Информация о курсе и лекторе

Название курса:

«Защита информационных процессов в компьютерных системах (ЗИП КС)»

Лектор:

АРУСТАМОВ Сергей Аркадьевич,
профессор кафедры ПБКС, д.т.н.
зам. декана ФКТУ по науке и проектной деятельности
ауд. 379

Определение объекта информатизации и информации

Объект информатизации:

совокупность информационных ресурсов, **средств и систем обработки информации, используемых в соответствии с заданной информационной технологией**, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров;

Информация:

Философский подход:

Свойство материальных объектов и процессов сохранять и порождать определенное состояние

Кибернетический подход:

Мера устранения неопределенности

Подход ГОСТ Р 51275-99 (ОБЪЕКТ ИНФОРМАТИЗАЦИИ. ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ НА ИНФОРМАЦИЮ) :

Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления

Подход курса ЗИП КС

все, что может быть представлено в символах конечного алфавита (например, бинарного)

Состав автоматизированной системы (АС)

-средства вычислительной техники (ВТ) (hardware);

-программного обеспечения (ПО) (software);

-каналов связи, терминального и сетевого оборудования (ИКТ: термин введен в связи с возрастанием роли компонента) (communication & network equipment)

-информация на различных носителях (information media);

-обслуживающий персонал и бизнес пользователи (maintenance staff and end users)

Информационная безопасность АС

-система способна противостоять дестабилизирующему воздействию внешних и внутренних угроз;

-функционирование и сам факт наличия системы не создают угроз для внешней среды и элементов самой системы;

Базовые свойства, определяющие безопасность информации

-**конфиденциальность (confidentiality),** означающая возможность доступа к информации только легальным пользователям;

-целостность (integrity), обеспечивающая *во-первых*, защиту информации, которая может быть изменена только законными и имеющими соответствующие полномочия пользователями, и, *во-вторых,*

внутреннюю непротиворечивость (корректность, правильность) информации и, если данное свойство применимо, отражение реального положения вещей (актуальность);

-доступность (availability), гарантирующая беспрепятственный доступ к защищаемой информации для легальных пользователей в течении оговоренного времени;

-аутентичность (authenticity), обеспечивающее истинность источника информации;

-неотказуемость (non-repudiation), гарантирующая невозможность отказа от авторства или факта получения информации

Основные методы обеспечения ИБ

Понятие угрозы АС (активу)

Под **угрозой** (threat) понимают потенциально возможное событие, действие, процесс или явление, которое может нанести ущерб чьим-либо интересам.

Угроза АС – это возможность реализации воздействия на информацию, обрабатываемою АС, приводящую в нарушению конфиденциальности, целостности или доступности, а также возможность воздействия на компоненты АС, приводящие к их утрате, уничтожению или сбою функционирования.

Классификация угроз

По природе возникновения:

-естественные и искусственные;

По степени преднамеренности:

-случайные и преднамеренные;

По типу источника угрозы:

-природная среда, человек, санкционированные и несанкционированные программно-аппаратные средства;

По положению источника угрозы:

в пределах и вне контролируемой зоны, непосредственно в АС;

По степени воздействия на АС:

пассивные и активные

По способу доступа:

использующие стандартный и нестандартный доступ

Случайные и преднамеренные угрозы

- **Случайные:**
- Аварийные ситуации из-за стихийных бедствий или отказов электропитания
- Отказы и сбои аппаратуры
- Ошибки в работе обслуживающего персонала
- Помехи в линиях из-за воздействия внешний среды
- **Преднамеренные:**
- Связанные с действиями нарушителя:
- Квалификация на уровне разработчика
- Постороннее лицо или законный (легальный пользователь)
- Нарушителю известен принцип работы системы
- Нарушитель информирован об слабых звеньях системы

Классификация угроз АС на основе градации доступа к информации-1

- **Уровень носителей информации** (хищение, уничтожение, выведение из строя)
- **Уровень средств взаимодействия с носителем** (получение информации о ПА среде, несанкционированный доступ, перехват данных, несанкционированное копирование ПО, перехват данных , передаваемых по каналом связи).

Классификация угроз АС на основе градации доступа к информации-2

- **Уровень представления информации** (определение способа представления информации, визуальное наблюдение, внесение искажений в представление данных)
- **Уровень содержания информации** (определение содержания информации на качественном уровне, раскрытие содержания, внесение дезинформации, запрет на использование информации).

Дерево угроз

Уязвимости, воздействия, риски и защитные меры

Уязвимость (vulnerability) - это слабость АС, которая может быть использована одной или несколькими угрозами (может существовать и в отсутствии угрозы);

Воздействие (impact) – результат инцидента ИБ, вызванного угрозой и нанесшего ущерб;

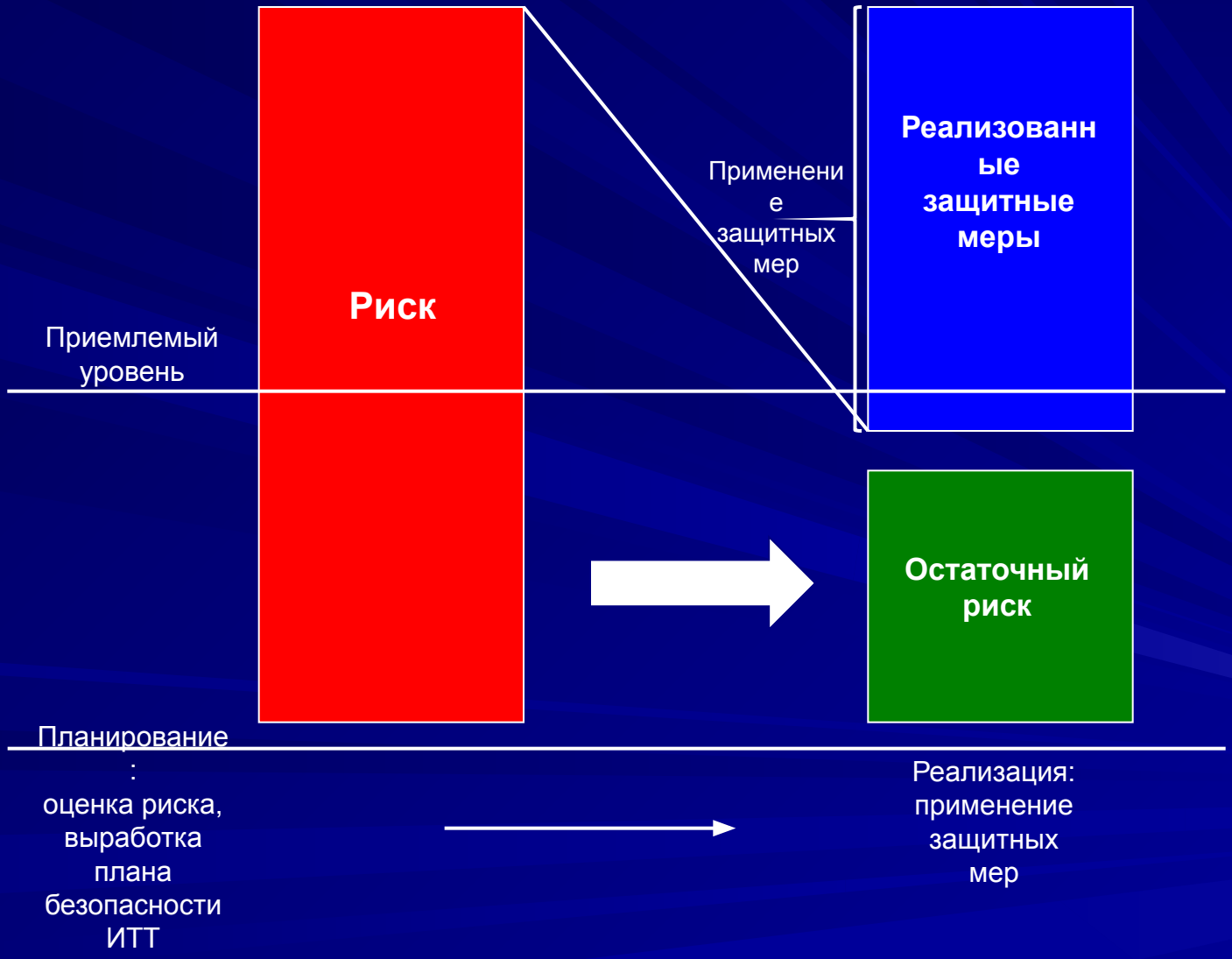
Количественное и качественное измерение воздействия могут быть проведены:

- определением финансовых потерь;
- использованием эмпирической шкалы серьезности воздействия, например от 1 до 10;
- использованием заранее оговоренных уровней (высокий, средний и низкий).

