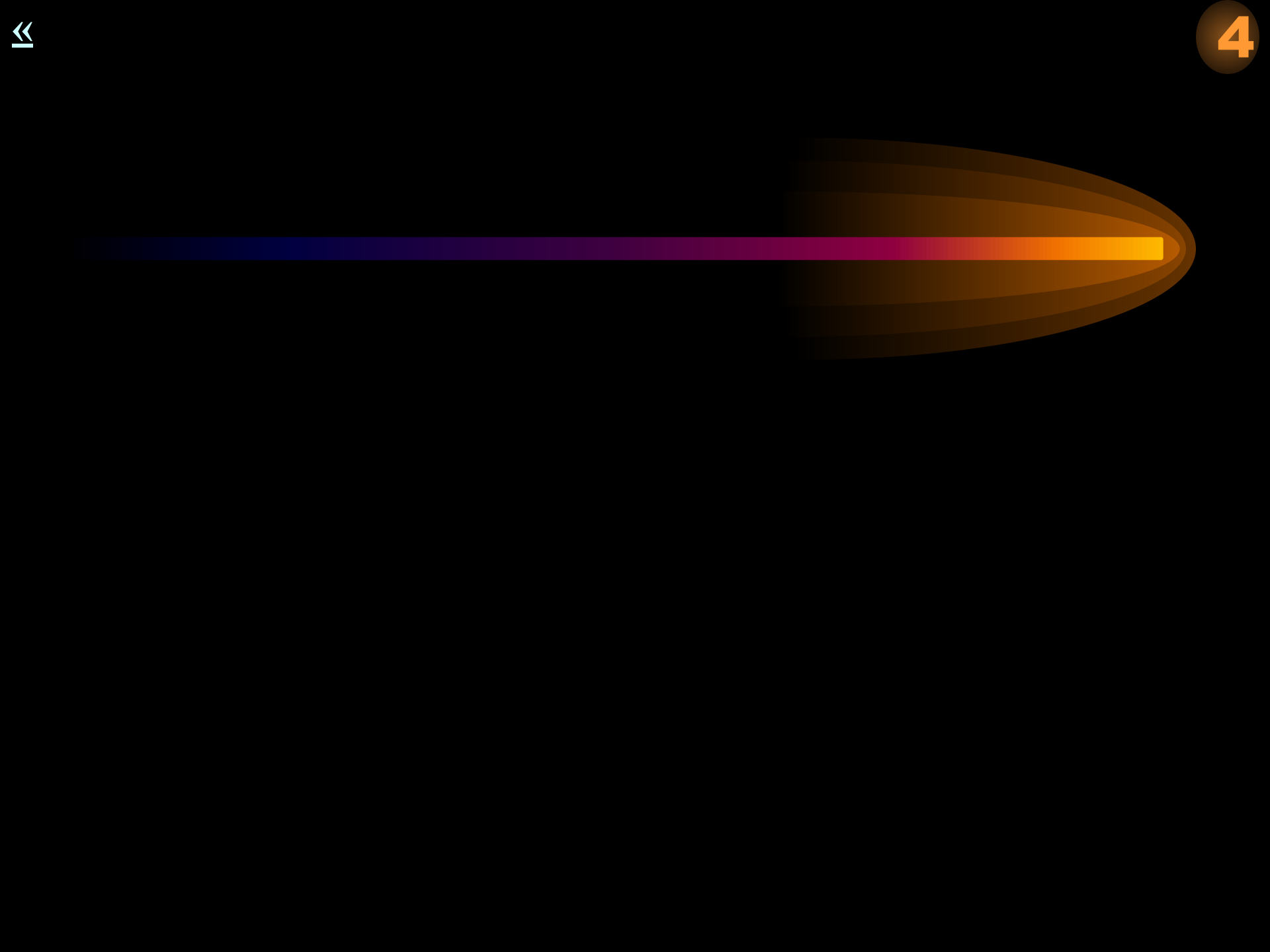
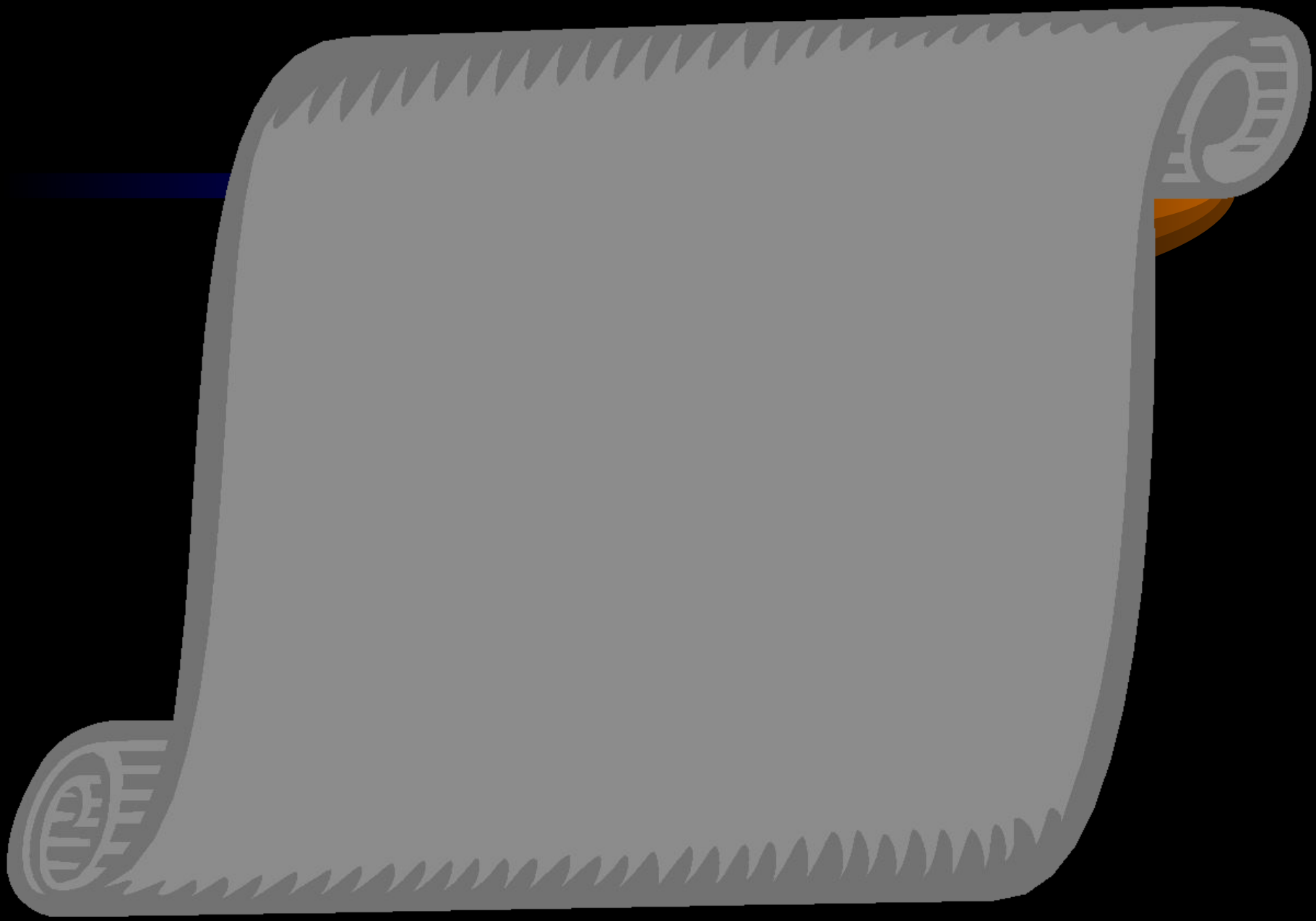
Теоретические основы компьютерной безопасности

Содержание

Содержание



3.



Литература по курсу

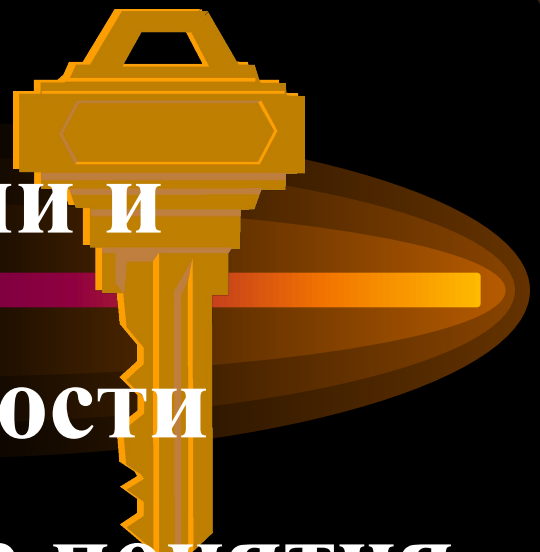
1. **Хоффман Л.** Современные методы защиты информации. М.:Сов. радио, 1980. – 264с.
2. **Грушо А.А.,Тимонина Е.Е.** Теоретические основы защиты информации. М.:Яхтсмен, 1996. - 192с.
3. **Теория и практика обеспечения информационной безопасности** / Под ред. П.Д. **Зегжды**. М.:Яхтсмен, 1996. - 302с
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 компьютерных 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 огромн 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:

Этап	Год	Основные факторы	Содержание
3-й этап	конец 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 "Информационного" законодательства	•Дальн. разв. формальных моделей и технологий защиты информации •Переход на "защищенность" при разработке коммерческих КС: -ОС -СУБД •Появление спец. проблемы КБ – **компьютерных 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

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

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

принимает меры по организации доступа к информации только уполномоченных лиц

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

«Теоретические основы компьютерной безопасности»

Тема 1. Исходные положения теории компьютерной безопасности

Лекция 1.2.

