$	0,40278	0,40278	0,29722	0,25833	0,23333	0,20556
$K_{дубл}{}_{u_5}$	0,43611	0,43611	0,33056	0,29167	0,24444	0,21667
$K_{дубл}{}_{u_6}$	0,40278	0,40278	0,29722	0,25833	0,23333	0,20556
$K_{дубл}{}_{u_7}$	0,40833	0,40833	0,30278	0,26389	0,26111	0,22778
Близость групп						
$\sigma^r\ g_1/g_2$	0,56190	0,56190	0,56190	0,56190	0,56190	0,525
$\sigma^r\ g_1/g_3$	0,66548	0,63690	0,66548	0,66270	0,63135	–
$\sigma^r\ g_1/g_4$	0,67103	0,64246	0,67103	0,75675	0,75675	–
$\sigma^r\ g_2/g_3$	0,88532	0,91389	0,88532	0,88254	0,905556	–
$\sigma^r\ g_2/g_4$	0,89087	0,91944	0,89087	0,74802	0,74802	–
$\sigma^r\ g_3/g_4$	0,99444	0,99444	0,99444	0,79722	0,82024	–
Превышение прав доступа						
$K_{превыш}$	0,06597	0,06597	0,06597	0,06597	0,06399	0,06399
$K_{превыш}{}_{u_1}$	0	0	0	0	0	0
$K_{превыш}{}_{u_2}$	0,11111	0,11111	0,11111	0,11111	0,11111	0,11111
$K_{превыш}{}_{u_3}$	0	0	0	0	0	0
$K_{превыш}{}_{u_4}$	0,08333	0,08333	0,08333	0,08333	0,07986	0,07986
$K_{превыш}{}_{u_5}$	0,07292	0,07292	0,07292	0,07292	0,06597	0,06597
$K_{превыш}{}_{u_6}$	0,08333	0,08333	0,08333	0,08333	0,07986	0,07986
$K_{превыш}{}_{u_7}$	0,11111	0,11111	0,11111	0,11111	0,11111	0,11111

$\Omega^u_{треб}$	u_1	u_2	u_3	u_4	u_5	u_6	u_7
u_1	–	–	–	–	–	–	–
u_2	0,6875	–	–	–	–	–	–
u_3	0,9757	0,7049	–	–	–	–	–
u_4	0,6979	0,9063	0,7153	–	–	–	–
u_5	0,6736	0,8507	0,6910	0,9063	–	–	–
u_6	0,6701	0,8576	0,6875	0,8646	0,9028	–	–
u_7	0,7222	0,8993	0,7396	0,8889	0,8646	0,9028	–

1. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам

Пример количественного анализа системы индивидуально-группового доступа