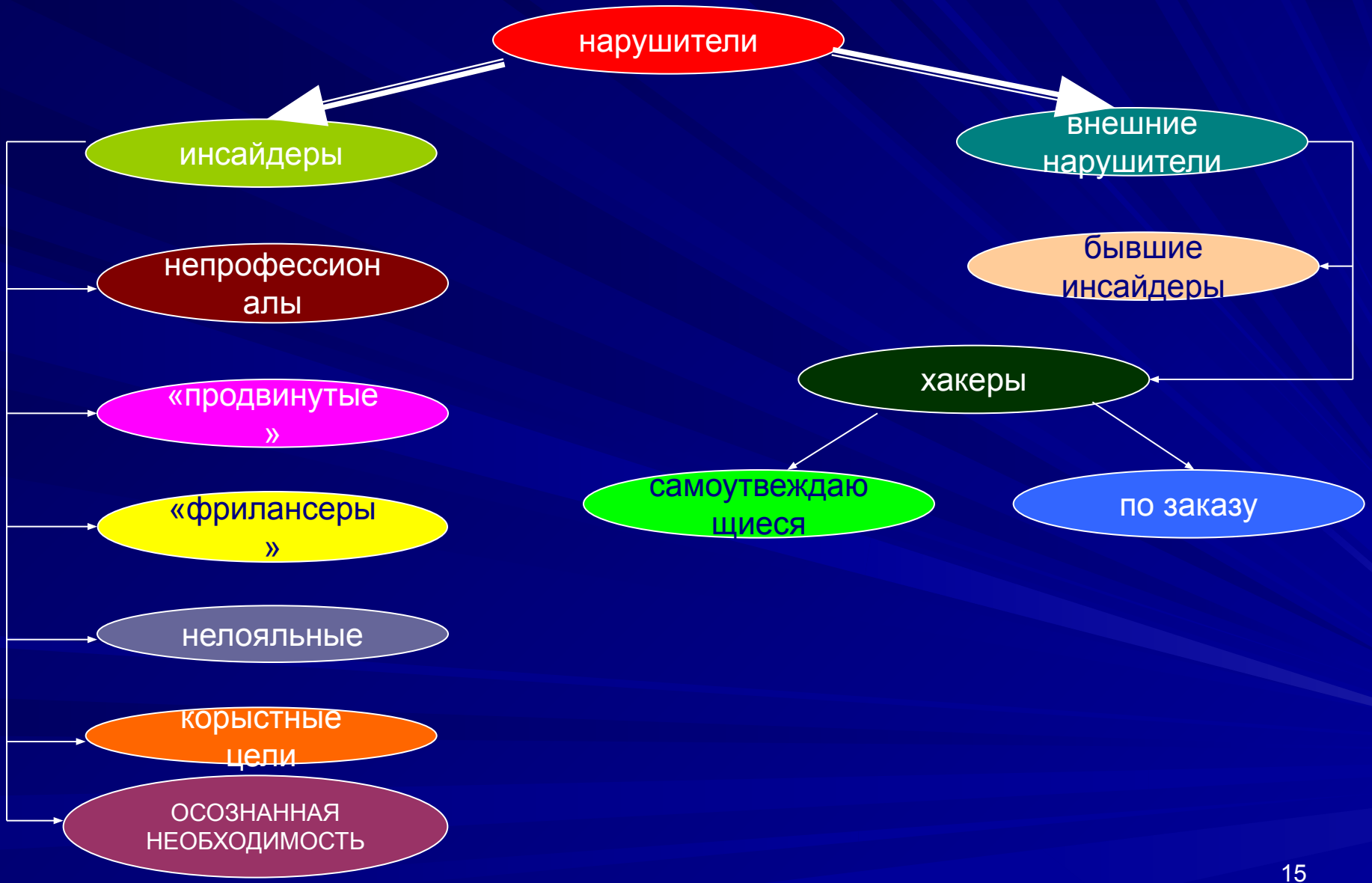
Риск (risk) –это вероятность конкретной угрозы использовать уязвимости для нанесения ущерба (характеризуется вероятностью использования и величиной ущерба)

Защитные меры (safeguards) — это действия, процедуры и механизмы, способные обеспечить уменьшение вероятности возникновения угрозы и величину воздействия, ускорить обнаружение инцидентов и облегчить восстановление активов.

Взаимосвязь защитных мер и риска



Модель нарушителя ИБ



Формальная теория защиты информации: основные определения

Пусть А- конечный алфавит, А* -множество слов конечной длины в алфавите А,

L - язык , т.е. множество слов , выделенных по определенным правилам из

А*. $L \subseteq A^*$

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

Назовем объектами языка L произвольное конечное множество слов языка L. **Преобразованием** информации будем называть отображение на множестве слов языка L.

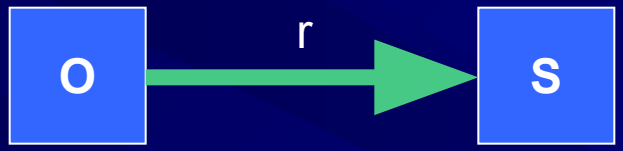
Преобразование может

-**храниться –** в этом случае описание преобразования хранится в некотором объекте и ничем не отличается от других данных;

-**действовать** – взаимодействовать с другими ресурсами АС.

Ресурсы АС, выделенные для действия называются **доменом.** Преобразование, которому передано управление, называется **процессом.** Объект описывающий преобразование , которому выделен домен и передано управление, называется субъектом. **Субъект** для реализации преобразования осуществляет доступ к **объекту.** Существует два основных вида доступа: **чтение и запись.**

Информационный поток от O к S



Информационный поток от S к O

Подавляющее большинство вопросов безопасности информации определяются доступами субъектов к объектам.

Монитор безопасности обращений (СКУД)

Свойства монитора безопасности обращений (МБО)

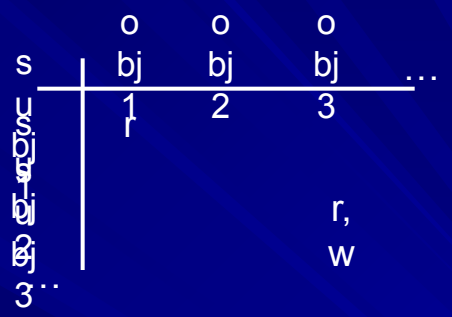
- Ни один запрос на доступ субъекта к объекту не должен выполняться в обход МБО
- Работа монитора должна быть защищена от постороннего вмешательства
- Описание МБО должно быть достаточно простым для возможной верификации корректности его работы

  Несмотря на абстрактность, перечисленные свойства реализуются в программно-аппаратных модулях, реализующих функции МБО в реальных системах.