Угрозы безопасности в компьютерных системах

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*

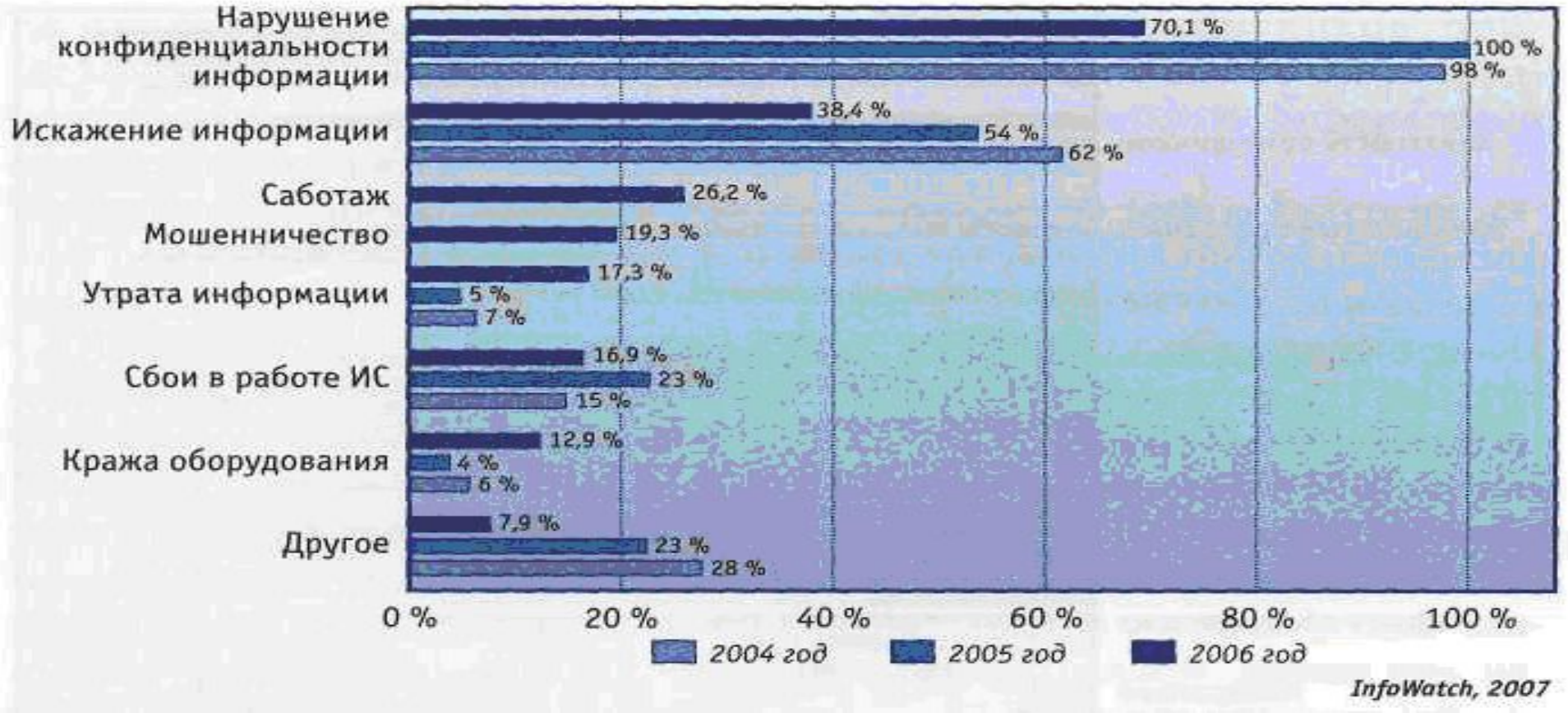
1. Понятие и классификация угроз

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

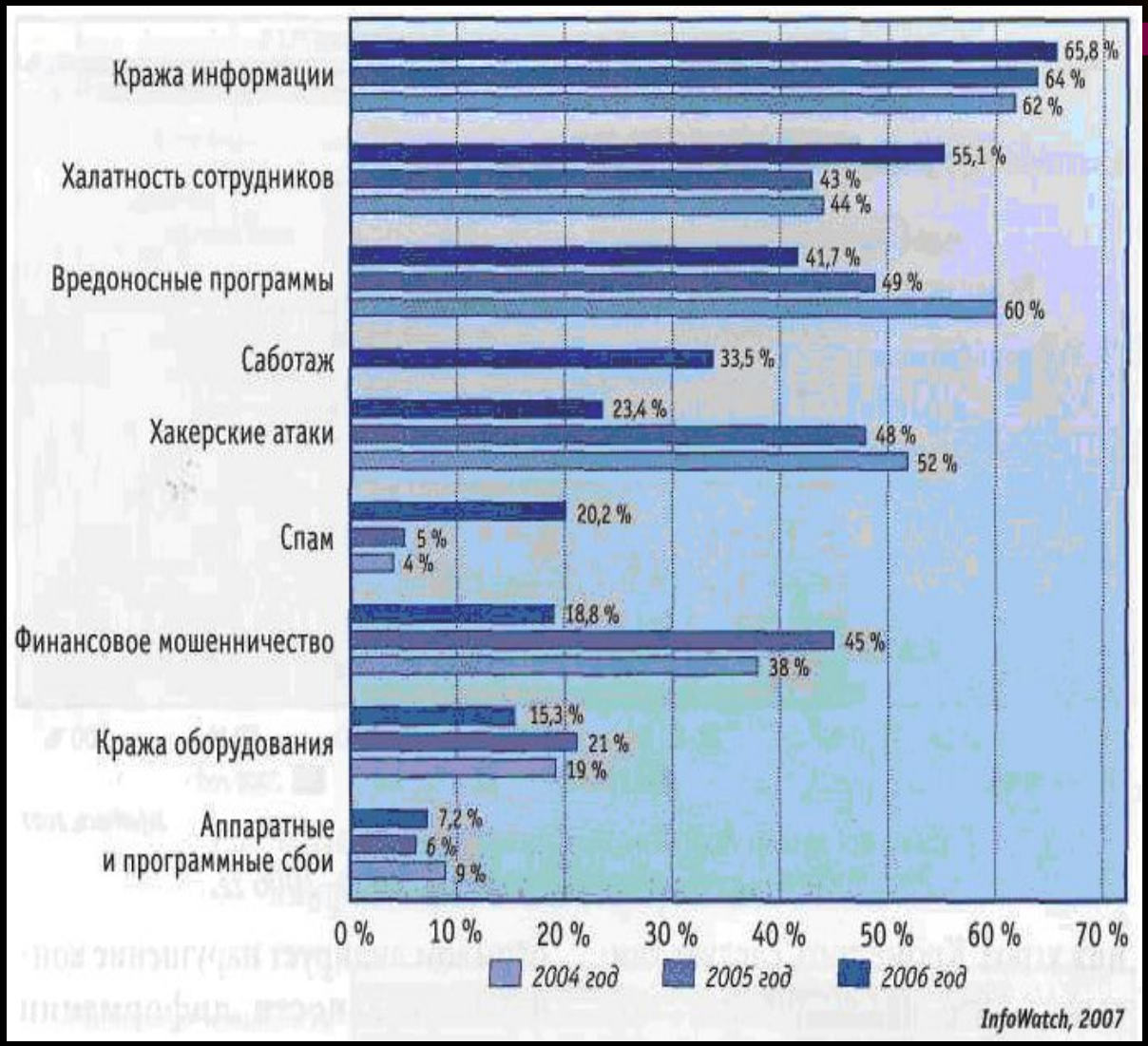
Внутренняя зона КС

Зона контролируемой территории

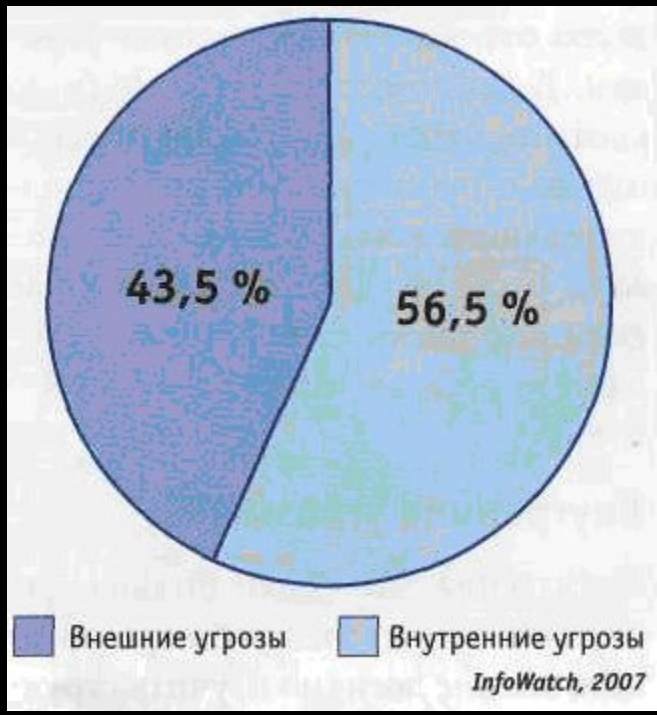
Зона помещений КС

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

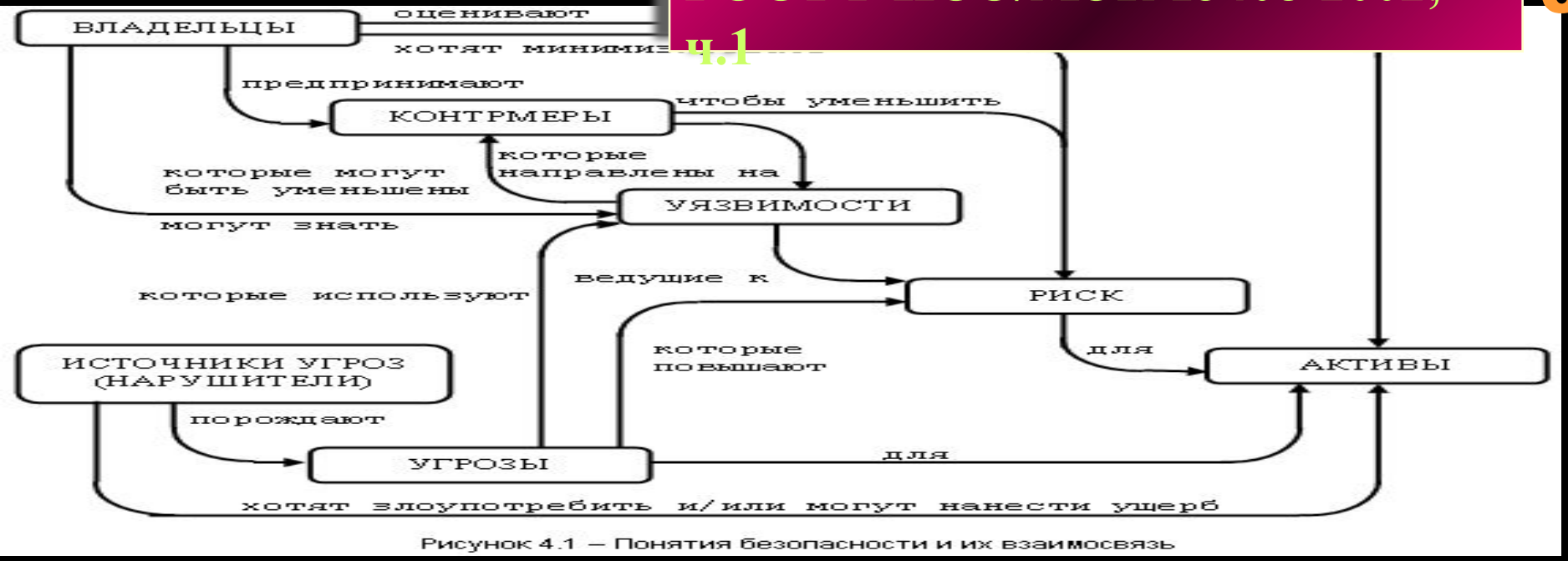


Рисунок 4.1 — Понятия безопасности и их взаимосвязь

Процесс создания КС в аспекте обеспечения безопасности:

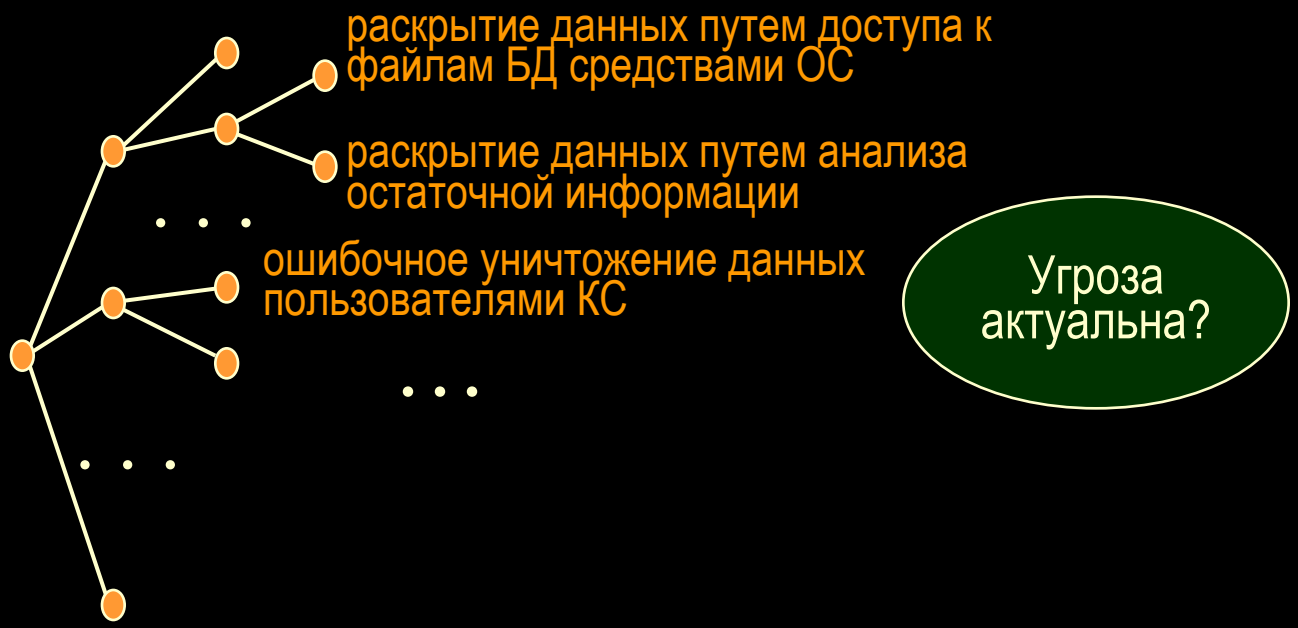
1. Идентификация и оценка защищаемых активов (*конфиденциальность*, *целостность*, *доступность*) и функций КС
2. Идентификация угроз безопасности (выявление и спецификация - источники/природа; активы/функции, подвергаемые воздействию; методы/способы/особенности реализации; используемые уязвимости) и 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

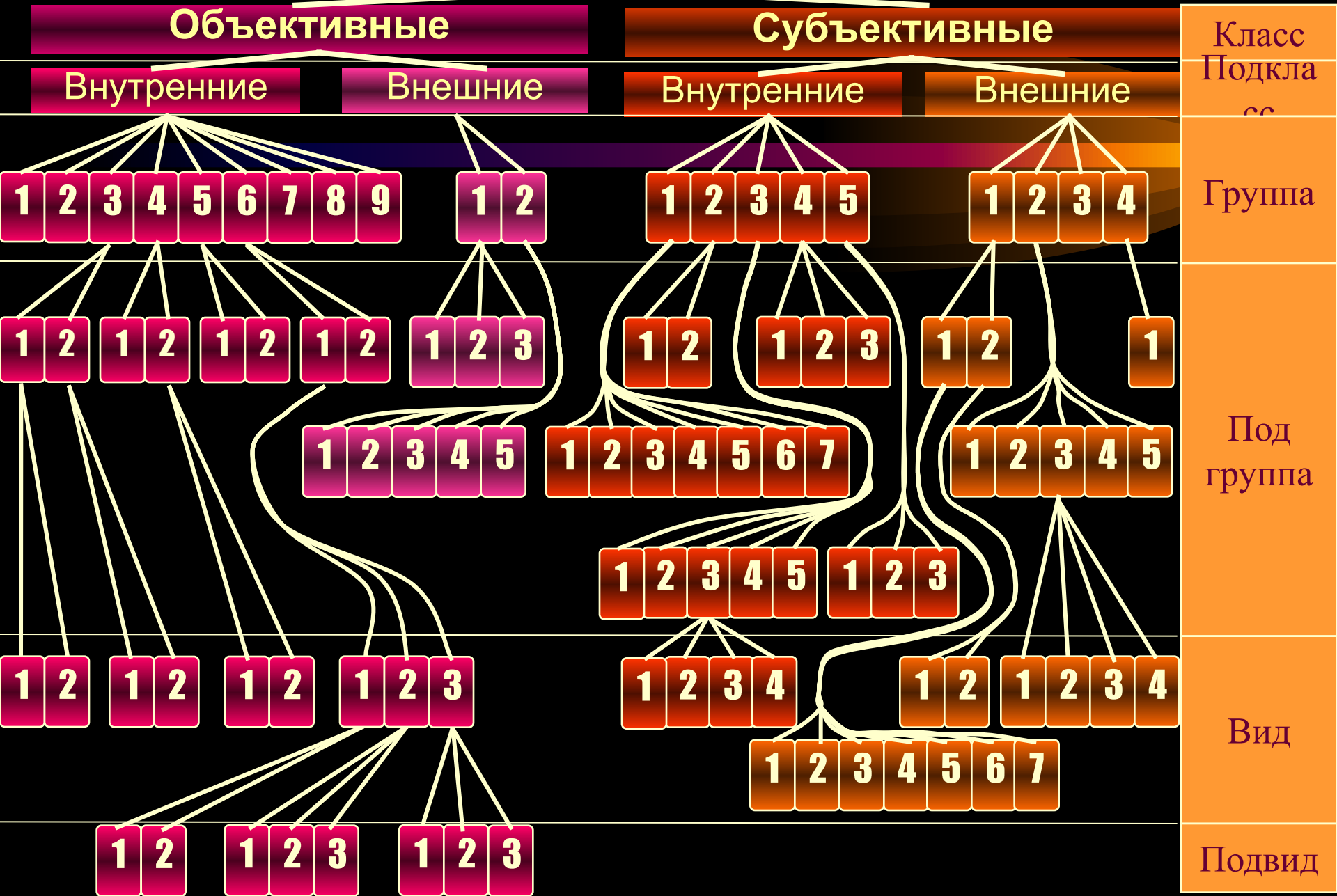
ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. http://linux.nist.fss.ru

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, 2003г., 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, 2003г., 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

Угрозы защищаемым активам в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2003г., 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, 2003г., 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 да…

- 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, 2003г., 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, 2003г., пример)

системные службы данные

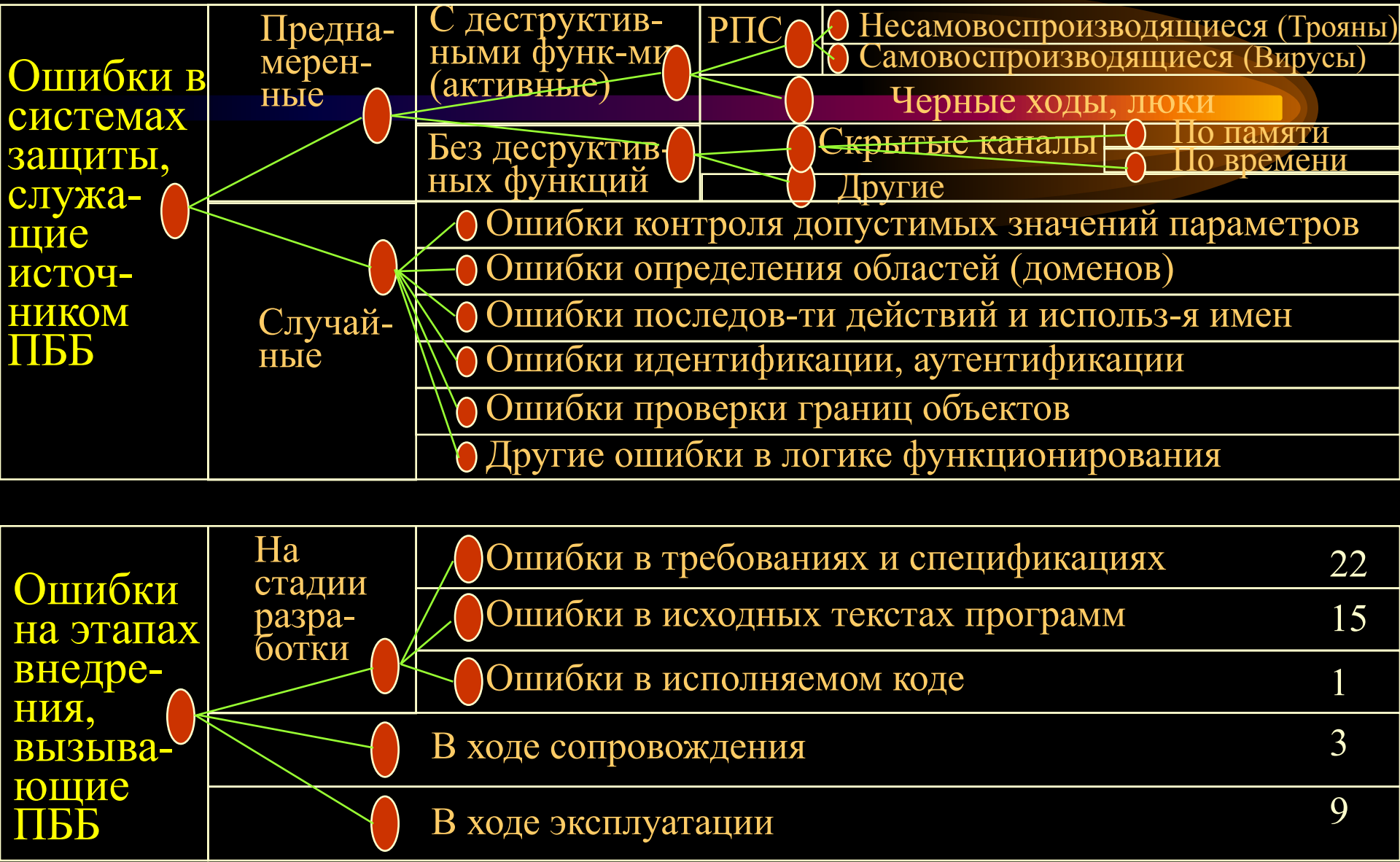
- нарушение безопасности системы путем раскрытия секретного ключа шифрования
- система незаконно используется пользователем, который выдает себя за оператора во время отсутствия оператора
- нарушение безопасности системы вследствие несанкционированного действия или ошибки уполномоченного пользователя
- 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