Матрица дискреционного доступа (модель Хариссона-Руззо-Ульмана) (Harisson M. Ruzzo W. Ullman J. 1976)

r

- Система $\sum = \{S, O, R, M, C, Q\}$ состоит их следующих элементов:
- Конечное множество исходных субъектов S
- Конечное множество исходных объектов O
- Конечное множество прав доступа R
- Исходная матрица доступа M
- Конечное множество команд C
- Конечное множество состояний Q



Поведение системы- последовательность состояний Q, причем каждое последующее состояние есть результат применения команды к предыдущему

Безопасность начального состояния

- Для заданной системы начальное состояние Q называется безопасным относительно права a (access) , если не существует применимой к Q последовательности команд, в результате выполнения которой право a будет занесено в ячейку матрицы, в которой оно отсутствовало в состоянии Q.
- В противном случает говорят об утечке права a.

Примеры команд, описывающих изменение системы (неформальное описание)

- Создание нового субъекта с получением по отношении к нему прав доступа r, w
- Передача права доступа {a} от любого субъекта любому субъекту, по отношению к которому субъект обладает правом записи (запись права)
- Получение права доступа {a} от любого субъекта любому субъекту, по отношению к которому субъект обладает правом чтения (чтение права)

Команды, описывающие изменение системы (формальное представление)

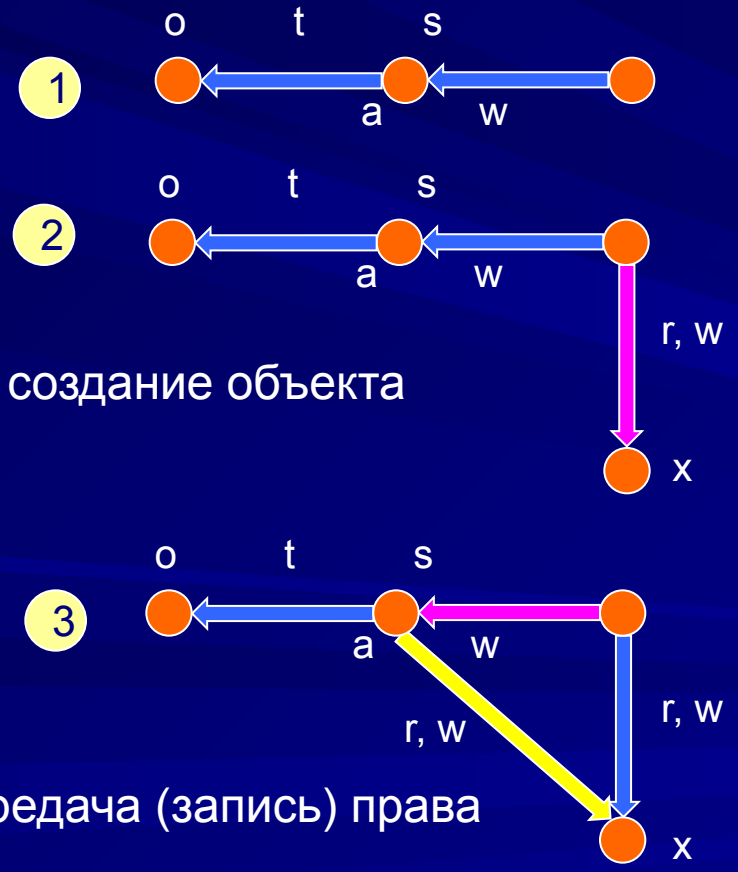
1 **Создание субъекта:**
create subject x,
enter r into M [s,x,], enter w into M [s,x]

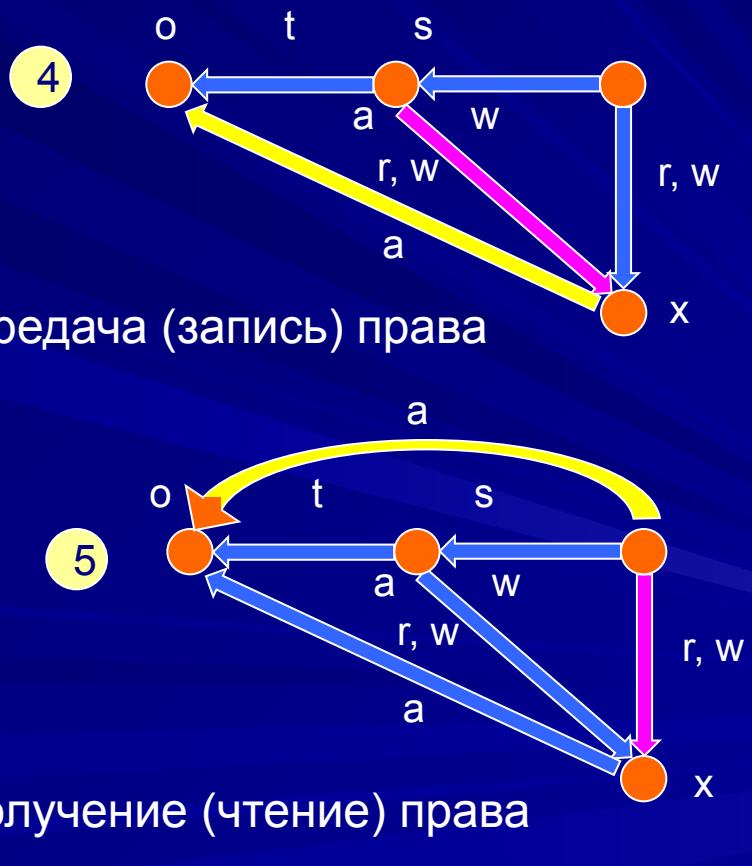
2 **Передача прав доступа**
grant a (s,x,p)
if w in M [s,x] and a in M {s,p]
then enter a into M [x,p]

3 **Получение прав доступа**
take a (s,x,p)
if r in M [s,x] and a in M {x,p]
then enter a into M [s,p]

Матрица доступа (модель Харисона-Руззо-Ульмана Harisson M. Ruzzo W. Ullman J. 1976)

Утечка права при передаче прав на «третий» субъект или получение прав от «третьего» субъекта (rights drain)





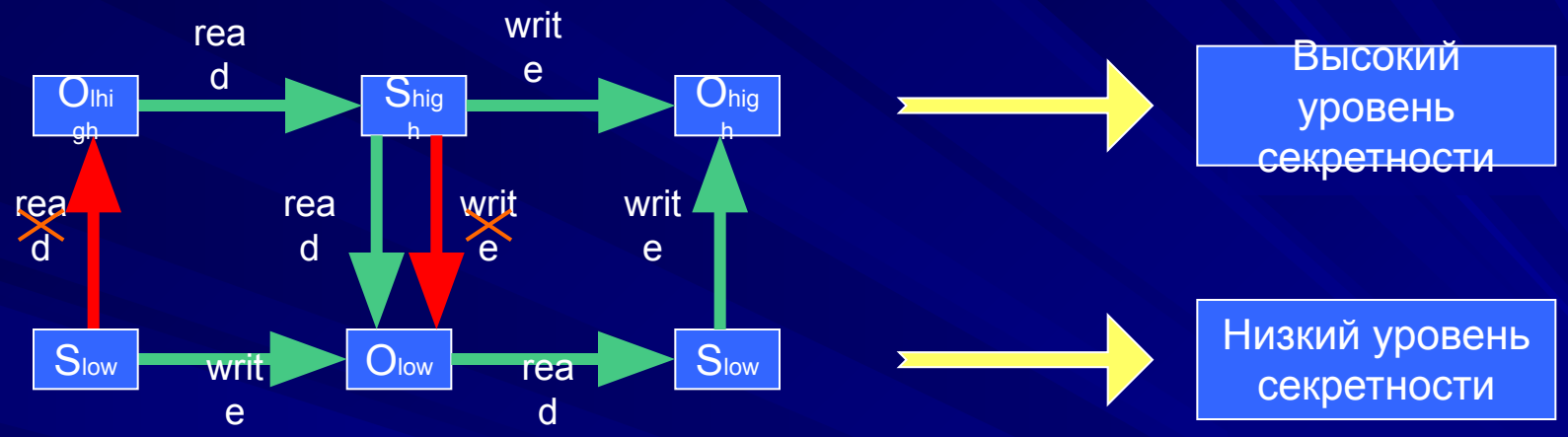
Критерий безопасности системы

- Система называется монооперационной, если каждая команда выполняет один примитивный оператор

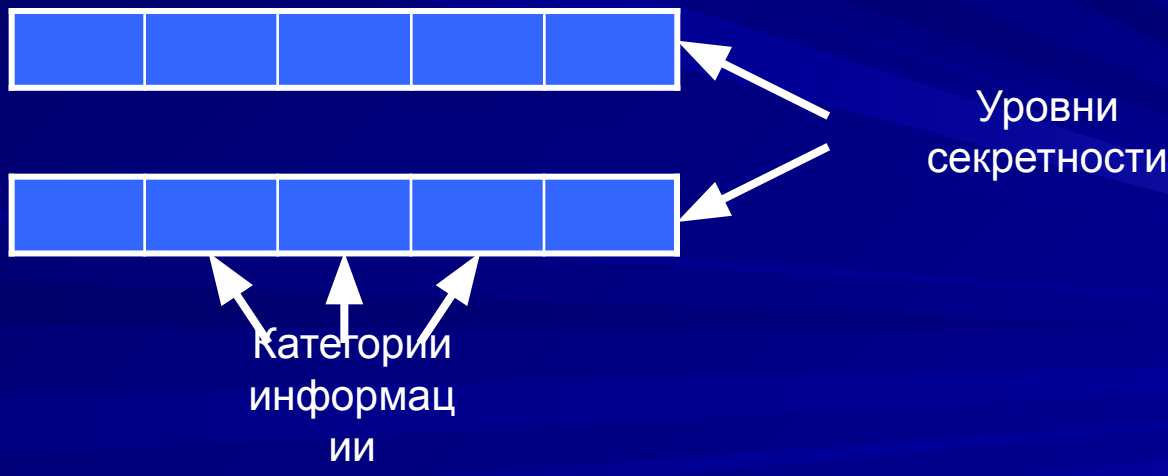
ТЕОРЕМА

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

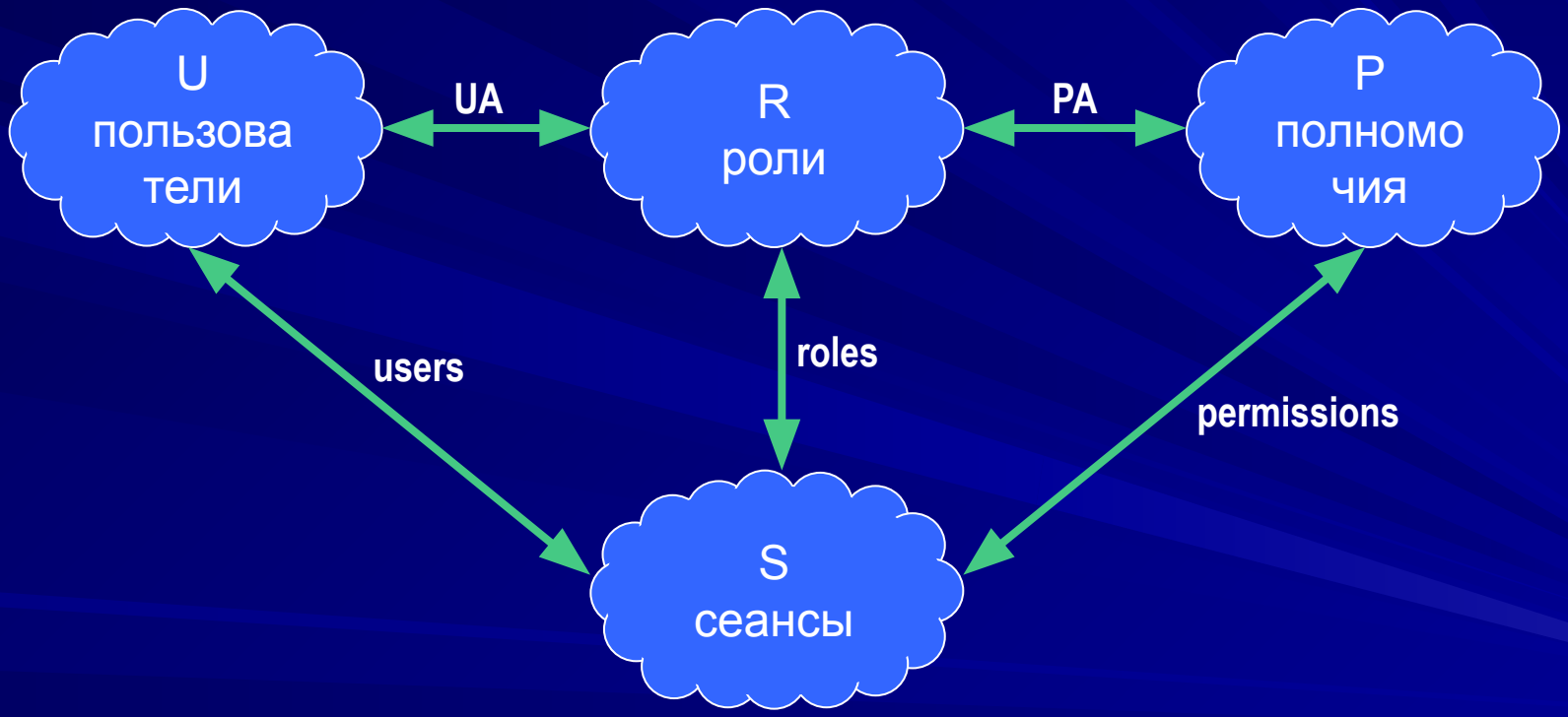
Диаграмма информационных потоков (модель Белла-ЛаПадулы Bell D.E., LaPadulla L.J.1975)



Уровни секретности и категории информации



Взаимосвязь ролей, полномочий, пользователей и сеансов



$DI \cup UDI, CDI \cap UDI = \otimes$

Модель целостности Кларка-Вилсона (Clark D.Wilson D. 1987)

S – множество субъектов;

D- множество данных;

CDI (Constrained Data Items) –данные, целостность которых контролируется;

UDI (Unconstrained Data Items) –данные, целостность которых не контролируется;

При этом: D=

TP (Transformation Procedure)- процедура преобразования, т.е. компонент, инициирующий транзакцию-последовательность операций, переводящей систему из одного состояния в другое

IVP (Integrity Verification Procedure) –процедура проверки целостности CDI

Правила модели целостности Кларка-Вилсона

1. В системе должны иметься IVP, подтверждающие целостность любого CDI.
2. Применение любой TP с любому CDI должно сохранять целостность CDI.
3. Только авторизованные TP могут вносить изменения в CDI.
4. Субъекты могут инициировать только авторизованные TP над определенными CDI (поддержка отношений вида: (s,t,d) , где s элемент S, t элемент TP, d элемент CDI).
5. Обеспечение политики разделения обязанностей: субъекты не должны изменять CDI без вовлечения в операцию других субъектов.
6. Специальные TP могут переводить UDI в CDI.
7. Каждое применение TP должно записываться в специальном CDI. При этом:

   -в CDI должен существовать запрет на изменение и удаление информации;

   -необходимо регистрировать полную информацию, достаточную для восстановления полной картины преобразований.
8. Система должна распознавать субъекты, пытавшиеся инициировать TP.
9. Тройки (s,t,d) могут модифицировать только уполномоченные субъкты.