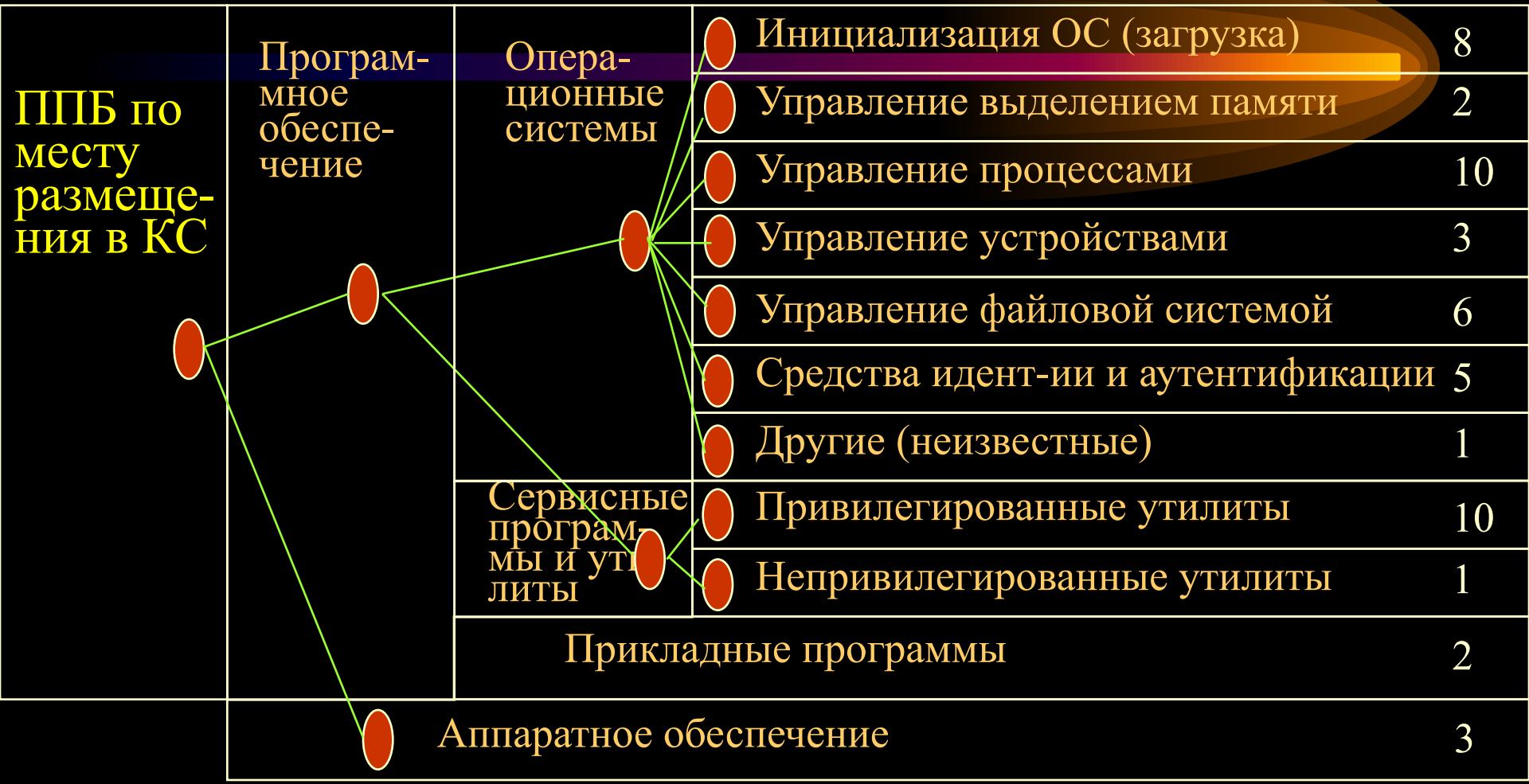
2. Идентификация и таксонометрия (каталогизация) угроз

Потенциальные бреши безопасности (по Зегжде)

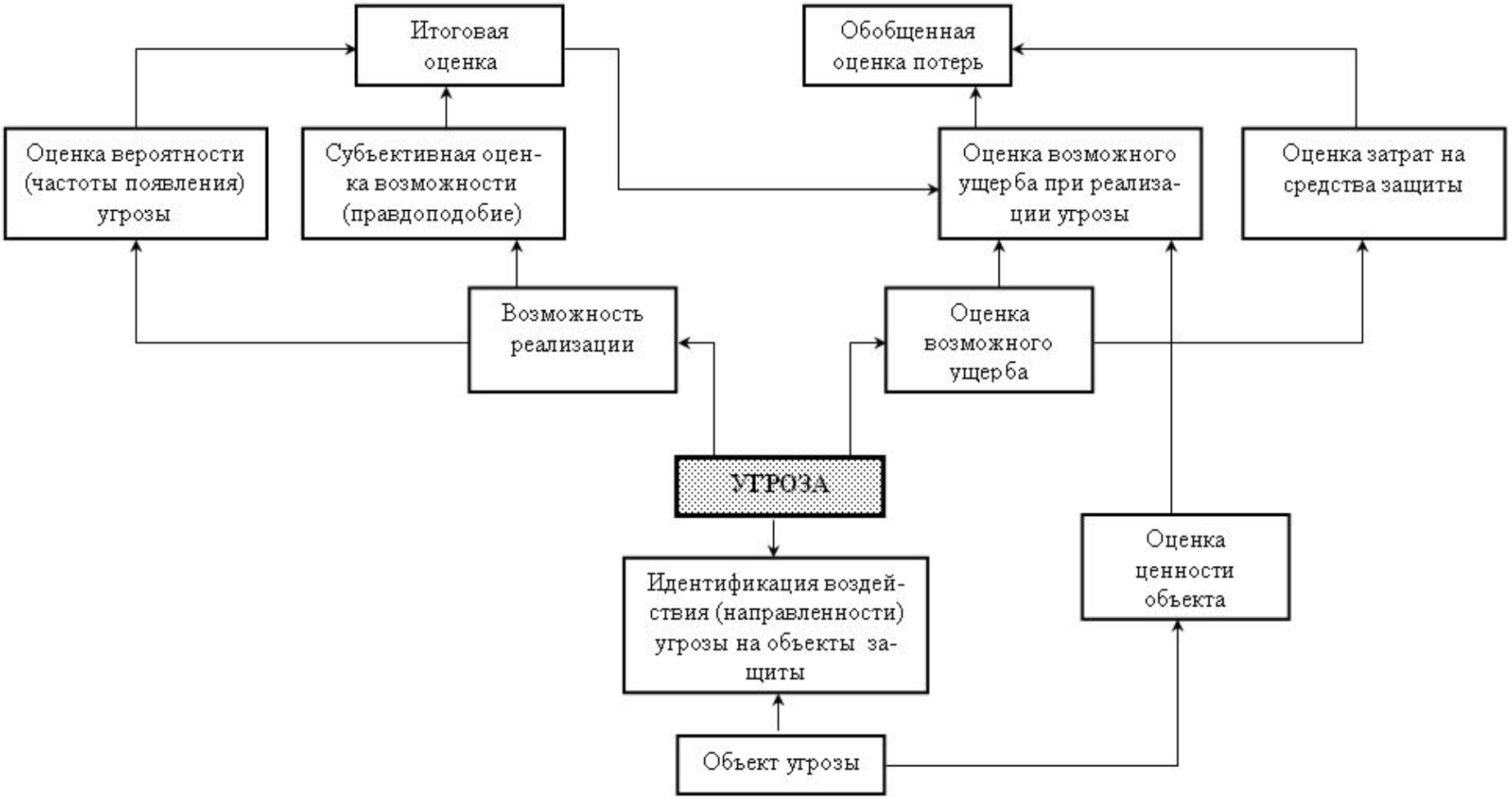


2. Идентификация и таксонометрия (каталогизация) угроз

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

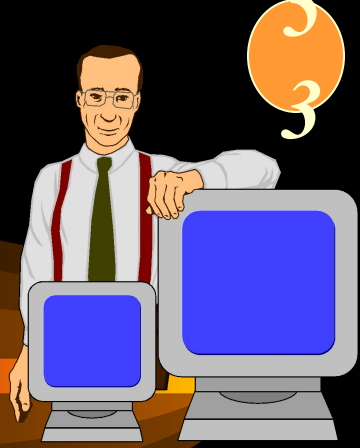
Тема 1. Исходные положения теории компьютерной безопасности

Лекция Лекция 1Лекция 1.Лекция 1.3Лекция

1.3. Политика и модели безопасности в ьютерных 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***

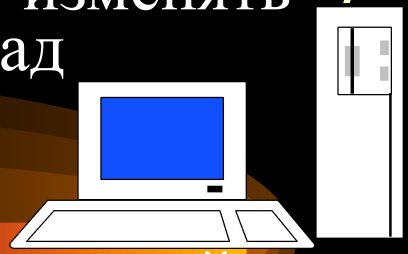
4. В каждый момент времени t_k субъекты могут порождать *процессы над объектами*, называемыми ***доступами***

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

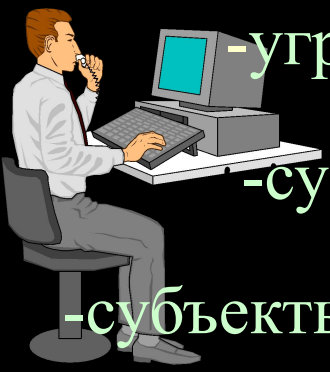


Объект -пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов

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

!!!Ось 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

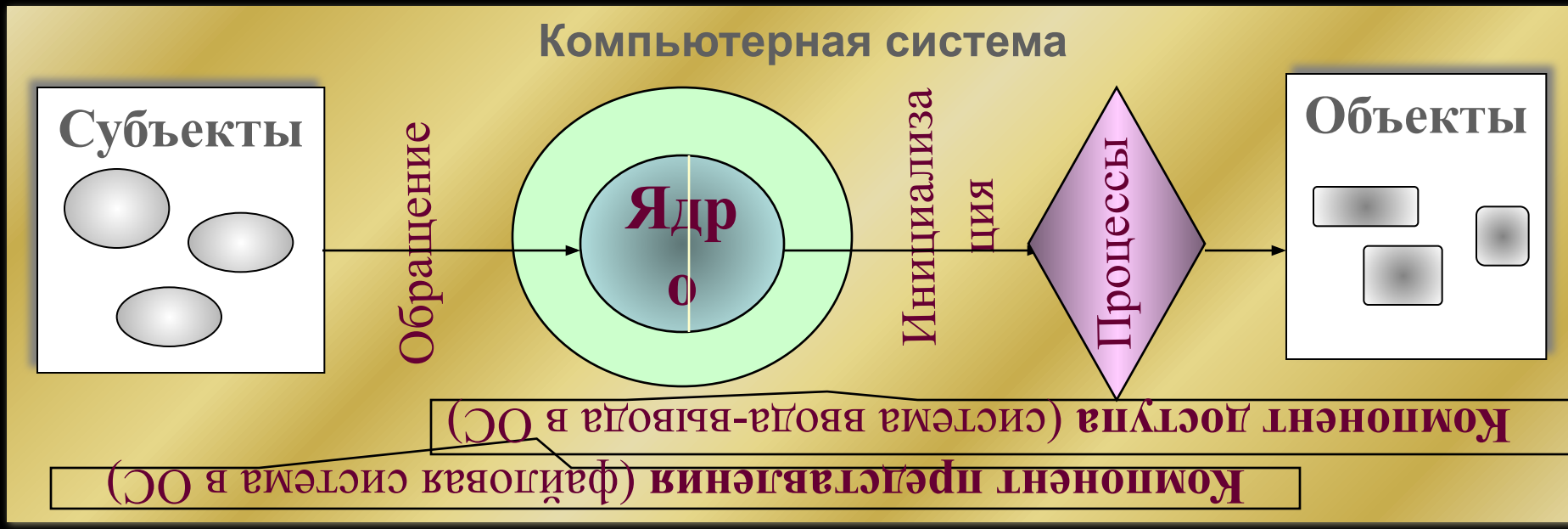
- множество P_L задается неявным образом через предоставление субъектам неких полномочий (допуска, мандата) порождать определенные потоки над объектами с определенными характеристиками конфиденциальности (метками, грифами секретности)

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

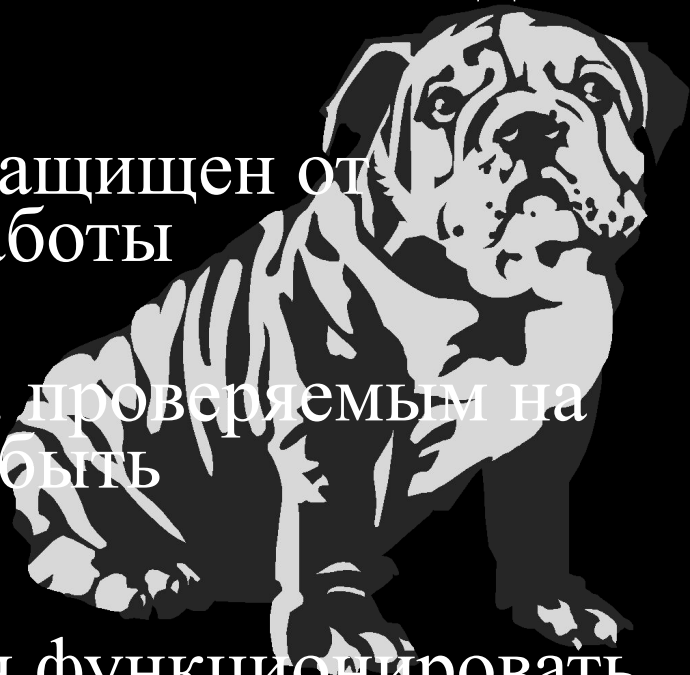


2. Монитор (ядро) безопасности КС

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

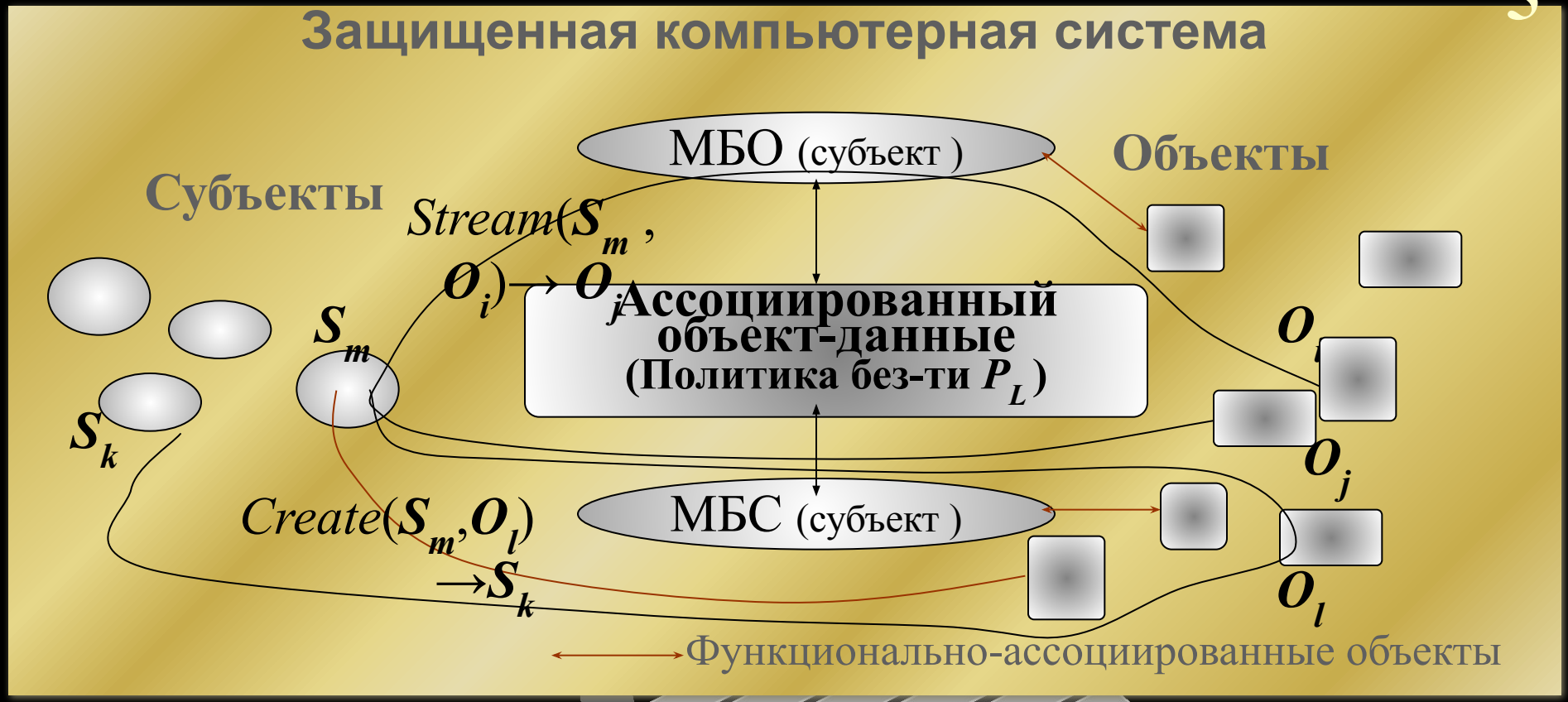
Особенности субъектно-объектной модели КС (определения 1, 2, 3 и 4) требуют структуризации монитора безопасности на две компоненты:

- **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.

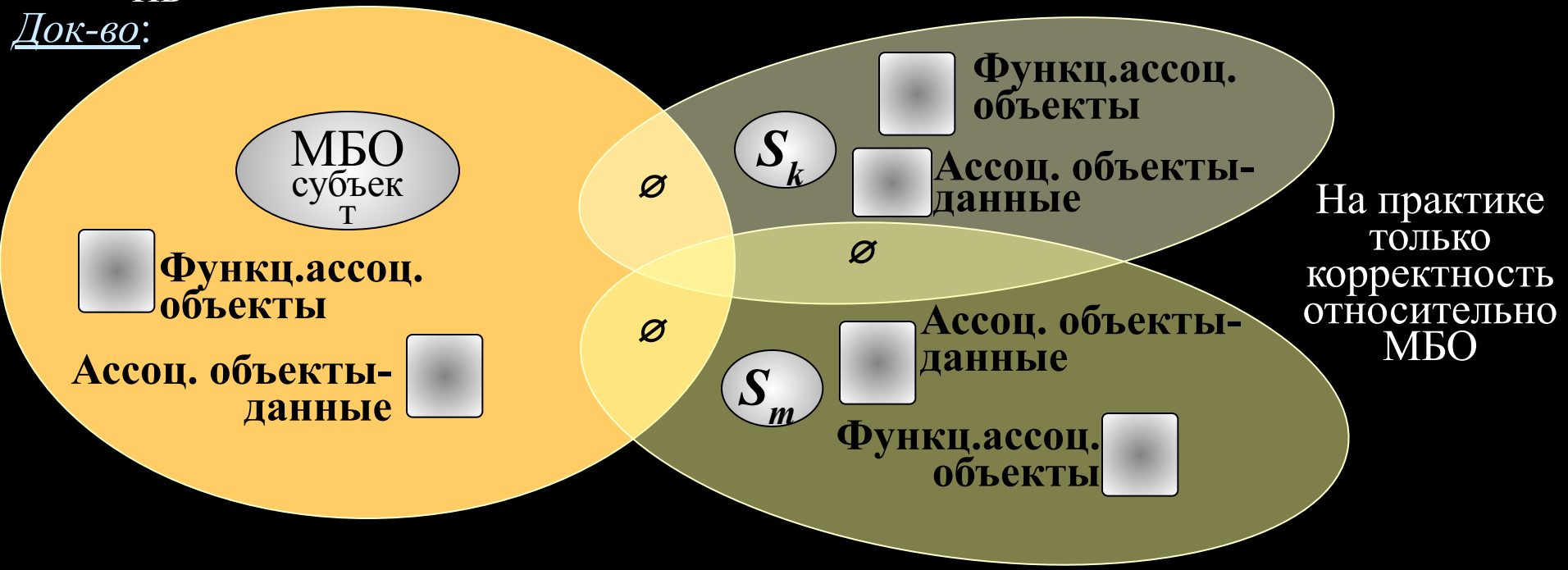
Определение 11. Субъекты S_i и S_j называются ***абсолютно невлияющими*** друг на друга (или ***абсолютно корректными*** относительно друг друга), если дополнительно к условию определения 10 множества ассоциированных объектов указанных субъектов не имеют пересечений

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:



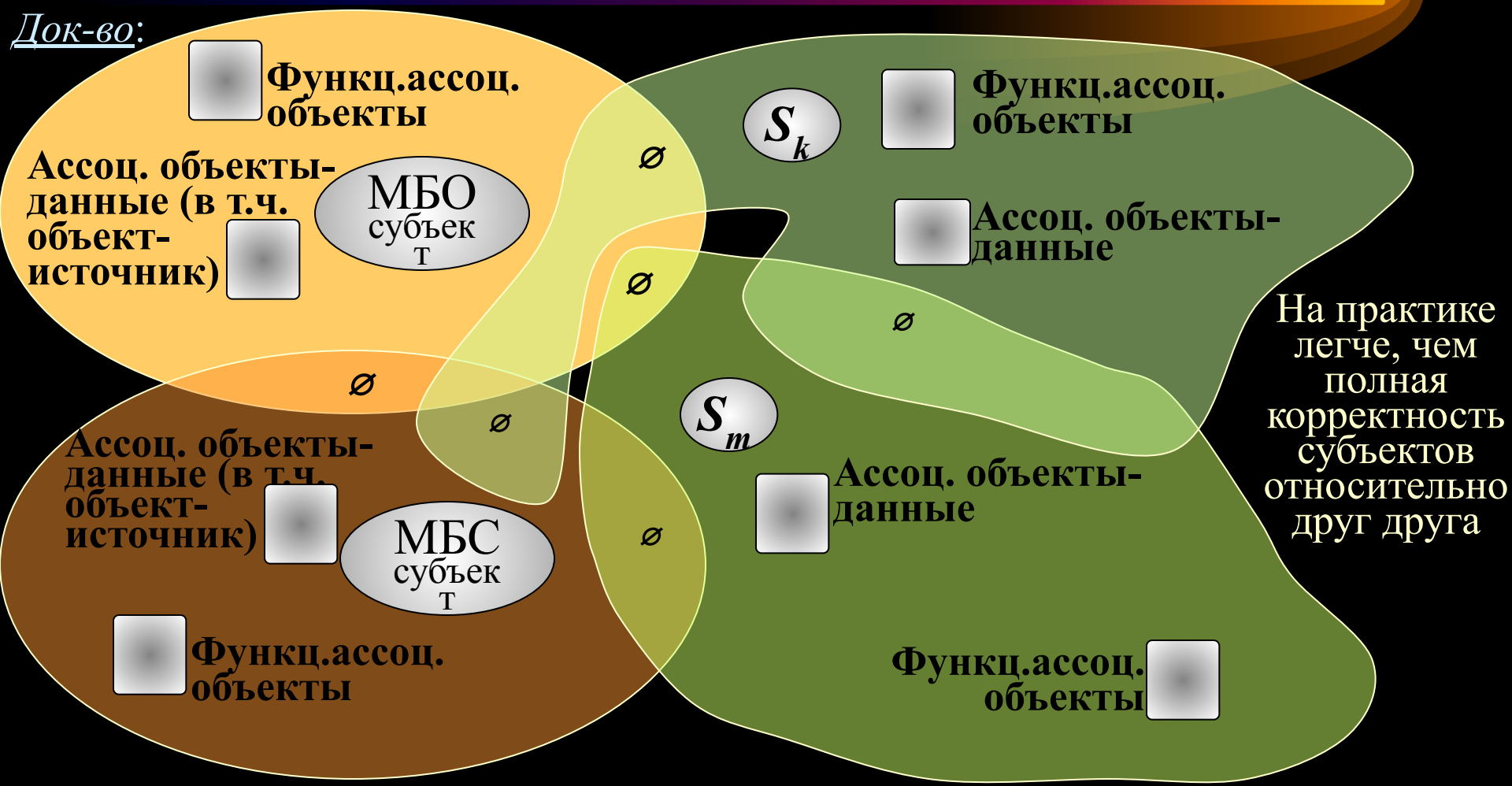
На практике только корректность относительно МБО

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

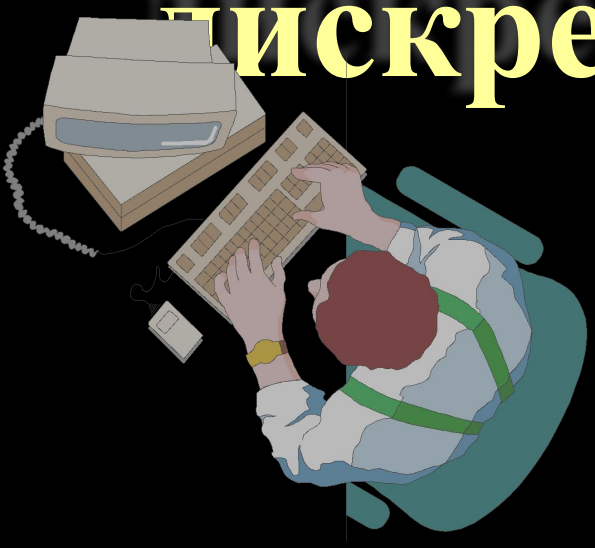
Проблемы реализации *Изолированной программной среды*

- 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***

Тема 2. **Модели безопасности компьютерных систем**

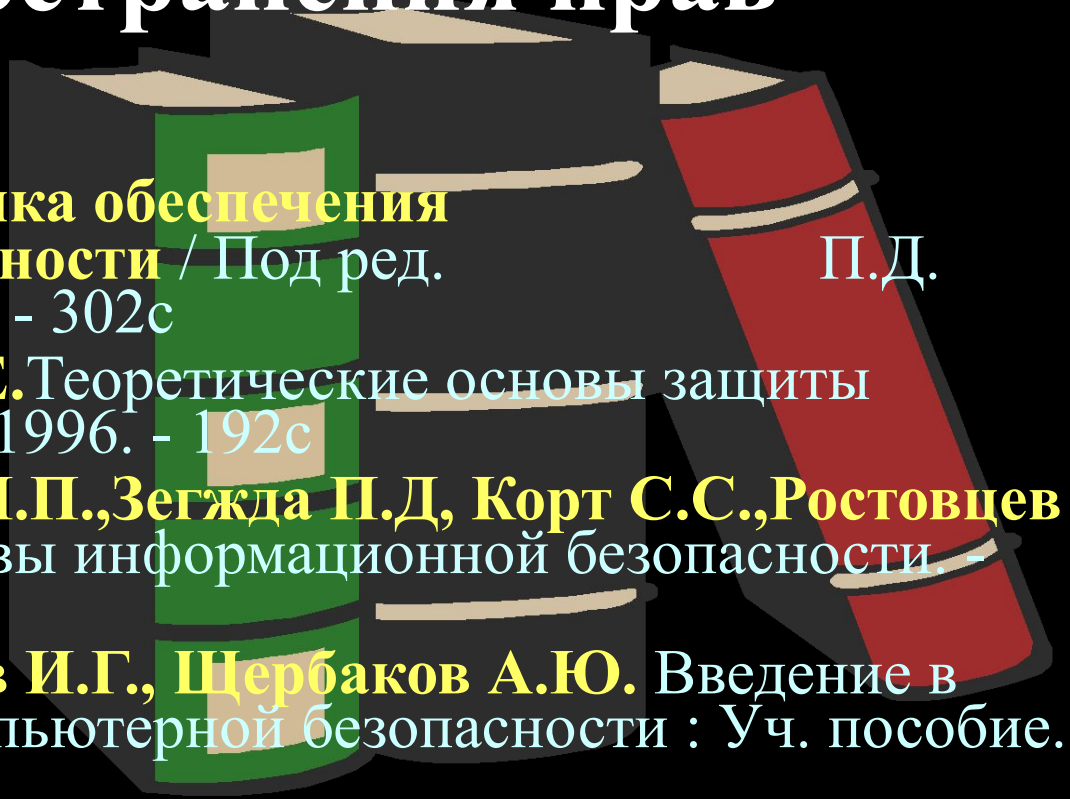
Лекция 2.1.

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 доступ

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

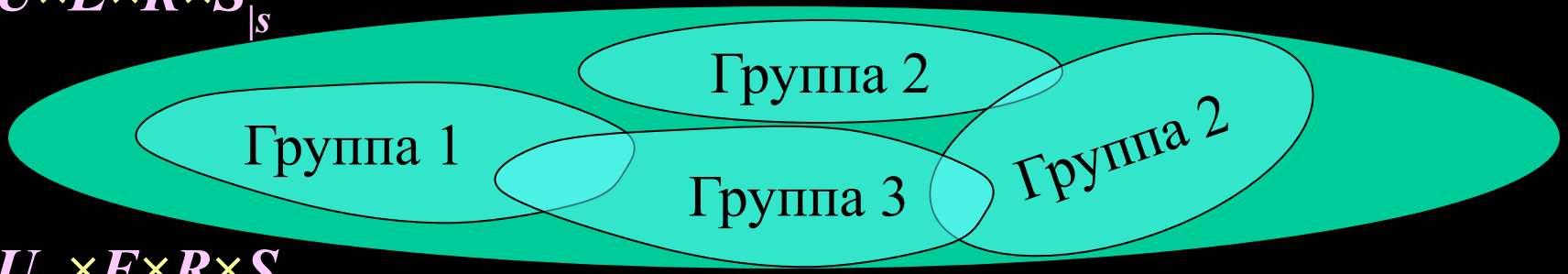
Процесс организации доступа по запросу осуществляется по следующему алгоритму:

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

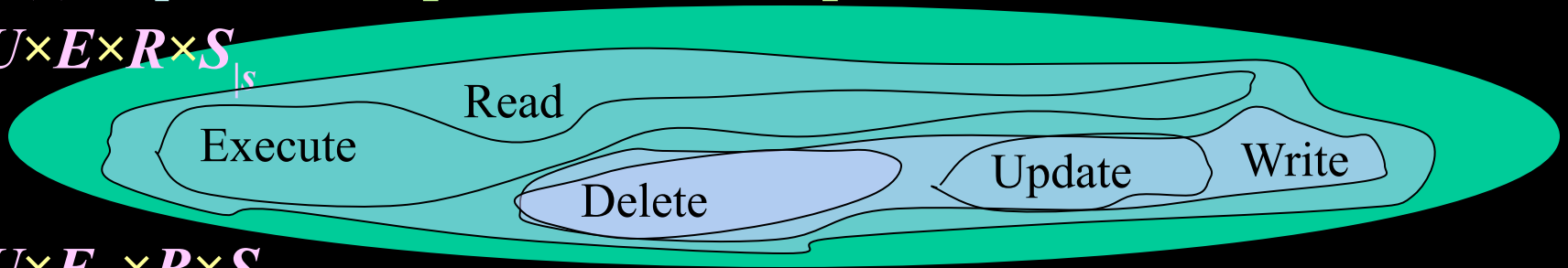
$A \times U \times E \times R \times S_{|s}$



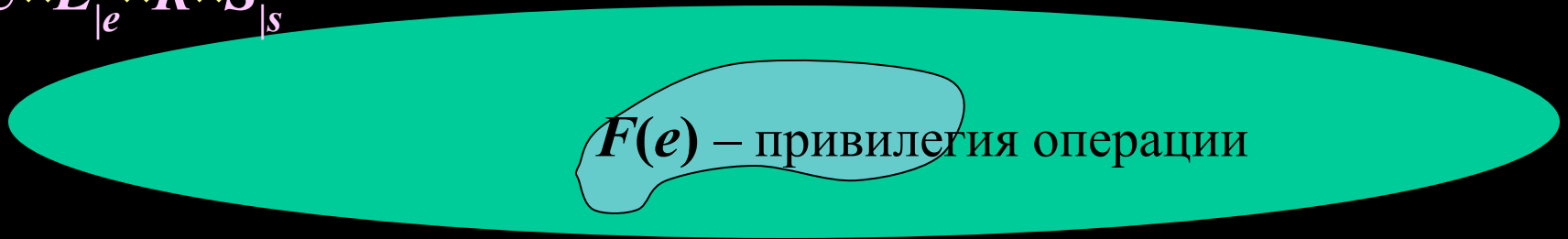
$A \times U_{|u} \times E \times R \times S_{|s}$

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**.

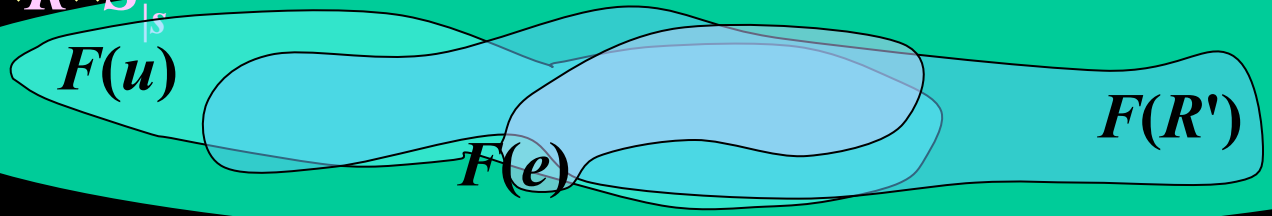
$A \times U \times E \times R_{|R'} \times S_{|S}$

$F(R')$ – привилегия запрашиваемых ресурсов

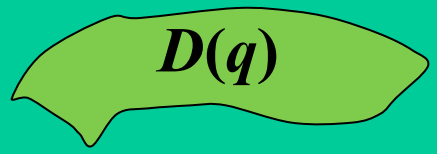
На основе $P=F(u)$, $P=F(e)$ и $P=F(R')$ образуется т.н. **домен полномочий запроса**:

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

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



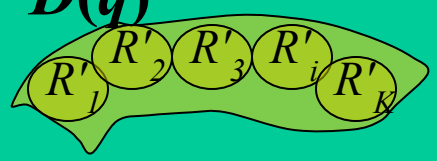
$A \times U_{|u} \times E_{|e} \times R_{|R'} \times S_{|S}$



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 $D(q)$.

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

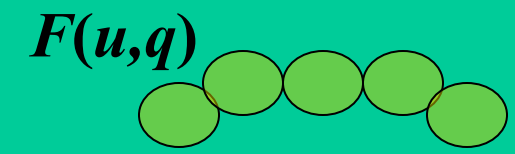


6. Осуществить разбиение $D(q)$ на эквивалентные классы, так, чтобы в один класс попадали полномочия (элементы $D(q)$), когда они специфицируют один и тот же ресурс r из набора R'.

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

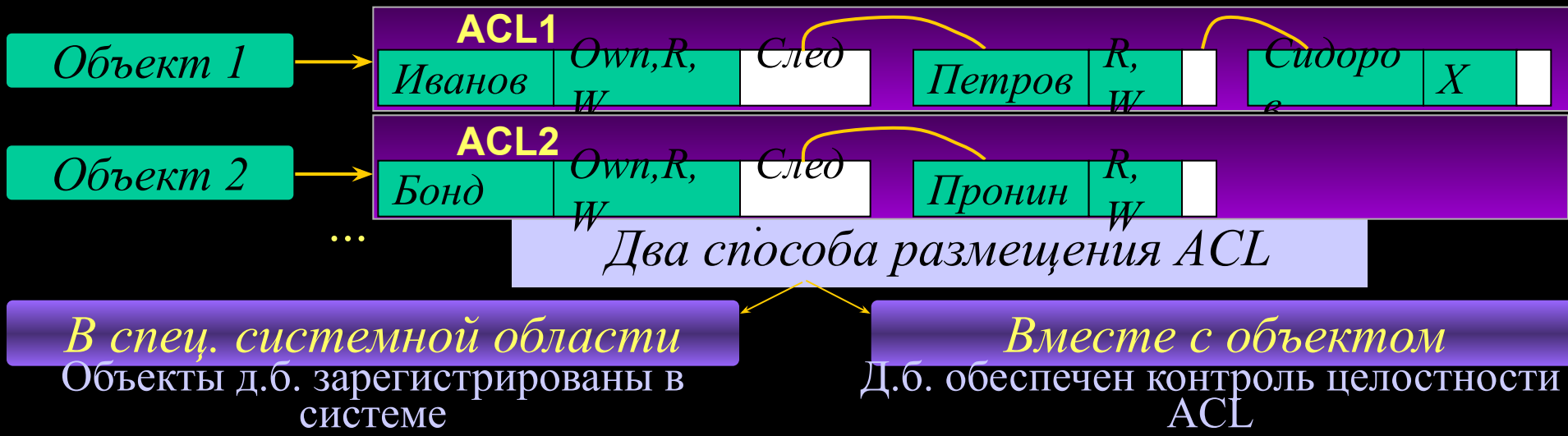
системная таблица с назначениями доступа

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	1	1	1	1	0	1	0	0	0
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

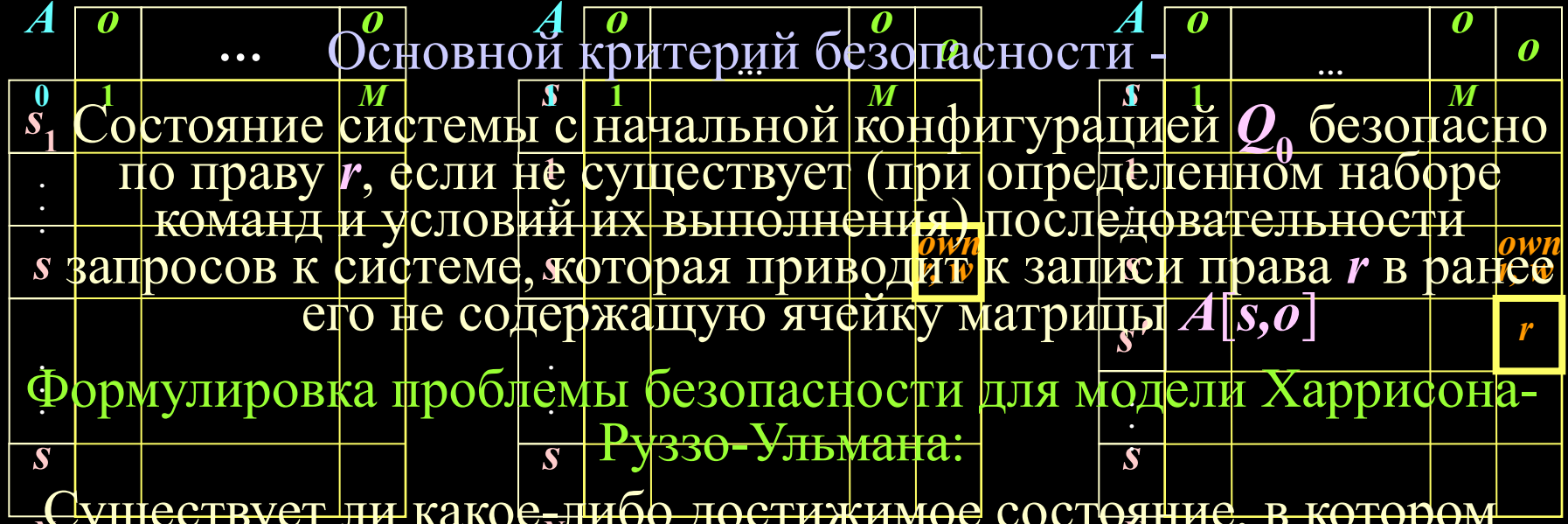
Команды с одной операцией – **монооперационные**, с одним условием - **моноусловные**

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

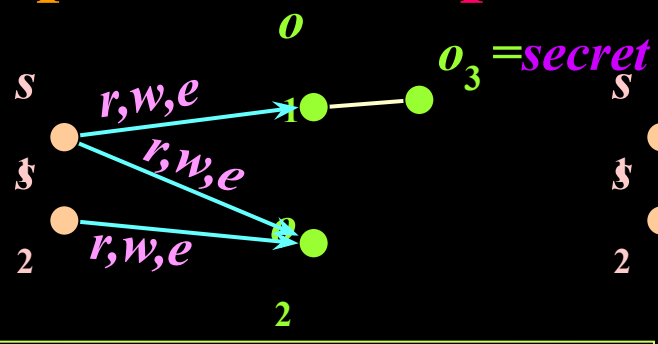
Теорема 2. Проблема безопасности неразрешима в общем случае

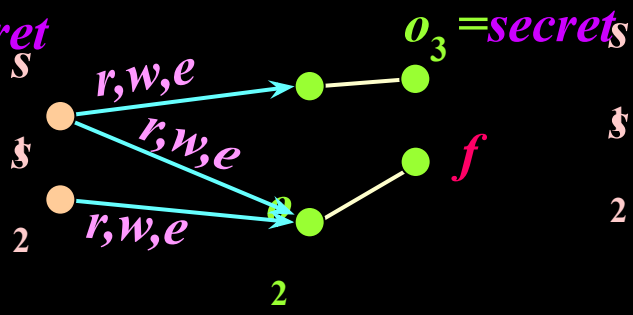
Выводы по модели Харрисона-Руззо-Ульмана:

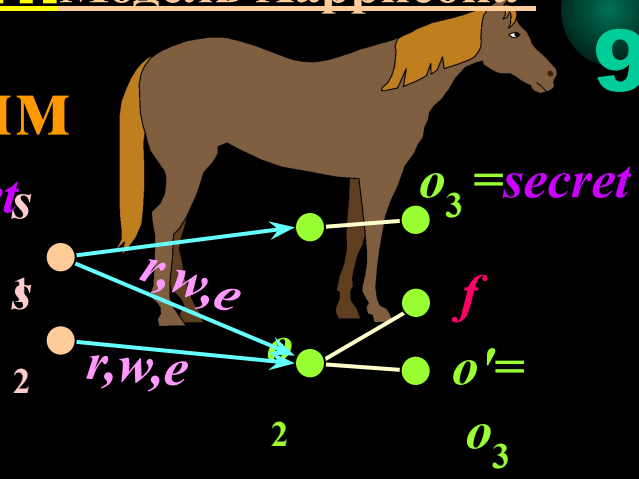
-данная модель в ее полном виде позволяет реализовать множество политик безопасности, но при этом проблема безопасности становится неразрешимой

-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



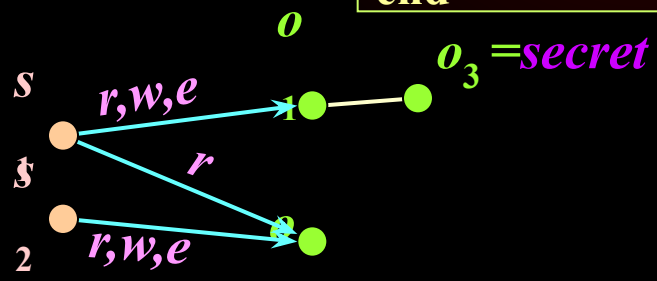




Command "создать файл" (s_2,f):
 if *write* ∈ [s_2, o_2] ;
 then
  Create object f ;
  Enter "read" into [s_2, f] ;
  Enter "write" into [s_2, f] ;
  Enter "execute" into [s_2, f];
 if *read* ∈ [s_1, o_2] ;
  then
  Enter "read" into [s_1, f] ;
 if *write* ∈ [s_1, o_2] ;
  then
  Enter "write" into [s_1,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

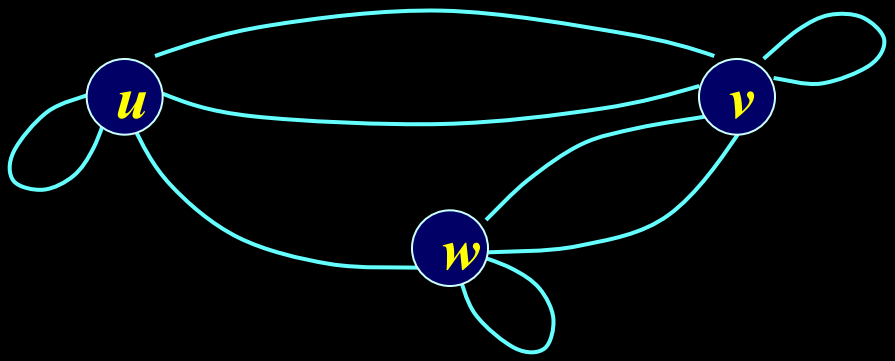
Анализ проблем безопасности в модели TAM основывается на понятии родительских и дочерних типов

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

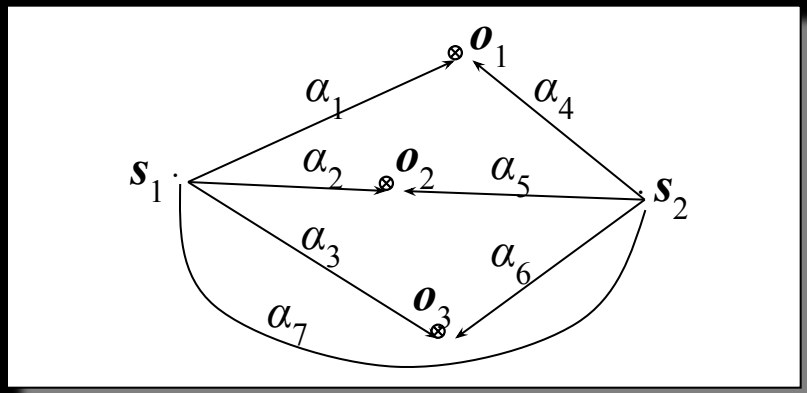
Джонс, Липтон, Шнайдер, 1976г.

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:

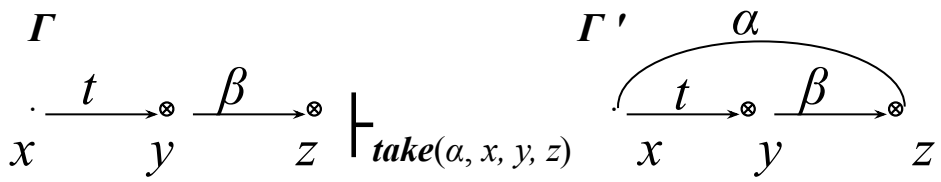
- множество исходных объектов $O\ (o_1,o_2,\ldots,o_M)$
- множество исходных субъектов $S\ (s_1,s_2,\ldots,s_N)$, при этом $S \subseteq O$
- множество прав, которые м.б. даны субъектам по отношению к объектам $(r_1,r_2,\ldots,r_K) \cup \{t, g\}$, в том числе с двумя специфическими правами – правом ***take*** (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



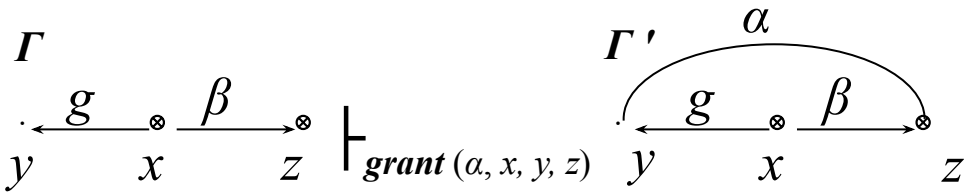
2.Состояние системы (**Графа доступов**) изменяется под воздействием элементарных команд 4-х видов

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



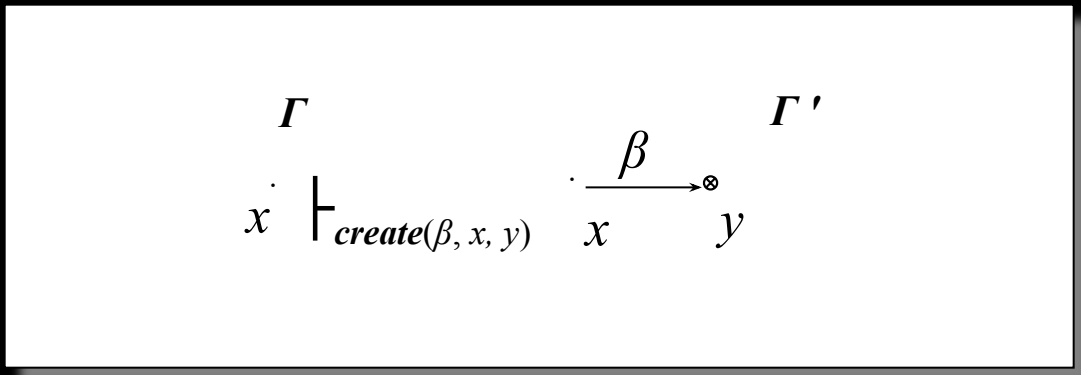
субъект ***x*** берет права доступа $\alpha \subseteq \beta$ на объект ***z*** у объекта ***y*** (обозначения: $\vdash_c$ – переход графа ***Г*** в новое состояние ***Г'*** по команде ***c*** ; $x \in S$; $y, z \in O$)

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



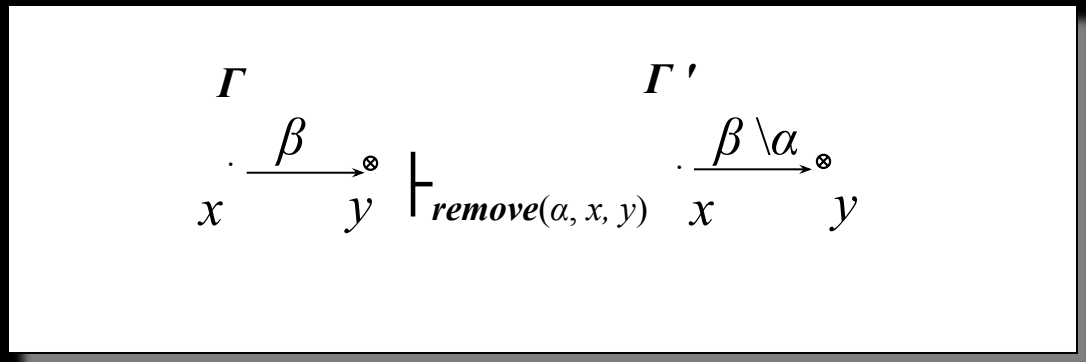
субъект ***x*** дает объекту ***y*** право $\alpha \subseteq \beta$ на доступ к объекту ***z***

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*

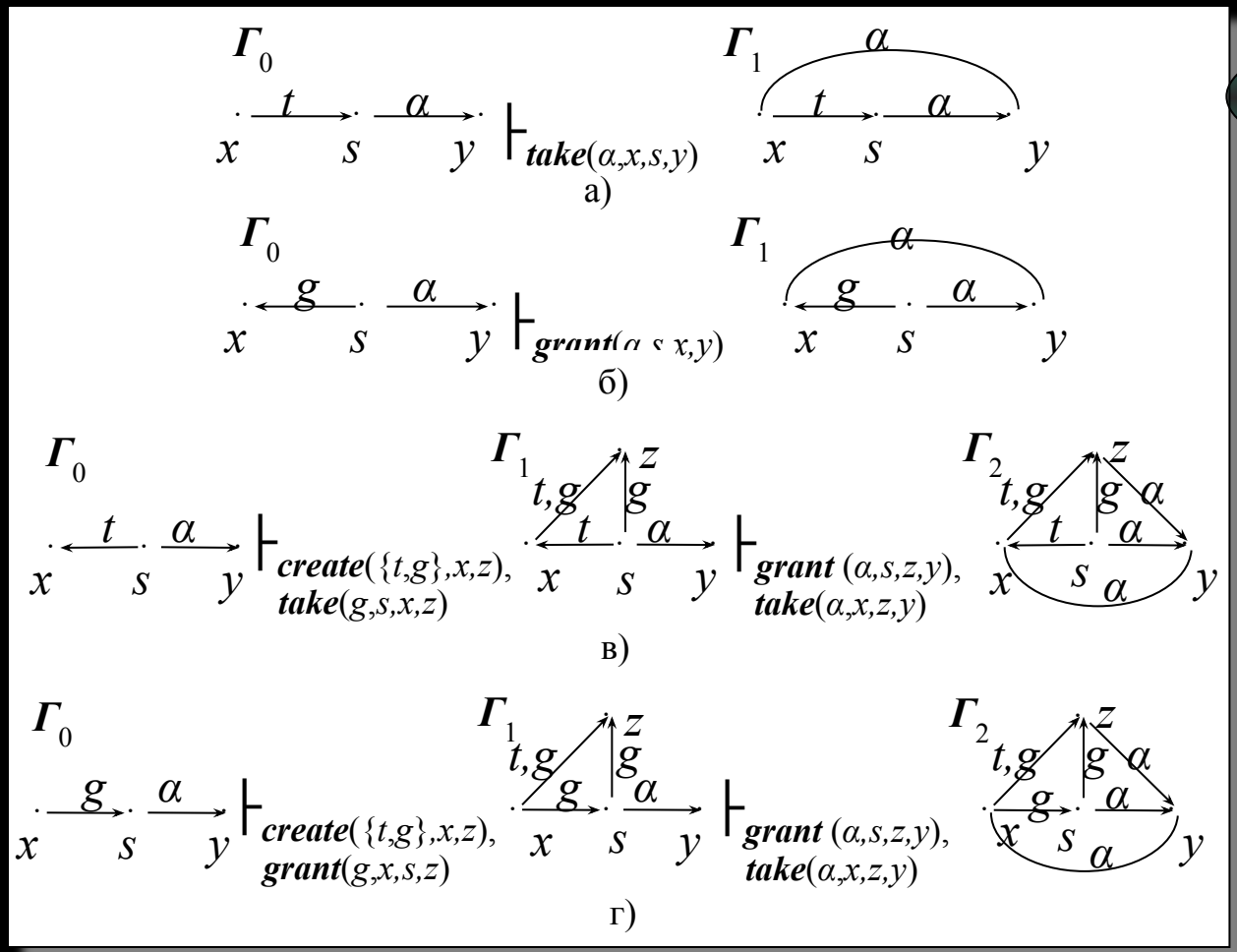
Определение **4**. *Вершины графа доступов являются **tg-связными** (соединены **tg**-путем), если в графе между ними существует такой путь, что каждая дуга этого пути выражает право **t** или **g** (без учета направления дуг)*

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

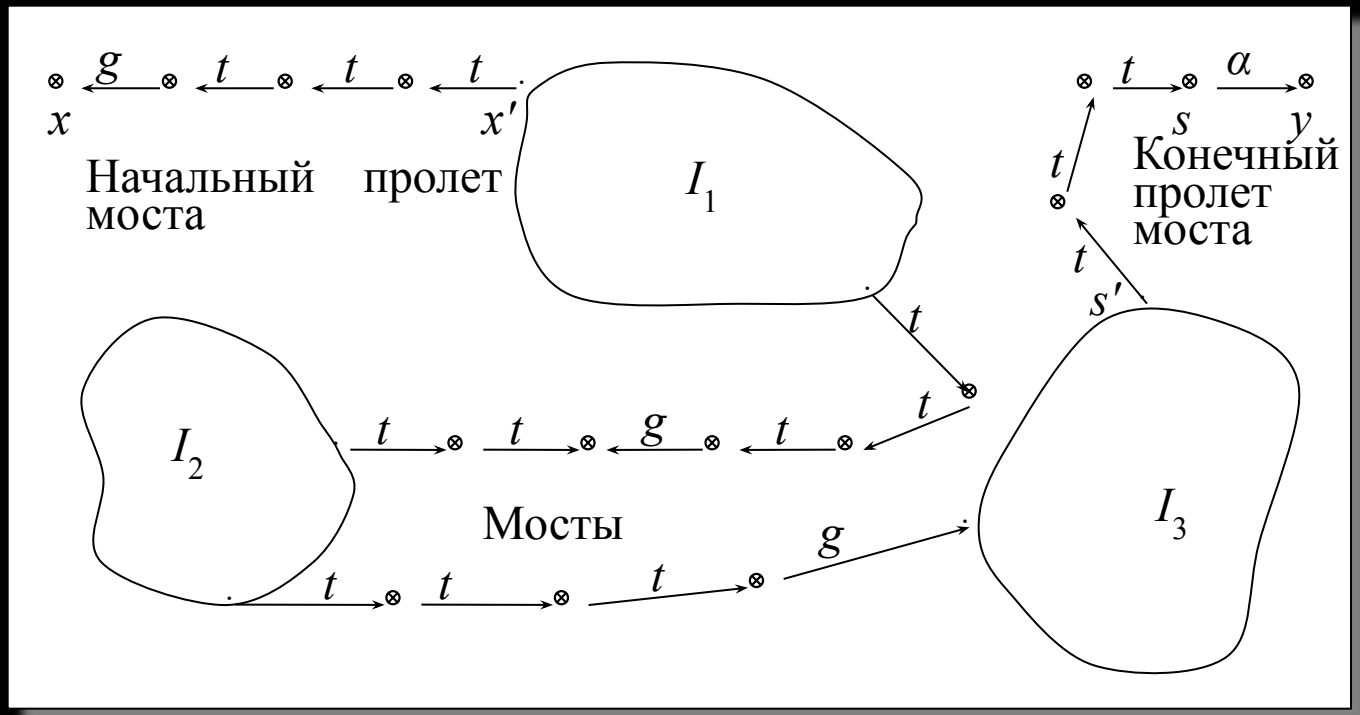
Теорема 4. *В произвольном графе доступов* $\Gamma_0 (O_0, S_0, E_0)$ *предикат "**возможен доступ**(α, x, y, Γ_0)" истинен тогда и только тогда, когда выполняются условия:*

- 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