Структура 20-разрядного счета

ББББББ-ВВВ-К-ФФФФ-НННННННН,

ББББББ- тип счета в соответствии с российским балансовым счетом

ВВВ – код валюты,

К- контрольная цифра, обеспечивающая целостность данных,

ФФФФ- номер филиала,

НННННННН- идентификатор счета

Пример расчета контрольного ключа в лицевом счете клиента кредитной организации -1

Определить значение контрольного ключа (К) в лицевом счете клиента кредитной организации 42301810X00011100005. Кредитная организация, в которой открыт лицевой счет, имеет БИК 044756882.

1. Выделяется условный номер кредитной организации - 882 (7 - 9 разряды БИК).

2. В номере лицевого счета приравнивается нулю значение контрольного ключа (К = 0) - 42301810000011100005.

3. Определяется произведение каждого разряда условного номера кредитной организации и номера лицевого счета на соответствующий весовой коэффициент по модулю 10:

Пример расчета контрольного ключа в лицевом счете клиента кредитной организации -2

882 42301 810 0 0001 1100005

713 71371 371 3 7137 1371371

686 82901 470 0 0007 1300005=67

7*3=21=1

882 42301 810 1 0001 1100005

713 71371 371 3 7137 1371371

686 82901 470 3 0007 1300005=70

0*3=0!

Этапы и технологии аутентификации

ЭТАПЫ

-идентификация

-собственно аутентификация

-авторизация

-администрирование.

ТЕХНОЛОГИИ:

-взаимная аутентификация:

система запрос-ответ

сертификаты и ЭЦП

Классификация методов аутентификации

- Основанные на знании некоторого секрета
- Основанные на использовании уникального предмета
- Основанные на использовании биометрических характеристик человека
- Основанные на информации, ассоциированной с пользователем (например, координаты, определяемые по GPS) (допустимы при совместном использовании)
- При сочетании методов говорят о многофакторной аутентификации

Классификация атак на протоколы аутентификации

-маскарад (impersonation)

-подмена стороны (interleaving attack)

-повторная передача (replay attack)

-принудительная задержка (forced delay)

-атака с перехватом данных (chosen text attack)

Методы противодействия атакам

-механизмы запрос-ответ A : X -> B: F (X) ->A ;
A: F (X) =B: F(X)

-привязка результатов к последующим действиям пользователя;

-периодическое повторение аутентификационных алгоритмов

Критерии качества аутентификации

-взаимность

-вычислительная эффективность

-коммуникационная эффективность

-наличие третьей стороны

-гарантии безопасности.

Особенности парольных методов и угрозы их безопасности

- Относительная простота реализации
- Традиционность
- Стойкие пороли малопригодны для интерактивного использования

Угрозы:

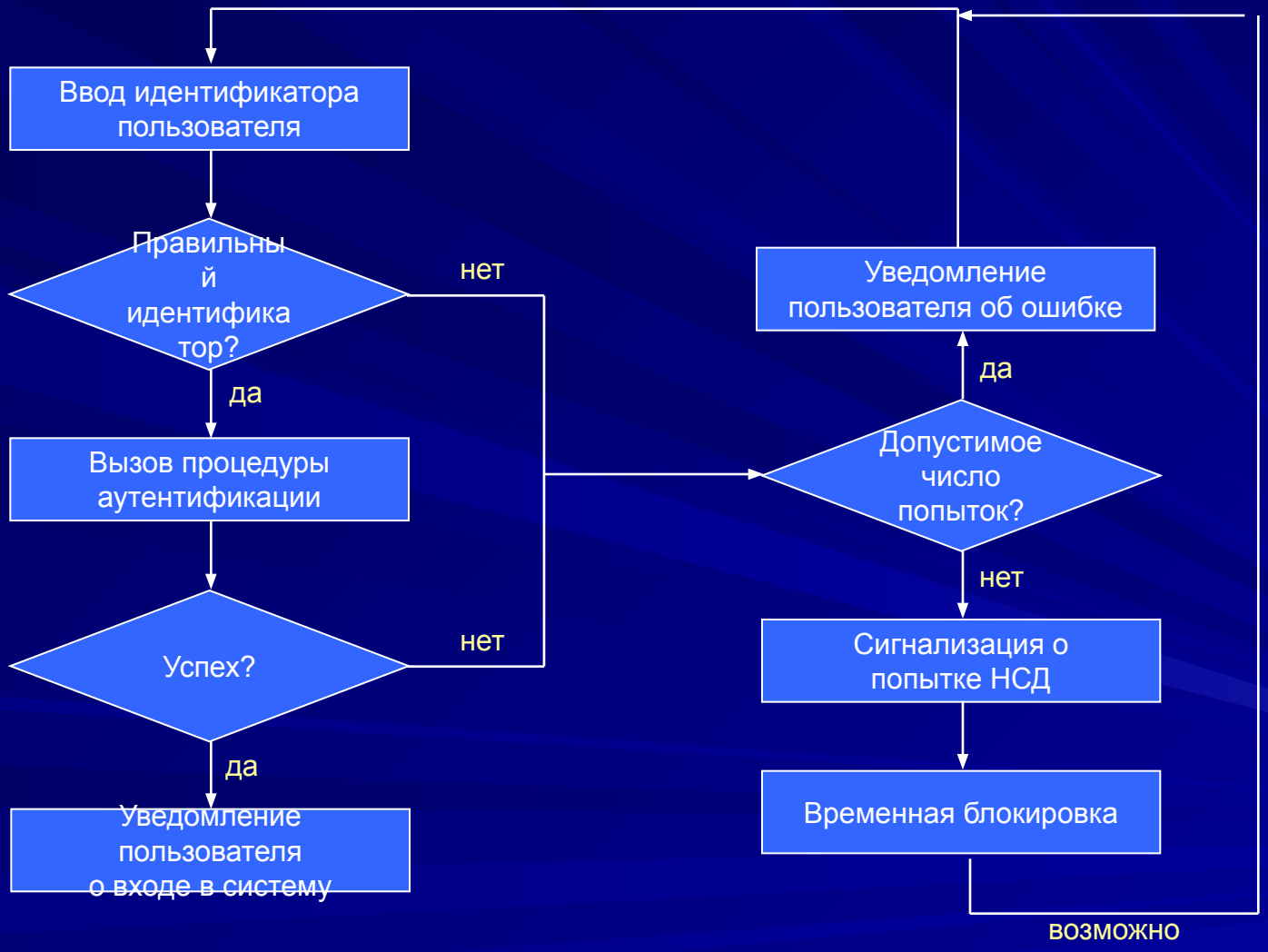
-слабости человеческого фактора;

-подбор:

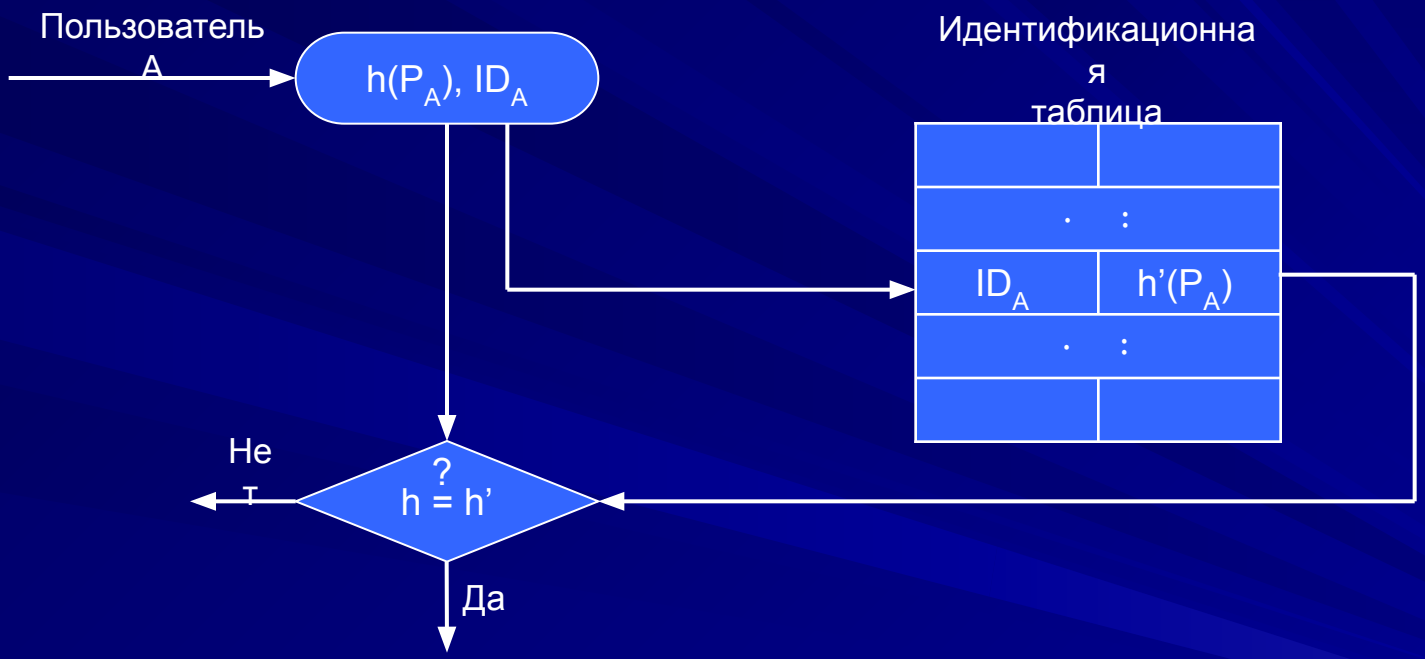
перебором, по словарю, с использованием сведений о пользователе

-недостатки реализации парольных систем (уязвимость сетевых сервисов, недекларированные возможности ПО).

Базовая схема идентификации и аутентификации на основе паролей



Использование односторонней хэш-функции для проверки пароля



Требования к хэш-функции

- может быть применена к аргументу любого размера
- выходное значение имеет фиксированный размер
- приемлемость сложности вычислительной реализации
- чувствительность к изменениям исходного текста
- однонаправленность
- вероятность совпадения для двух аргументов ничтожно мала

Классификация известных функций хэширования

- Российский стандарт ГОСТ Р34.11-94 (256 бит)
- MD (Message Digest)- семейство алгоритмов (128 бит) MD2 –наиболее медленный, MD4 – наиболее быстрый, MD5 – более безопасная модификация MD4 (используется в MS Windows для преобразования пароля пользователя в 16-байтовое число
- SHA (Secure Hash Algorithm) 160 бит

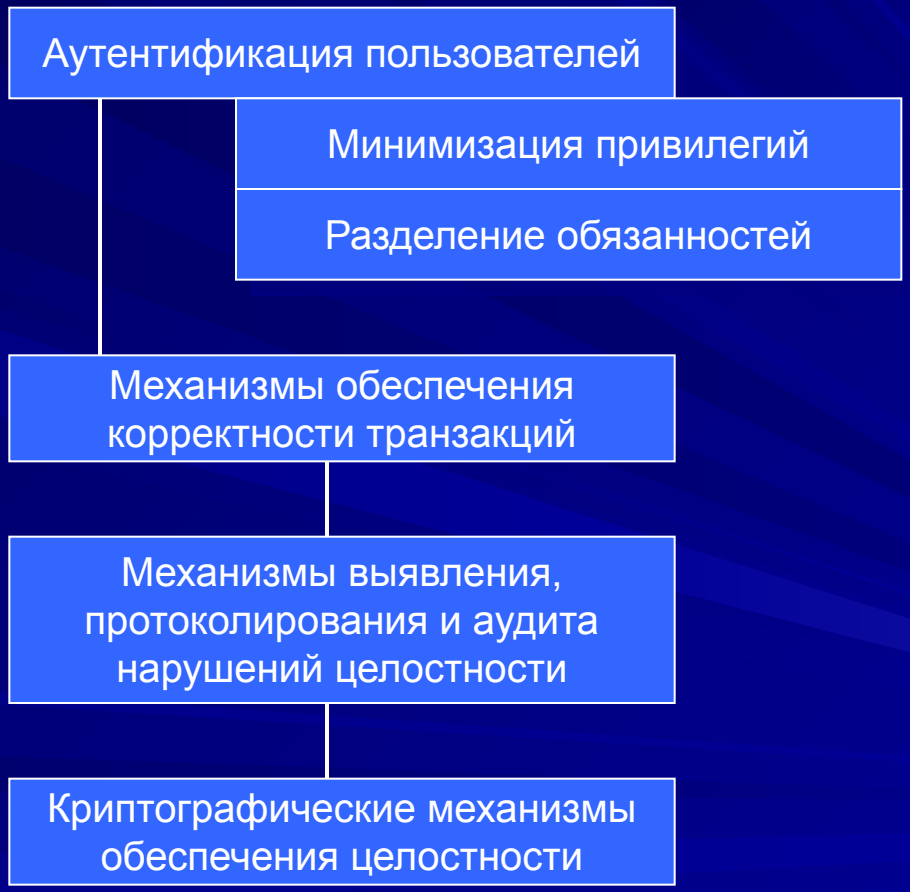
Рекомендуемые положения парольной политики

- Установление минимальной длины пароля
- Увеличение мощности алфавита
- Отбраковка словарных единиц
- Установка срока действия пароля (максимального и минимального)
- Отбраковка по журналу истории
- Ограничении числа попыток ввода
- Принудительная смена пароля при первом входе в систему
- Задержка при вводе неправильного пароля
- Автогенерация паролей

Классификация СИА по виду идентификационных признаков

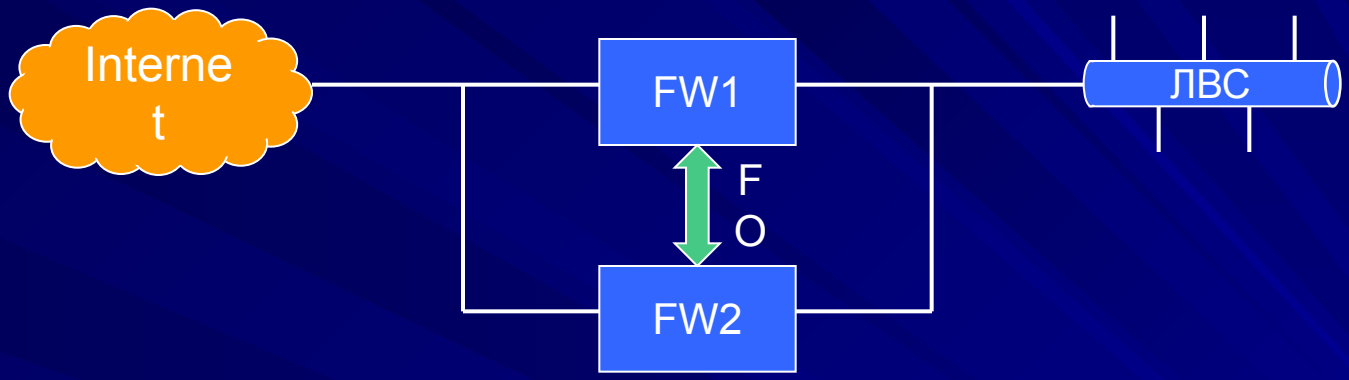
Структура системы защиты от угроз нарушения конфиденциальности информации

Структура системы защиты от угроз нарушения целостности

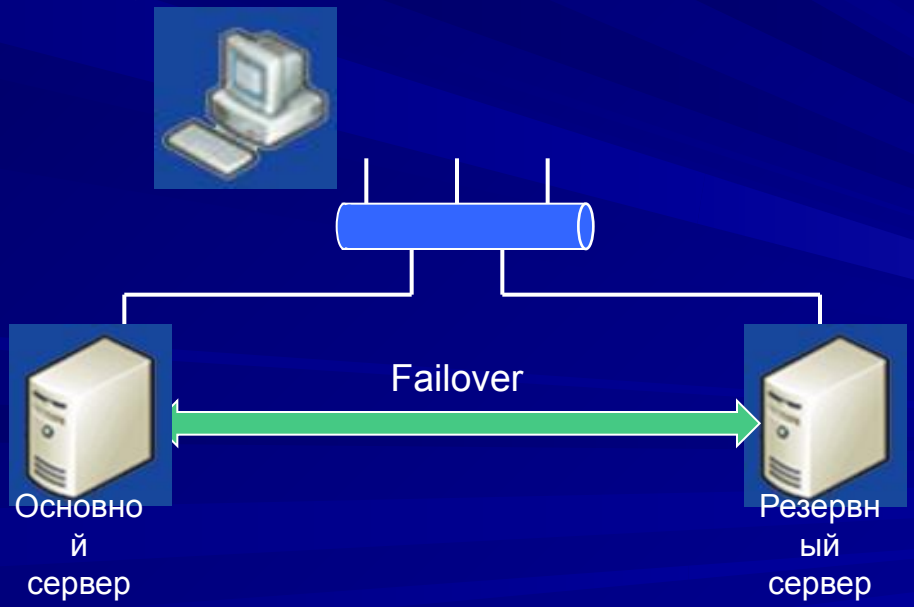


Структура системы защиты от угроз нарушения доступности

Дублирование шлюзов и межсетевых экранов



Дублирование серверов



Классификация технических сбоев и катастроф.

Уровень	Время простоя	Типичные причины	Доступность территории предприятия	Число лиц, затронутых аварией	Воздействие на предприятие
A	Не более 2 часов	Отказ нескольких рабочих станций	Да	Не более пяти	Низкое
B	Не более 8 часов	Отказ сервера, нарушение работы локальной сети	Да	Более десяти	Умеренное
C	Не более 24 часов	Затопление, длительное отключение энергии	Нет	Около 50 %	Значительное
D	Более 24 часов	Землетрясение, наводнение, пожар, террористический акт, война	Нет	Практически все сотрудники	Критическое

Предпосылки успешной разработки плана восстановления бизнеса после катастроф (Disaster Recovery Planning) (DRP)

- признание приоритетности проекта
- удачный выбор резервного офиса
- учреждение антикризисного комитета
- аудит информационно-коммуникационных ресурсов
- определение критического набора поддерживаемых бизнес-процессов
- оценка минимально возможного количества персонала

Планирование ИКТ резервного офиса

- выбор расположения резервного офиса
- формирование перечня оборудования, подлежащего резервированию
- разработка политики поддержки актуализации данных
- сценарии настройки рабочих мест пользователей
- выбор провайдеров телекоммуникационных услуг в резервном офисе

Политика поддержки актуализации данных

Базируется на классификации данных:

по степени влияния на бизнес:

-критические;

-существенные;

-некритические.

по частоте изменяемости:

-динамические;

-квазидинамические;

-статические.

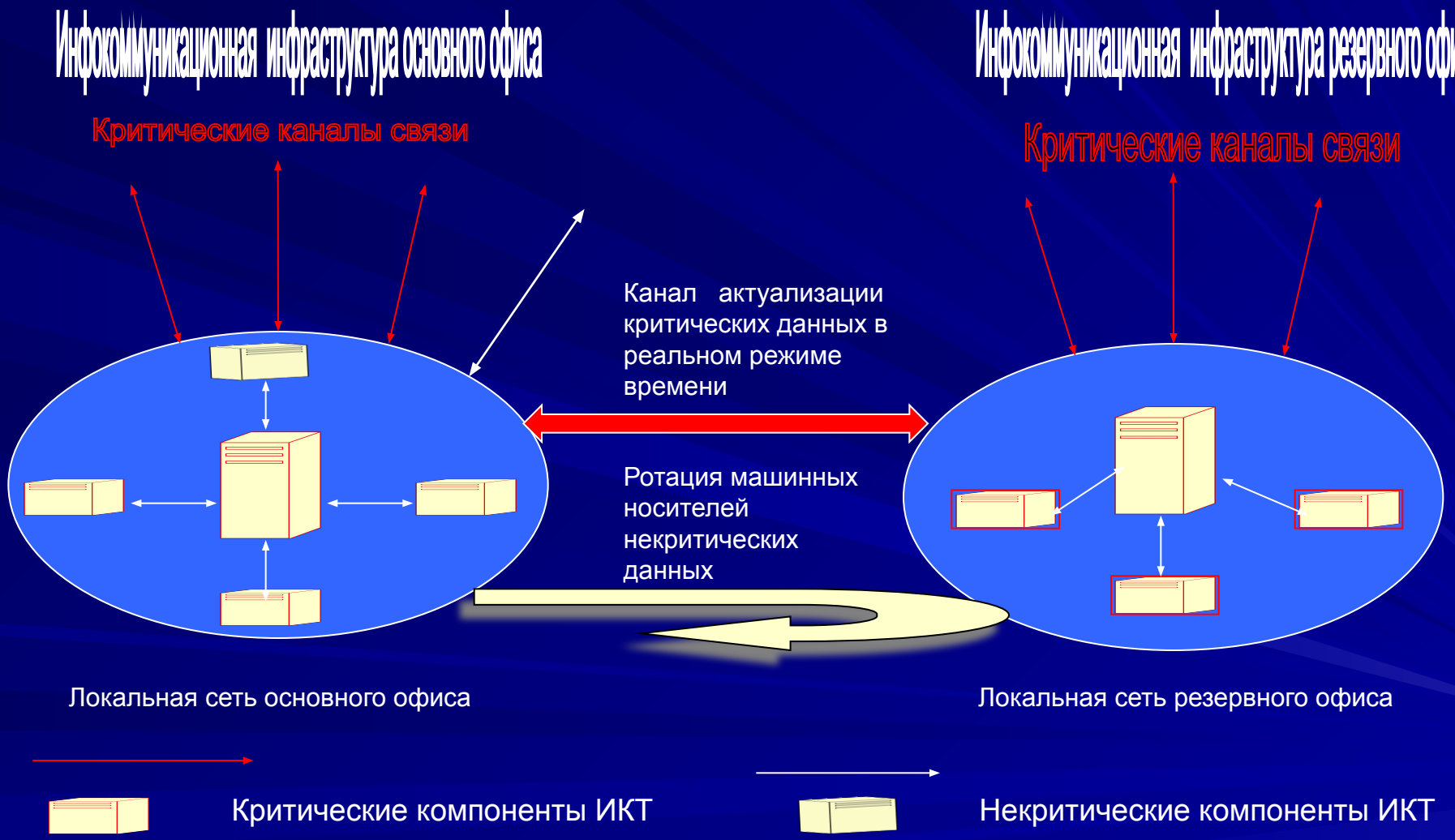
Технологии актуализации данных

для критических и существенных данных:
-в реальном режиме времени

некритических :
-создание и доставка резервных копий.

Реализации режима реального времени:
-аппаратная;
-программная.

Резервирование критических компонентов ИКТ



Документирование плана

- «дерево вызовов» (call tree);
- описание маршрута следования;
- инструкция по индивидуальной настройке рабочего места (без участия разработчиков плана);
- детальный сценарий для отдела ИТ.

Тестирование работоспособности плана

- модель деструктивного события;
- тестовые копии данных;
- категории участников тестов;
- модель «отсутствующих партнеров»;
- технологии корректного возврата.

Коэффициент качества решения:

$$K=L/(P*N),$$

где
L – число обращений в службу поддержки,
P- число тестируемых процедур,
N- число пользователей, принимавших участие в тестировании

Классификация стандартов в области ИБ

Оранжевая книга (Критерии оценки доверенных компьютерных систем/Trusted Computer System Evaluation Criteria)-1

- Политика безопасности

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

  С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для контроля процедур доступа.

- Подотчетность

  Все субъекты должны иметь уникальные идентификаторы. Контроль должен осуществляться на основании идентификации и аутентификации правил разграничения доступа.

  Для определения степени ответственности пользователя за действия в системе все происходящие в ней события должны регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него события, влияющие на безопасность.

  Протокол должен быть надежно защищен от НСД, модификации и уничтожения.

Оранжевая книга (Критерии оценки доверенных компьютерных систем/Trusted Computer System Evaluation Criteria)-2

- Гарантии

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

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

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

  А- содержит единственный класс А1;

  В- содержит классы В1,В2 и В3;

  С- содержит классы С1 и С2;

  D- содержит единственный класс D1.

  Группа D – минимальная защита (относятся системы, представленные для сертификации по требованиям одного из более высоких классов ,но не прошедшие испытания).

  Группа С – дискреционная или ролевая защита, С1 – только защита , С2 – плюс управление доступом.

Оранжевая книга (Критерии оценки доверенных компьютерных систем/Trusted Computer System Evaluation Criteria)-3

Класс С1 рассчитан но однопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиденциальности.

Класс С2 обеспечивает более избирательное управление доступом путем применения средств индивидуального контроля за действиями пользователями, регистрации, учета событий и выделением ресурсов.

Группа В –мандатная защита

Класс В1 – защита с применением меток безопасности

Класс В2 – структурированная защита с ядром безопасности, поддерживающем определенную и четко структурированную модель безопасности. Должен осуществлять контроль скрытых каналов передачи информации.

Класс В3 – домены безопасности: ядро поддерживает монитор безопасности, который контролирует все типы доступа и который невозможно обойти. Средства аудита включает механизмы оповещения администратора о события, имеющих отношение в безопасности. Необходимо наличие средств восстановления работоспособности системы.

Группа А –верифицированная защита (формальные методы верификации корректности механизмов управления доступом и систем защиты.

Руководящие документы Гостехкомиссии России (в настоящее время Федеральная Служба Технического и Экспортного Контроля)

- Защита от НСД. Термины и определения
- Концепция защиты средств СВТ и АС от НСД
- АС. Защита от НСД к информации
- СВТ. Защита от НСД к информации. Показатели защищенности от НСД.
- СВТ. Межсетевые экраны. Защита от НСД. Показатели защищенности
- Защита от НСД. Программное обеспечение средств защиты информации. Классификация по уровню недекларированных возможностей.

Руководящие документы Гостехкомиссии России Основные положения концепции защиты средств СВТ и АС от НСД –Определения и способы

- Под НСД понимается доступ к информации, нарушающий установленные правила доступа, с использованием штатных средств, предоставляемых СВТ или АС
- Основные способы НСД:

  -непосредственное обращение в объектам доступа;

  -создание программных и аппаратных средств, выполняющих обращение в обход средств защиты;

  -модификация средств защиты;

  -внедрение программных и аппаратных механизмов, нарушающих структуру и функции СВТ или АС.

Руководящие документы Гостехкомиссии России Основные положения концепции защиты средств СВТ и АС от НСД –Принципы защиты

- Принципы защиты от НСД

-защита основывается на положениях и требованиях соответствующих законов, стандартов и нормативных документов;

-защита СВТ и АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер;

-защита СВТ и АС должна обеспечиваться на всех стадиях жизненного цикла, в том числе и при проведении ремонтных и регламентных работ;

-программно-технические средства защиты не должны существенно ухудшать функциональные характеристики АС;

-неотъемлемой частью работ по защите является оценка эффективности средств защиты

-защита АС должна предусматривать контроль эффективности, который может быть либо периодическим, либо инициироваться проверяющими органами.

Руководящие документы Гостехкомиссии России Основные положения концепции защиты средств СВТ и АС от НСД – Классификация нарушителей

- Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ:

  -возможность ведения диалога в АС;

  -возможность создания и запуска собственных программ;

  -возможность управления функционированием АС, т.е. воздействие на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования;

  -полный объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения с состав СВТ собственных технических средств с новыми функциями по обработке информации.

Недостатки стандартов ИБ первого поколения

- Документы ориентированы на обеспечение защиты от нарушения конфиденциальности и, в определенной степени целостности. Угрозы нарушения доступности не рассматриваются.
- Используемый «табличный» подход не позволяет учесть специфику конкретных продуктов и систем. В РД Гостехкомиссии отсутствует понятие политики безопасности.
- Документы содержат перечень механизмов, наличие которых необходимо для отнесения СВТ или АС с тому или иному классу защищенности. Не формализованы методы проверки корректности и адекватности реализации функциональных требований.
- Формулировки ряда требований допускают неоднозначную интерпретацию

Стандарт ISO/IEC 15408-1999 “Common Criteria for Information Technology Security Evaluation” (ГОСТ Р ИСО/МЭК 15408-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ» (Общие критерии (ОК)

- Введение и общая модель
- Функциональные требования безопасности
- Требования доверия к безопасности

Введен в действие в РФ с 01.01.2004.

Основное свойство максимально возможная универсальность: под **объектом оценки (ОО)** понимается произвольный продукт ИТ или система и руководствами администратора и пользователя. **Продукт** рассматривается как совокупность программно-аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в состав различных систем. **Система** – это специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Категории пользователей и среда безопасности в ОК

- Категории пользователей:
  -потребители
  -разработчики
  -оценщики
  Объект оценки рассматривается в контексте т.н. среды безопасности:

-законодательная среда;

-административная среда;

-процедурная среда;

-программно-техническая среда.

Аспекты среды ОО

- Предположения безопасности
- Угрозы безопасности
- Политика безопасности
- Требования безопасности

-функциональные требования

-требования доверия.

При формулировании требований возможна разработка двух документов:

Профиль защиты (ПЗ)

Задание на безопасность (ЗБ)

Ограничения стандарта ОК

- Не содержит критериев оценки, касающихся администрирования механизмов безопасности, не относящимся к ИТ (управление персоналом, физическая безопасность). Эти аспекты могут рассматривать как предположения безопасности.
- Контроль ПЭМИН не затрагивается
- Использование результатов оценки при аттестации продуктов и систем находятся вне области действия ОК
- Не входят критерии оценки специфических свойств криптографических алгоритмов. Должны выполняться как самостоятельная процедура
- Не рассмотрена ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки.