**КОНСПЕКТ ЛЕКЦИЙ ПО ТОКБ**

[**Лекция №1. Нормативно-правовая база обеспечения ИБ в РФ** 2](#_Toc123181570)

[**Лекция №2. Обеспечение информационной безопасности** 6](#_Toc123181571)

[**Лекция №3. Угрозы ИБ** 11](#_Toc123181572)

[**Лекция №4. Вспомогательные структуры (модели), используемые в защите информации. Ценность информации** 16](#_Toc123181573)

[**Лекция №5. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO). Информационный поток** 19](#_Toc123181574)

[**Лекция №6. Угрозы информации** 22](#_Toc123181575)

[**Лекция №7. Политика безопасности. Модели безопасности** 23](#_Toc123181576)

[**Лекция №8. Вероятностные модели на основе анализа угроз системе. Политика MLS** 28](#_Toc123181577)

[**Лекция №9. Модели мандатного доступа** 31](#_Toc123181578)

[**Лекция №10. Модели** 37](#_Toc123181579)

# **Лекция №1. Нормативно-правовая база обеспечения ИБ в РФ**

* ФЗ №149 «Об информации, информационных технологиях и о защите информации»
  + Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

* ФЗ №390 «О безопасности»
  + ФЗ-390 регулирует принципы обеспечения безопасности:
    - личной;
    - общественной;
    - государственной;
    - экологической;
    - национальной.
  + **Основными принципами обеспечения безопасности** являются:
  1. соблюдение и защита прав и свобод человека и гражданина;
  2. законность;
  3. системность и комплексность применения федеральными органами государственной власти и тд. политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;
  4. приоритет предупредительных мер в целях обеспечения безопасности;
  5. взаимодействие федеральных органов государственной власти и т.д. с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.
* Закон РФ №5485 «О государственной тайне»
  + Положения настоящего Закона обязательны для исполнения на территории Российской Федерации и за ее пределами.
  + В этом законе используется ряд основных понятий:
    - **Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
    1. сведения в военной области;
    2. сведения в области экономики, науки и техники;
    3. сведения в области внешней политики и экономики;
    4. сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.
    - Не подлежат отнесению к государственной тайне сведения (общедоступная информация):

1. о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
2. о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
3. о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
4. о фактах нарушения прав и свобод человека и гражданина;
5. о размерах золотого запаса и государственных валютных резервах Российской Федерации;
6. о состоянии здоровья высших должностных лиц Российской Федерации;
7. о фактах нарушения законности органами государственной власти и их должностными лицами.
   * + **Средства защиты информации** – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.
     + Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "**особой важности**", "**совершенно секретно**" и "**секретно**".



|  |  |  |  |
| --- | --- | --- | --- |
| Природные  Техногенные  Общественные  Экономические | Эконом. Сфера  Внутриполитическая  Социальная  Международная  Информационная  Военная  Пограничная  Экологическая | Внутренние  Внешние | Целостности  Доступности  Конфиденциальности |

Главными составляющими информации являются: Конфиденциальность, Целостность, Доступность. Поэтому обеспечение безопасности складывается из этих трех главных составляющих информации.

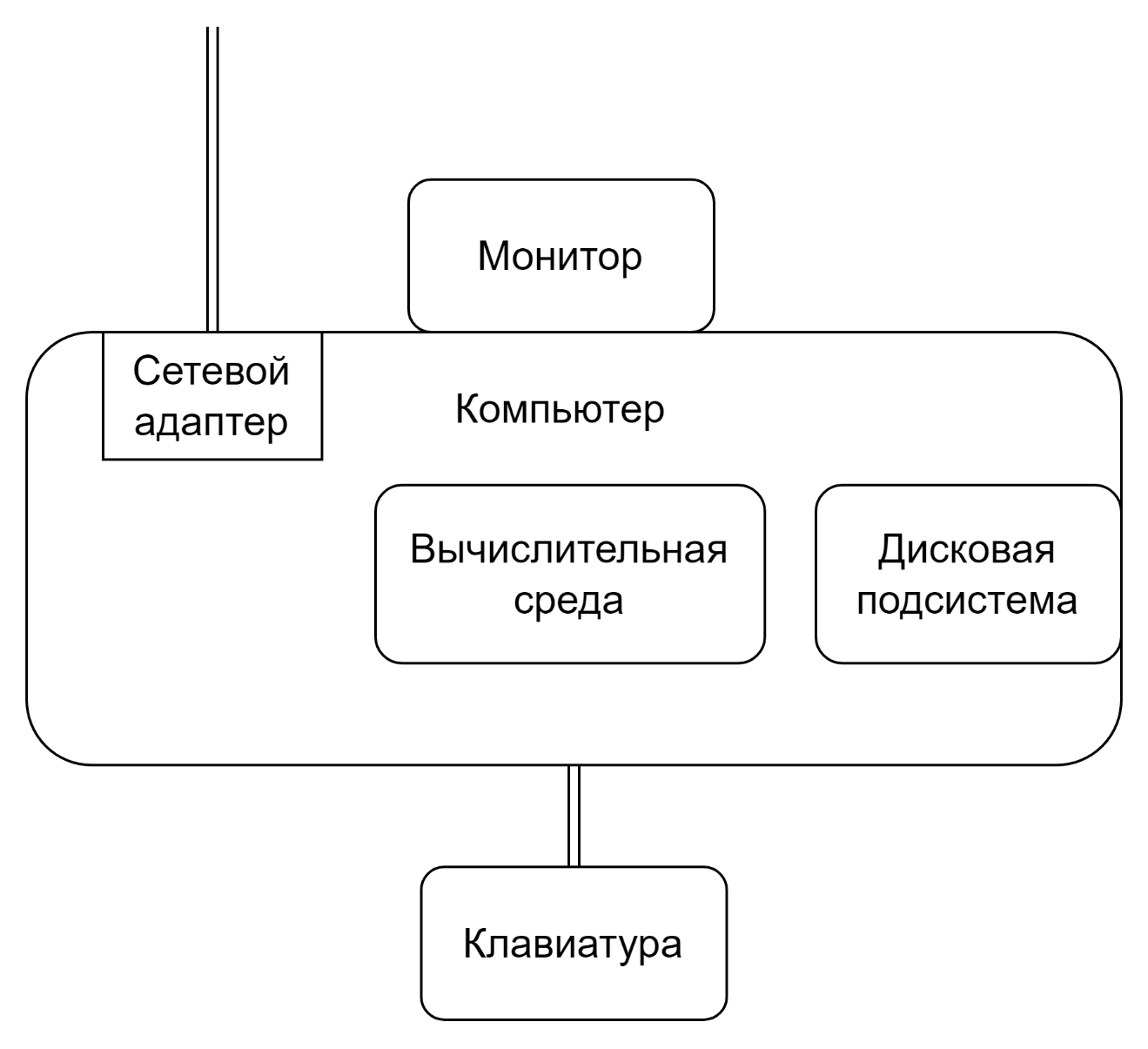
Точками взаимодействия процесса ЗИ и ИС являются:

* Аппаратное обеспечение,
* ПО
* Обеспечение связи(коммуникации).

Механизмы Защиты разделяются на несколько уровней:

* Физический
* Персонал
* Организационный

# **Лекция №2. Обеспечение информационной безопасности**



**Интегральный показатель защищенности информации**

* В общем случае интегральный показатель защищенности информации **Z**  определяется в виде:

Где ***K***– показатель полноты учета возможных стратегий нападения, на противостояние которым нацелено СЗИ при ее разработке

***R*** – показатель эффективности применения конструктивно заложенных в СЗИ стратегий защиты информации на интервале от *0* до *t*.

* Если известно распределение вероятностей применения СИН всех стратегий нападения, то возможна трактовка показателя учета стратегий нападений ***K***:

, n > k

* Где n – это количество стратегий нападения, учитываемых в данной СЗИ.

**Выделяют  и другие категории модели безопасности:**

* неотказуемость или апеллируемость — невозможность отказа от авторства;
* подотчётность  — обеспечение идентификации

субъекта доступа и  регистрации его  действий;

* достоверность — свойство соответствия

предусмотренному поведению или  результату;

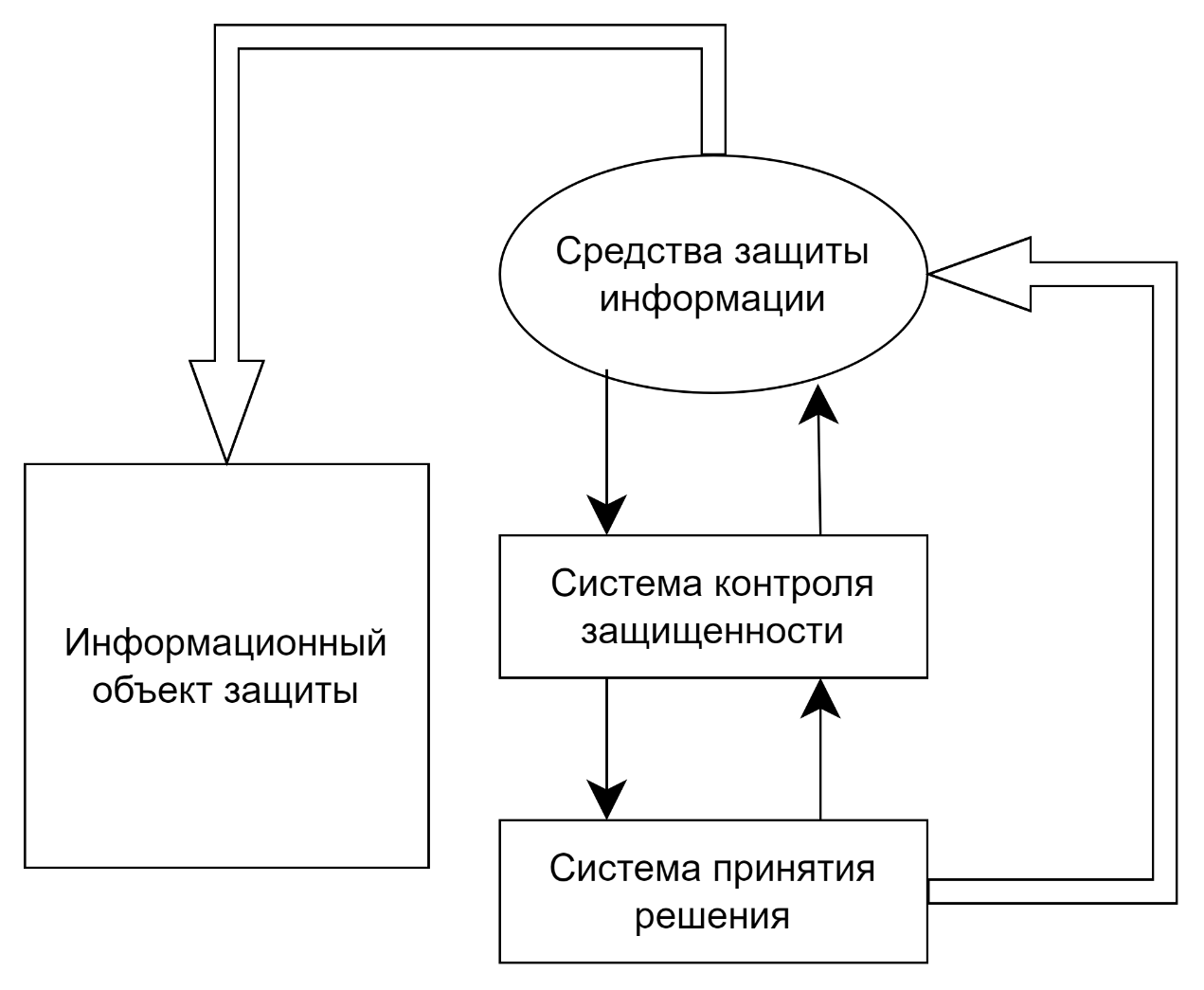
* аутентичность или подлинность — свойство,

гарантирующее, что субъект  или  ресурс идентичны  заявленным.

Основным *содержанием* обеспечения ИБ должна являться работа по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации:

* прогнозирование (выявление) угроз ИБ;
* защита информационных объектов;
* комплексное противодействие угрозам ИБ;
* целенаправленное воздействие на объекты, представляющие угрозу ИБ.

**Контур управления ЗИ**

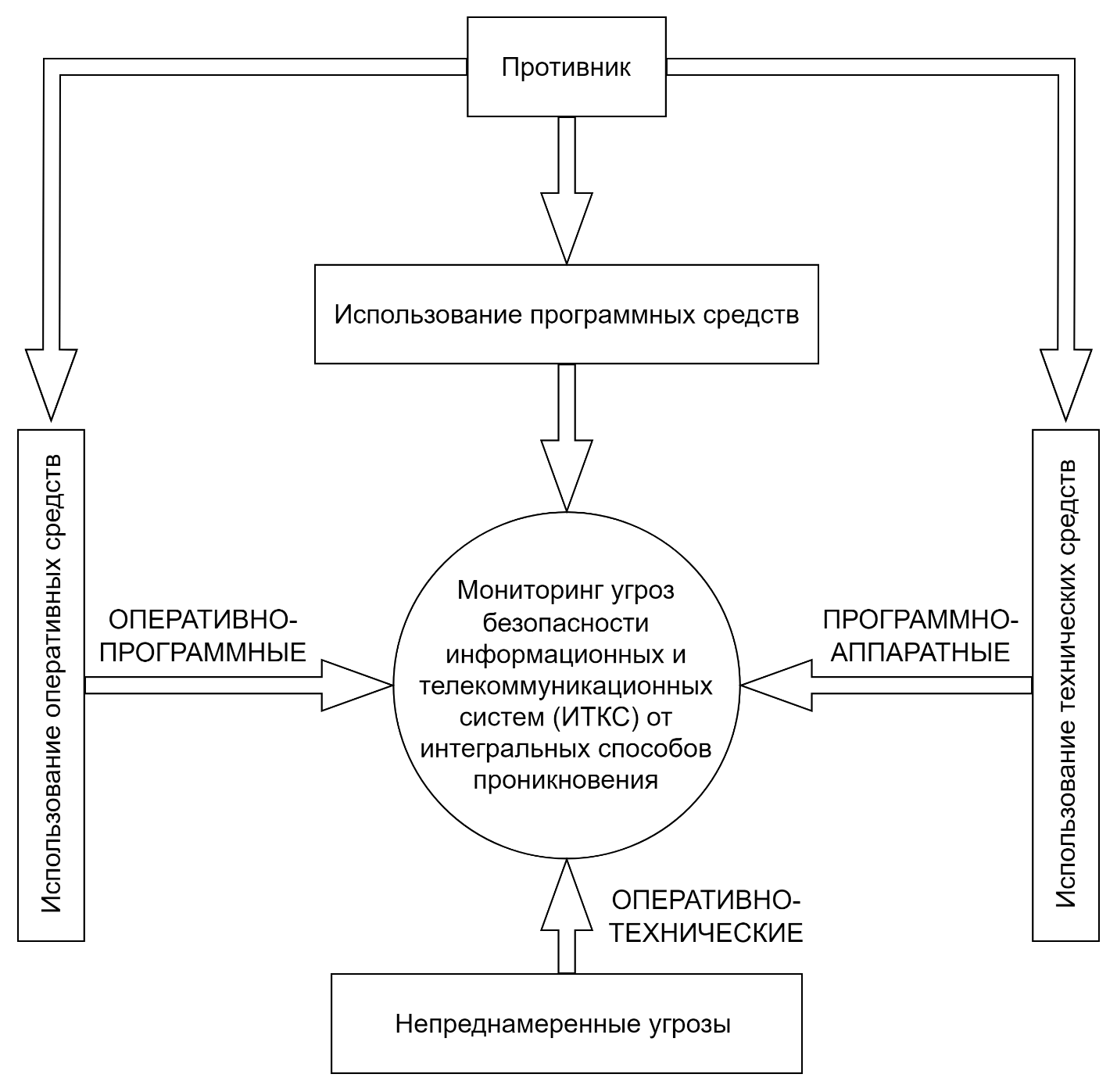


**Обобщенная модель мониторинга угроз**

Цели противника:

* добыча информации
* искажение информации
* замена информации
* внесение информации
* уничтожение информации
* полное нарушение функционирования ИТКС

Для достижения своих целей противник использует различные способы достижениях этих целей



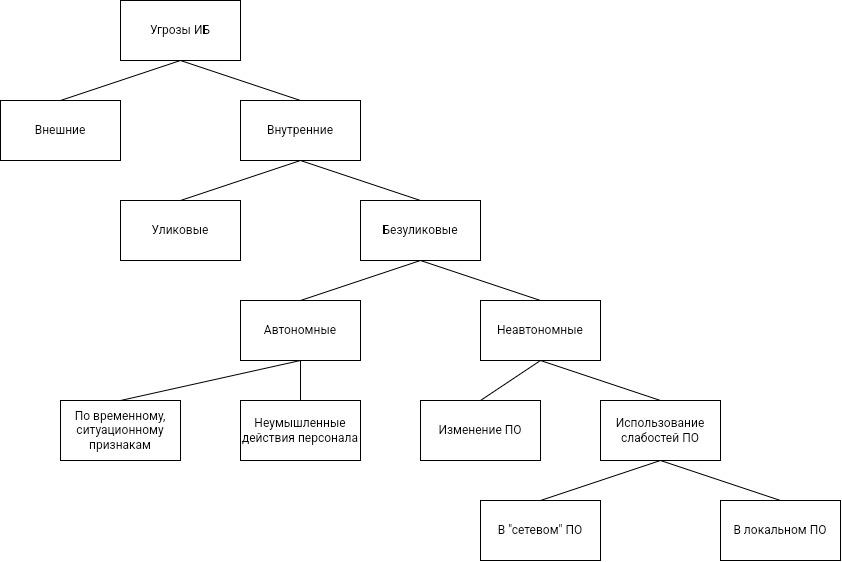
|  |  |
| --- | --- |
| **Использование программных средств** | |
| Несанкционированный доступ в ИТКС | Внедрение программных закладок и компьютерных вирусов |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Непреднамеренные угрозы** | | | | |
| Природные катаклизмы | Ошибки операторов | Ошибки программистов | Ошибки инженерно-технического персонала | Ошибки и отказы аппаратно-программного средств |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Использование оперативных средств** | | | | | | | | | |
| **Обслуживающий персонал ИТКС** | | | | **Пользователи ИТКС** | | **Сотрудники спецслужб противника** | | | |
| Внесение изменений в программы | Нарушение работы технических средств | Использование «в темную», копирование | Копирование программ и информации | | Внедрение технических и программных закладок (вирусов) | | Террористические акты | Физическое уничтожение программ и оборудования | Хищение носителей информации |

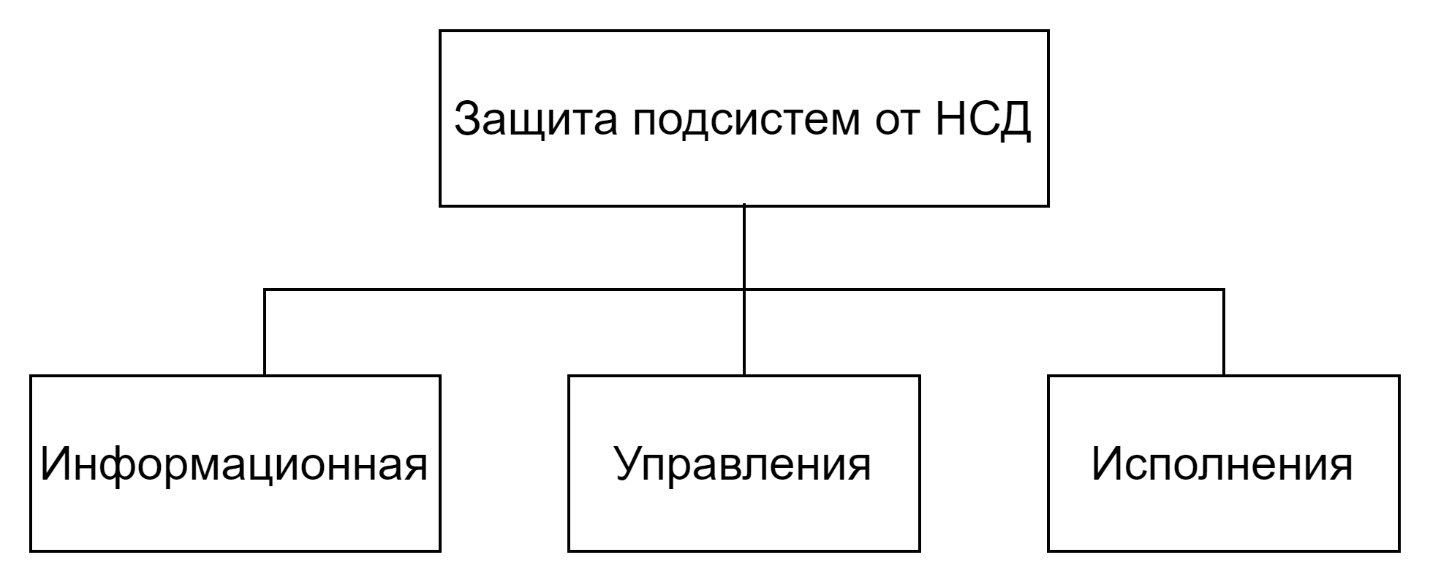
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Использование технических средств** | | | | | | | | | |
| **Энергетическое воздействие** | | | | **П-перехват** | | | **А-перехват** | | |
| Облучение электромагнитными полями | Воздействие по сети электропитания и заземления | Телевидеонаблюдение | Виброакустические каналы | | Радиоперехват | От технических закладок | | Облучение технических средств электромагнитными полями | От управляемых технических закладок |

# **Лекция №3.** **Угрозы ИБ**

****

Внешние угрозы:

* Гарантирования шифрование
* Имитозащита, ЭЦП
* Защита ключевой структуры
* Защита от электромагнитных каналов утечки (ПЭМИН)
* Защита от ИО (РИВ и вирусов)
* Система регистрации сообщений и действий, контроль доступа
* Построение защищенных ВОЛС
* Использование МСЭ(Firewalls)
* Передача ключей с использованием квантовой криптографии



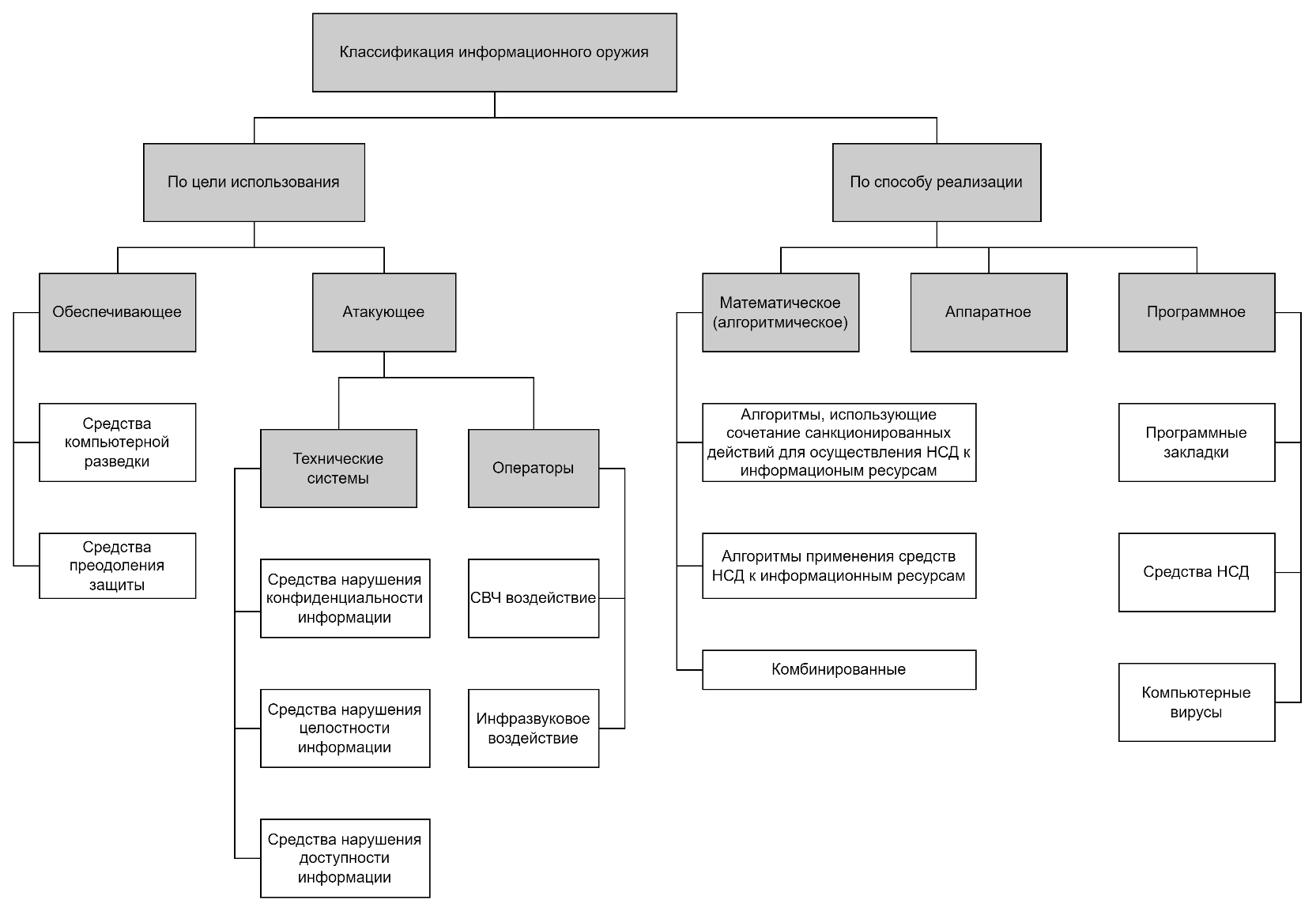
Внутренние угрозы:

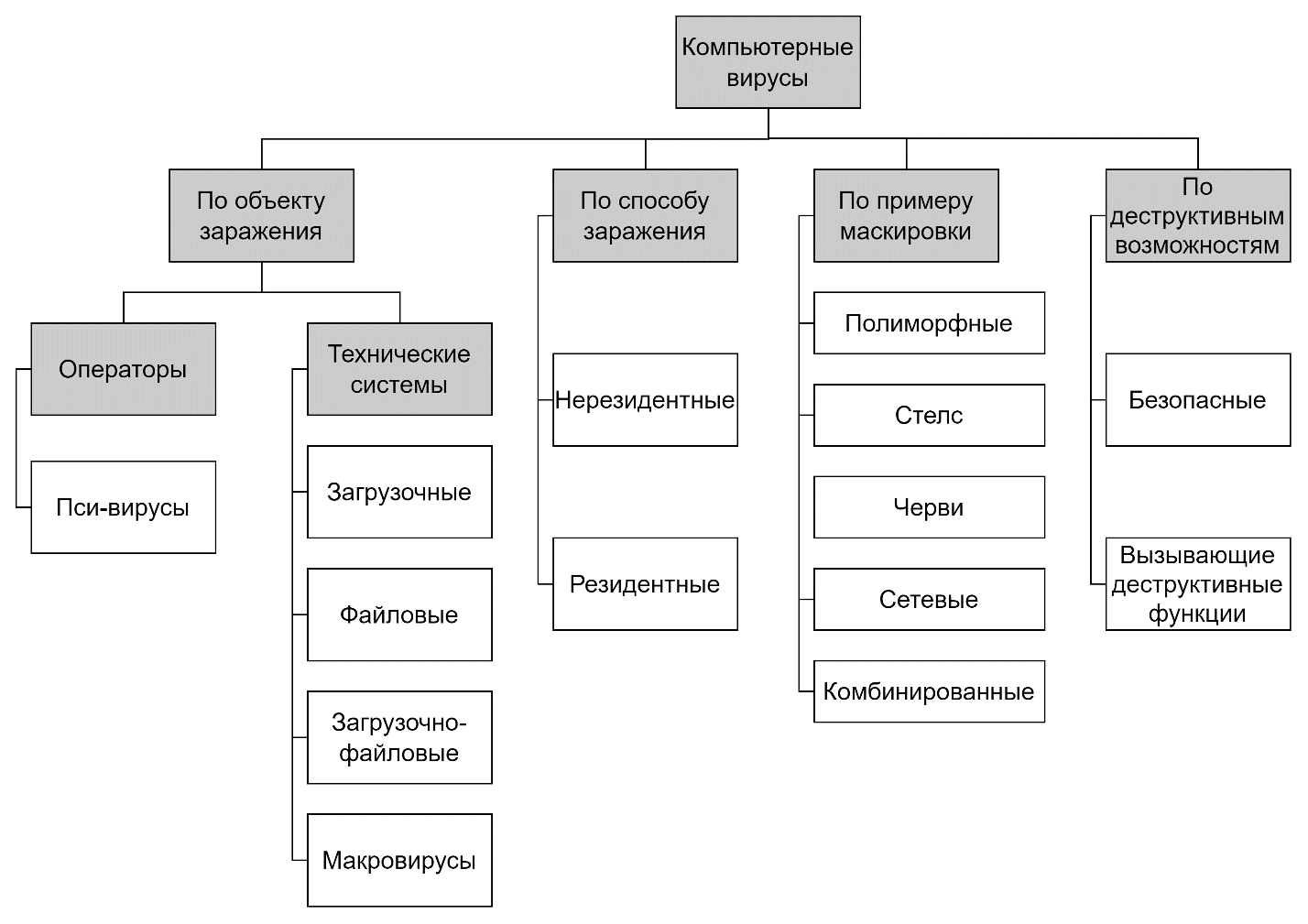
* Специсследования и спецпроверки
* Тестовые исследования на стендах
* Абонентское шифрование
* Замыкание операционной среды
* Комплекс мер по защите от НСД и информационного оружия

Комплекс мер по защите от НСД и информационного оружия:

* Windows NT UNIX
* Создание FIREWALL
* Защита ЦАТС
* Поиск вирусоподобных вставок
* Защита видеоконференций
* TCP/IP, NTERNET
* Защита ORACLE

|  |  |
| --- | --- |
| **Требования** | **Функция защиты от НСД** |
| 1. Идентификация и аутентификация пользователей | Используется при проверке подлинности и осуществлении контроля доступа субъектов:   * К ЭВМ * К узлам сети ЭВМ * К каналам связи * К внешним устройствам ЭВМ * К процессам * В систему * К информации |
| 2. Шифрование информации | Обеспечивает:   * Защиту конфиденциальности информации * Разграничение доступа субъектов к информационным объектам |
| 3. Регистрация и учет | Используется для контроля:   * Входа (выхода) субъектов в (из) системы * Доступа субъектов к аппаратным ресурсам системы * Доступа субъектов к информационным объектам и процессам * Попыток нарушения защиты |

****

****

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Классы информационного оружия** | | | |
|  | **Персонального поражения** | **Группового поражения** | **Массового поражения** | **Глобального поражения** |
| **Индивидуальное и общественное сознание** | Человек | * Исполнительные органы власти * Представительные органы власти * Судебные органы власти * Политические движения и партии * Профсоюзы * Соц группы * Возратсные группы | Население страны | Инфосфера человечества |
| **Технические средства** | * ЭВМ * Терминалы * Рабочие станции * АРМы * Телефонные аппараты * Телеграфные аппараты * Факсимильные аппараты * Модемы | * Вычислительные центры * Центры коммутации и маршрутизации сообщений * СУБД * Хосты * Браузеры * Серверы | Федеральные и ведомственные вычислительные сети  Ситуационные центры администрации президента  Сети коммерческой, банковской и деловой связи | Глобальные сети:   * INTERNET * Система глобальной подвижной персональной спутниковой связи «Iridium» * Система глобальной подвижной персональной спутниковой связи «Globalstar» * Глобальный информационный супертракт (GIG) |

# **Лекция №4. Вспомогательные структуры (модели), используемые в защите информации. Ценность информации**

**Опр.** Объектом относительно языка Я (или просто объектом) называется произвольное конечное множество языка Я.

**Опр.**Ресурсы системы, выделяемые для действия преобразования, называются доменом.

**Опр.**Преобразование, которому передано управление, называется процессом.

**Опр.**Объект, описывающий преобразование, которому выделен домен и передано управление, называется субъектом.

Основные примеры доступов субъекта S к объекту O:

1. Доступ на чтение (r) данных.

При этом доступе данные считываются в объекте О и используются в качестве параметра в субъекте S.

2. Доступ на запись (w) данных.

При этом доступе некоторые данные процесса *S* записываются в объект О. Здесь возможно стирание предыдущей информации.

3. Доступ на активизацию процесса, записанного в О как данные (ехе).

При этом доступе формируется некоторый домен для преобразования, описанного в О, и передается управление соответствующей программе.

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

Главная сложность защиты информации может быть описана так:

Когда имеется возможность использовать набор местных ограничений на доступ в каждый момент времени, должна быть решена глобальная проблема недопуска выхода любой возможной траектории в неблагоприятное множество N. При этом траектории множества N не обязательно являются ограничениями на доступы конкретных субъектов к конкретным объектам.

**Аддитивная модель**

Пусть информация – конечное множество элементов. Тогда необходимо оценить суммарную стоимость в денежных единицах из оценок компонент.

Оценка строится:

* на основе экспертных оценок компонент,
* если денежные оценки объективны,

то сумма дает искомую величину.

Однако, количественная оценка компонент не всегда объективна: это связано с неоднородностью компонент в целом. Поэтому делают единую иерархическую относительную шкалу (линейный порядок, который позволяет сравнивать отдельные компоненты по ценности относительно друг друга).

**Анализ риска**

Пусть в рамках аддитивной модели проведен учет стоимости информации в системе. Оценка возможных потерь строится на основе полученных стоимостей компонент, исходя из прогноза возможных угроз этим компонентам. Возможности угроз оцениваются вероятностями соответствующих событий, а потери подсчитываются как сумма математических ожиданий потерь для компонент по распределению возможных угроз.

**Модель решетки ценностей**

Обобщением порядковой шкалы является модель решетки.

Пусть дано SC - конечное частично упорядоченное множество относительно бинарного отношения <, т.е. для каждых А, В, С выполняется

1) рефлексивность: А<А,

2) транзитивность: А<В, В<С==>А<С,

3) антисимметричность: А<В, В<А => А=В.

**Опр.**Для А, B∈SC элемент C=A⊕B∈SC называется наименьшей верхней границей (верхней гранью), если

1) А<С, В<С;

2) A<D, B<D⇒C<D для всех D∈SC.

**Опр.**Для А, B∈C элемент E=A⊗B∈SC называется наибольшей нижней границей (нижней гранью), если

1) Е<А, Е<В;

2) D<A, D<B⇒D<E.

**Опр.**(SC, <) называется решеткой, если для любых А, B∈SC существует A⊕B∈SC и A⊗B∈SC.

**Лемма.** Для любого набора S={А1,...,Аn} элементов из решетки SC существуют единственные элементы,:

⊕S=A1⊕...⊕An - наименьшая верхняя граница S;

⊗S=A1⊗...⊗An - наибольшая нижняя граница S.

**Опр.**Конечная линейная решетка - это линейно упорядоченное множество, можно всегда считать {0, 1 ,..., n}=SC .

**MLS решетка**

Название происходит от аббревиатуры Multilevel Security и лежит в основе государственных стандартов оценки информации.

Решетка строится как прямое произведение линейной решетки L и решетки SC подмножеств множества X, т.е. (α,β), (α’,β’) - элементы произведения, β,β’∈L - линейная решетка, α,α’∈SC - решетка подмножеств некоторого множества X. Тогда

(α,β)<(α’,β’)⇔α⊆α’,β<β’

Верхняя и нижняя границы определяются следующим образом:

(α,β)⊕(α′,β′)⇔(α∪α′,max{β,β’}),

(α,β)⊗(α′,β′)⇔(α∩α′,min{β,β’}).

# **Лекция №5. Иерархические модели и модель взаимодействия открытых систем (OSI/ISO). Информационный поток**

**Универсальные принципы описания иерархического метода**

Предположим, что сложная система А адекватно описана на языке Я. Предположим, что мы провели разложение языка Я на семейство языков D1,D2,...,Dn. Если язык Di, i=2,.., n, синтаксически зависит только от словоформ языка Di-1, то будем говорить, что они образуют два соседних уровня. Тогда система А может быть описана наборами слов B1,...,Bn в языках D1,D2,...,Dn причем так, что описание Вi синтаксически может зависеть только от набора Вi-1. В этом случае будем говорить об иерархической декомпозиции системы A и уровнях декомпозиции B1,...,Bn , где уровень Вi непосредственно зависит от Bi-1. Рассмотрим ряд простейших примеров иерархического построения сложных систем.

**Влияние угроз на свойства информации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Угроза** | **Конфиденциальность** | **Целостность** | **Доступность** |
| Аппаратные сбои | + | + | + |
| Блокировка информации (препятствование использованию - denial of use) |  |  | + |
| Вирусы |  | + | + |
| Диверсии |  | + | + |
| Излучения | + |  |  |
| Использование сетевых анализаторов | + |  |  |
| Кража | + | + | + |
| Логические бомбы | + | + | + |
| Модификация | + |  |  |
| Маскарад |  | + |  |
| Ошибки в работе персонала | + | + | + |
| Ошибки в маршрутизации | + |  |  |
| Ошибки программирования | + | + | + |
| Остаточная информация | + |  |  |
| Перегрузка |  |  | + |
| Перехват | + |  |  |
| Пиггибекинг (piggybacking) | + | + | + |
| Пожары и стихийные бедствия |  | + | + |
| Самозванство (impersonation) | + | + | + |
| Скрытые возможности в ПО и архитектуре системы | + | + | + |
| Супперзаппинг (superzapping) | + | + | + |
| Существование различных версий программ и данных |  | + |  |
| Троянские программы | + | + | + |
| Умышленное повреждение данных или программ |  | + |  |

**Информационный поток**

1. Пусть субъект S осуществляет доступ на чтение (r) к объекту О. В этом случае говорят об информационном потоке от О к S. Здесь объект О является источником, а S - получателем информации.

2. Пусть субъект S осуществляет доступ на запись (w) к объекту О. В этом случае говорят об информационном потоке от S к О. Здесь объект О является получателем, а S - источником информации.

Из простейших потоков можно построить сложные.

С точки зрения защиты информации, каналы и информационные потоки бывают:

* законными
* незаконными – создают утечку информации и могут нарушать секретность данных.

Если незаконный канал нельзя полностью перекрыть, то доля количества информации в объекте, утекающая по этому каналу, служит мерой опасности этого канала.

Будем считать, что всю информацию о вычислительной системе можно описать конечным множеством объектов (каждый объект - это конечное множество слов в некотором языке ***Я****).* В каждом объекте выделено состояние, а совокупность состояний объектов назовем состоянием системы.

Функция системы - это последовательное преобразование информации в системе под действием команд.

В результате, из состояния s мы под действием команды α перейдем в состояние s'.

**Опр.**Выполнение команды α в состоянии s, переводящей состояние s в s', вызывает информационный поток от X к Y (обозначение Х-->αY ), если I(Х, Y)>0. Величина I(Х, Y) называется величиной потока информации от X к Y.

**Опр.** Для объектов X и Y существует информационный поток величины С (бит), если существуют состояния s и s' и последовательность команд α такие, что s|-- s'(α), X-->αY.

Оценка максимального информационного потока определяется пропускной способностью канала связи Х→αY и равна по величине

C(α, X, Y) = max I(X, Y).

# **Лекция №6. Угрозы информации**

**Угрозы нарушения секретности в ЭСОД и механизмы их предотвращения**

Два пути нарушения секретности:

* утрата контроля над системой защиты – возникает в критической ситуации, которая может быть создана стихийно или искусственно или за счет взламывания защиты самой системы защиты
* каналы утечки информации – характеризуют ситуацию, когда либо проектировщики не смогли предупредить, либо система не в состоянии рассматривать такой доступ как запрещенный.

Основной класс каналов утечки в ЭСОД - каналы по памяти (т.е. каналы, которые образуются за счет использования доступа к общим объектам системы).

w

r

(t, exe)

Следующий основной класс каналов утечки – каналы по времени, передающее противнику информацию о процессе, промодулированном ценной закрытой информацией.

exe

w

(t, exe)

r

где U1 - злоумышленник; U2 - пользователь, оперирующий ценной информацией; Sц - субъект, информация о котором представляет интерес; Sm -субъект, процесс которого модулируется информацией процесса Sц;

**Угрозы нарушения целостности и механизмы защиты от них**

Нарушения целостности информации - это незаконные уничтожение или модификация информации.

Основные источники угроз целостности

* пожары
* стихийные бедствия
* преднамеренные критические ситуации в системе, вирусы, "троянские кони" и т.д.

Каналы утечки здесь заменяются таким понятием как каналы воздействия на целостность (или о каналах разрушающего воздействия).

# **Лекция №7. Политика безопасности. Модели безопасности**

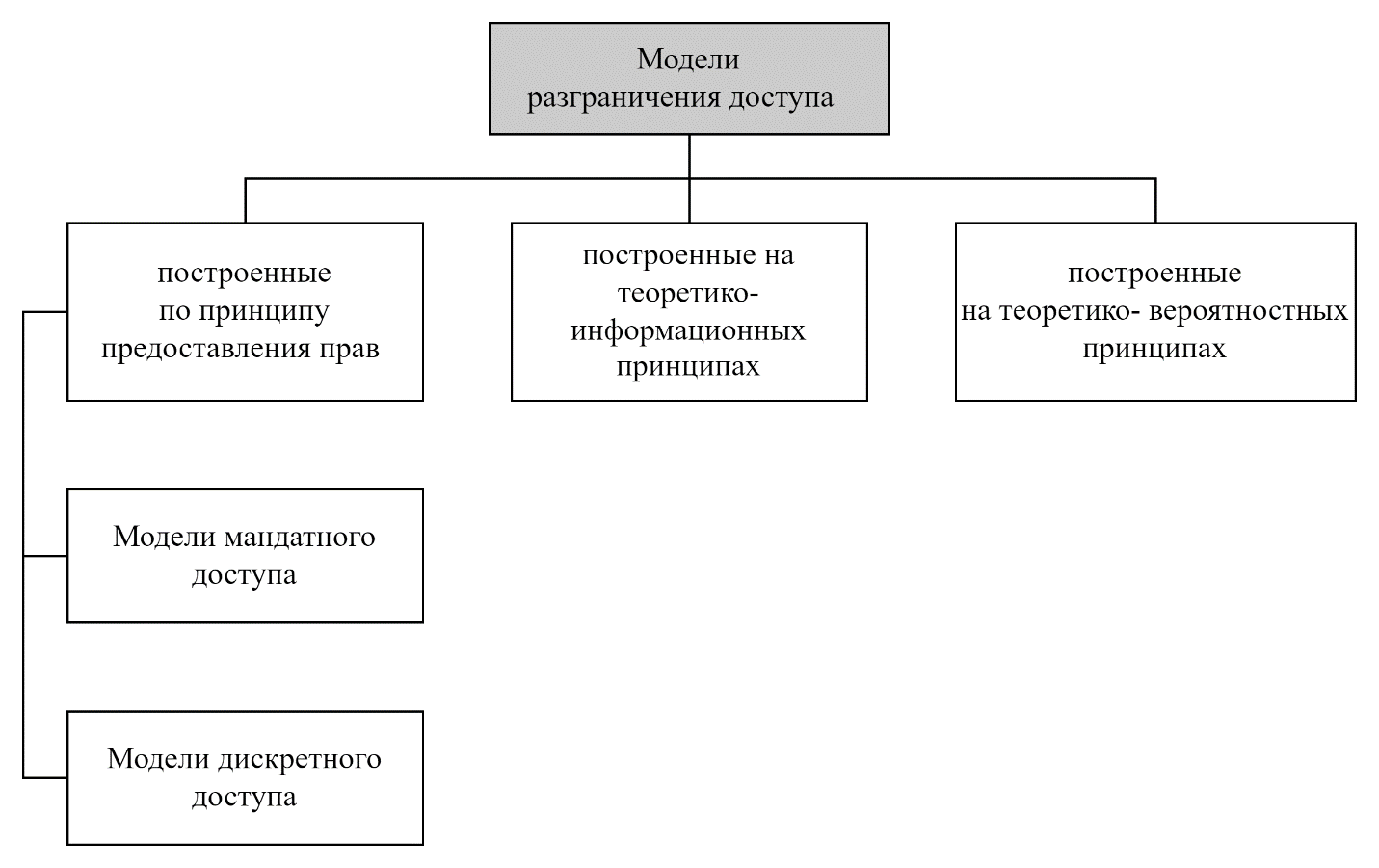
ПБ СОД может быть выполнена

* формально – в основе лежат модели безопасности (т.е. абстрактные описания поведения целого класса систем без рассмотрения конкретных деталей их реализации). *Преимущество* – отсутствие противоречий в ПБ и возможность теоретического доказательства безопасности СОД при соблюдении всех условий ПБ.
* неформально – широкое распространение получило описание права доступа субъектов и объектов в виде таблиц, наглядно представляющих права доступа. *Преимущество* – легкость для понимания мало квалифицированных пользователей и разработчиков пользователями. *Недостаток* – легко допустить логические ошибки, и сложные выражения затруднительно представить в табличной форме.

Модель безопасности - это абстрактное описание поведения классов систем, без рассмотрения конкретных деталей их реализации.

Виды моделей безопасности:

* Модели разграничения доступа служат для синтеза ПБ, направленных на предотвращение угрозы конфиденциальности информации
* Модели контроля целостности
* модели, построенные по принципу предоставления прав (модели дискретного и мандатного доступа)
* модели, построенные на теоретико- информационных принципах.
* модели, построенные на теоретико- вероятностных принципах.



**Опр*.*** Политика безопасности это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Отличия ПБ от НСД:

1. Политика определяет как разрешенные, так и неразрешенные доступы

2. ПБ по своему определению конструктивна, может быть основой определения некоторого автомата или аппарата для своей реализации.

Построение ПБ:

**1 шаг.** В информацию вносится структура ценностей и проводится анализ риска.

**2 шаг.** Определяются правила для любого процесса пользования данным видом доступа к элементам информации, имеющим данную оценку ценностей.

**Дискреционная политика (discretionary policy)**

1. Система представляется совокупностью пяти наборов

(множеств):

- множества пользователей U;

- множества ресурсов R;

- множества состояний S;

- множества установленных полномочий A;

- множества операций E.

2. Область безопасности представляется декартовым

произведением:

A × U × E × R × S

3. Пользователи подают запросы на доступ к ресурсам,

осуществление которых переводит систему в новое состояние.

Указанные права доступа записываются в виде матрицы доступа, элементы которой - суть подмножества множества **R**, определяющие доступы субъекта S, к объекту 0i(i = 1, 2,...,; j = 1, 2,... )*.*

Варианты задания матрицы доступа:

1. Листы возможностей: Для каждого субъекта Si создается лист (файл) всех объектов, к которому имеет доступ данный объект.

2. Листы контроля доступа: для каждого объекта создается список всех субъектов, имеющих право доступа к этому объекту.

Одна из самых существенных слабостей этого класса политик - то, что они не выдерживают атак при помощи "Троянского коня".

Следующая проблема дискреционной политики -это автоматическое определение прав.

**Модель распространения прав доступа «take-grant»**

Основные положения модели сводятся к следующему:

1. КС рассматривается как граф Γ (O, S, E), в котором

множество вершин представлено (см. рис. 2.2):

- множеством объектов O доступа;

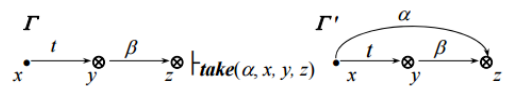
- множеством субъектов S доступа, причем S ⊆ O, а

множество ребер:

- множеством E установленных прав доступа (x, y, α) субъекта x к объекту y с правом α из конечного набора прав ∪ {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).

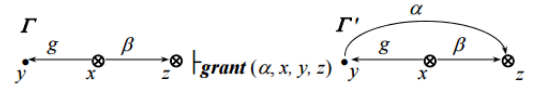
2. Состояния КС (т. е. состояние системы разграничения доступа) изменяются под воздействием команд 4-х видов:

2.1. Команда «Брать» – take(α, x, y, z)



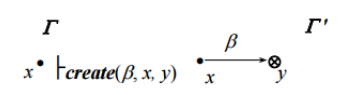
Изменение состояния фрагмента графа доступов Γ по команде **«Брать»** – субъект x берет права доступа α ⊆ β на объект z у объекта y (обозначения: **├с** – переход графа **Γ** в новое состояние **Γ '** по команде **c**; x∈ **S**; y, z∈ **O**)

2.2. Команда «Давать» – grant(α, x, y, z)



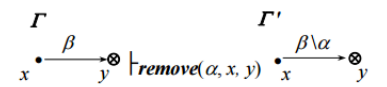
Субъект x дает объекту y право α ⊆ β на доступ к объекту

2.3. Команда «Создать» – create(β, x, y)



Субъект x создает объект y с правами доступа на него β ⊆ R (y – новый объект, O'=O ∪{y})

2.4. Команда «Удалить» – remove(α, x, y)



Субъект x удаляет права доступа α ⊆ β на объект y.

3. Безопасность системы рассматривается с точки зрения возможности получения каким-либо субъектом прав доступа к определенному объекту (в начальном состоянии такие права отсутствуют) при определенной кооперации субъектов путем последовательного изменения состояния системы на основе выполнения команд. Предметом анализа при этом являются установленные в начальный момент времени отношения между субъектами по получению и передаче прав доступа на объекты системы, а также возможные ограничения на дальнейшую кооперацию субъектов в процессе функционирования системы. Рассматриваются два возможных

варианта:

- санкционированное получение прав доступа (безопасное функционирование системы);

- похищение прав доступа (условия, в которых безопасность не обеспечивается).

**Опр.**В графе доступов G вершины Р и S называются tg-связными, если существует путь в G, соединяющий Р и S, безотносительно ориентации дуг, но такой, что каждое ребро этого пути имеет метку, включающую t или *g.*

**Теорема 1.** Субъект Р может получить доступа к, объекту X, если существует субъект S, имеющий доступ а, к вершине X такой, что субъекты Р и S связаны произвольно ориентированной дугой, содержащей хотя бы одно из прав t или g.

**Теорема. 2.** Пусть в системе все объекты являются субъектами. Тогда субъект Р может получить доступ а к субъекту X тогда и только тогда, когда выполняются условия:

1. Существует субъект S такой, что в текущем графе G есть дуга



2. S tg-связна с Р.

# **Лекция №8. Вероятностные модели на основе анализа угроз системе. Политика MLS**

Вероятностные модели на основе анализа угроз системе исследуют вероятность преодоления системы защиты за определенное время Т.

***Игровая модель***

Игровая модель системы защиты строится по следующему принципу. Разработчик создает первоначальный вариант системы защиты. После этого аналитик-«злоумышленник» начинает его преодолевать. Если к моменту времени Т, в который злоумышленник преодолел систему защиты, у разработчика нет нового варианта, система защиты преодолена. Если нет - процесс продолжается. Данная модель описывает процесс эволюции системы защиты в течение времени.

***Модель системы безопасности с полным перекрытием***

Основное положение данной модели — тезис (аксиома) — система, спроектированная на основании модели безопасности с полным перекрытием, должна иметь, по крайней мере, одно средство (субъект) для обеспечения безопасности на каждом возможном пути проникновения в систему.

В модели точно определяется каждая область, требующая защиты (объект защиты), оцениваются средства обеспечения безопасности с точки зрения их эффективности и их вклад в обеспечение безопасности во всей вычислительной системе.

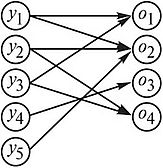
Если ущерб не может быть определен количественно, то его полагают равным некоторой условной (как правило, средней) величине. Количественная категория «ущерба» может быть выражена в стоимостном (ценовом) эквиваленте, либо в терминах, описывающих системы (например, единицах времени, необходимых для достижения тех или иных характеристик ИС после СИВ).

С каждым объектом, требующим защиты, связывается некоторое множество действий, к которым может прибегнуть злоумышленник для получения несанкционированного доступа к объекту. Можно попытаться перечислить все потенциальные злоумышленные действия по отношению ко всем объектам безопасности для формирования набора угроз, направленных на нарушение безопасности. Основной характеристикой набора угроз является вероятность проявления каждого из злоумышленных действий. В любой реальной системе эти вероятности можно вычислить с ограниченной степенью точности.

***Модели безопасности с полным перекрытием множества угроз***

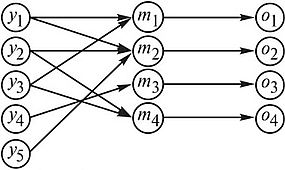
Строится исходя из постулата, что система безопасности должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути воздействия нарушителя на информационную систему. В модели точно определяется каждый объект, требующий защиты, оцениваются средства обеспечения безопасности в отношении их эффективности и их вклад в обеспечение безопасности всей ИС.

Множество отношений «объект-угроза» образует двудольный граф, в котором ребро (yi , оj ) существует тогда и только тогда, когда yi является средством получения доступа к объекту oj.



Угроза может распространяться на любое число объектов, а объект может быть уязвим со стороны более чем одной угрозы.

Цель защиты — «перекрыть» каждое ребро данного графа и воздвигнуть барьер для доступа по этому пути. Набор М средств обеспечения безопасности преобразует двудольный граф в трехдольный.



**Выводы по моделям анализа угроз**

Основное преимущество метода моделирования – возможность численного получения оценки степени надежности системы защиты информации.

При синтезе систем защиты в ИС данный подход полезен тем, что позволяет минимизировать накладные расходы (ресурсы вычислительной системы) для реализации заданного уровня безопасности.

При анализе систем защиты информации модели данного типа позволяют оценить вероятность преодоления системы защиты и степень ущерба системе в случае преодоления системы защиты.

Основа политики MLS:

* Решетка ценностей SC
* Понятие информационного потока.

**Опр.** Политика MLS считает информационный поток Х->Y разрешенным тогда и только тогда, когда c(Y)>c(X) в решетке SС.

**Опр.** В системе с двумя доступами r и w политика MLS определяется следующими правилами доступа:



Структура решетки очень помогает организации поддержки политики MLS.

MLS политика в современных системах защиты реализуется через мандатный контроль (или, также говорят, через мандатную политику).

Устройство мандатного контроля, удовлетворяющее некоторым дополнительным, кроме перечисленных, требованиям, называется монитором обращений.

# **Лекция №9. Модели мандатного доступа**

**Модель Белла-ЛаПадулы**

Основные положения модели Белла-ЛаПадулы сводятся

к следующему:

1. Модель системы  представляется совокупностью:

- множества объектов **O** доступа;

- множества субъектов **S** доступа;

- множества прав доступа **R** всего два элемента – **read и write**;

- матрицы доступа **A[s,o];**

- решетки  уровней безопасности L субъектов и объектов системы;

- функции  **: S ∪ O → L**, отображающей элементы множеств **S** и **O** на множество **L**;

- множества состояний системы **V,** которое определяется множеством упорядоченных пар ( , A);

- начального состояния  **∈ V**;

- набора запросов **Q** субъектов на доступ (осуществление операций) к объектам, выполнение которых переводит систему в новое состояние;

- функции переходов , которая переводит систему из одного состояния **V** в другое **V\*** при выполнении запросов из **Q**.

Состояния системы разделяются на опасные и безопасные. Для анализа и формулировки условий, обеспечивающих безопасность состояний системы, вводятся следующие определения:

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

**∀ s ∈ S, ∀ o ∈ O, read ∈ A[s, o] → (s) ≥ (o)** .

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

**∀ s ∈ S, ∀ o ∈ O, write ∈ A[s, o] → (o) ≥ (s) .**

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

**Опр.(Критерий безопасности в модели Белла-ЛаПадулы).** Система безопасна тогда и только тогда, когда ее начальное состояние безопасно и все состояния, достижимые из путем применения конечной последовательности запросов из Q, безопасны.

**Теорема (Basic Security Theorem - основная теорема безопасности» (ОТБ)).** Система безопасна тогда и только тогда, когда:

1. Состояние безопасно , и

2. Функция переходов  такова, что для любого состояния v, достижимого из  при выполнении конечной последовательности запросов из множества Q таких, что при  **(v,q)=v\*,** где **v=( ,A)** и **v\*=( \*,A\*),** переходы системы из состояния в состояние подчиняются следующим ограничениям для s ∈ **S** и для o ∈ **O**

- если **read ∈ A\*[s, o] и read ∈A[s, o], то \*(s) ≥ \*(o);**

- если **read ∈ A[s, o] и \*(s) < \*(o), то read ∉ A\*[s, o];**

- если **write ∈ A\*[s, o] и write ∉A[s, o], то \*(s) ≥ \*(o);**

- если **write ∈ A[s, o] и \*(s) < \*(o), то write ∉A\*[s, o]**

**Критика модели Белла-ЛаПадулы**

1. Рас­пределенные компьютерные системы.

2. Предотвращение угрозы нарушения секретности для доверенных субъектов

**Модель Джона МакЛина системы, названной «Система Z»**

МакЛин описал конфигурацию, в которой все субъекты могут чи­тать и записывать любой объект путем назначения соответствующих уровней сек­ретности объекта перед выполнением запросов на доступ. В такой системе все состояния могут быть рас­смотрены как удовлетворяющие требованиям модели Белла и Лападула.

В оригинальной модели, представленной авторами, было введено требование силь­ного и слабого спокойствия. Данные требования снимают проблему Z-системы.

Правило сильного спокойствия – уровни секретности субъектов и объ­ектов никогда не меняются в ходе системной операции.

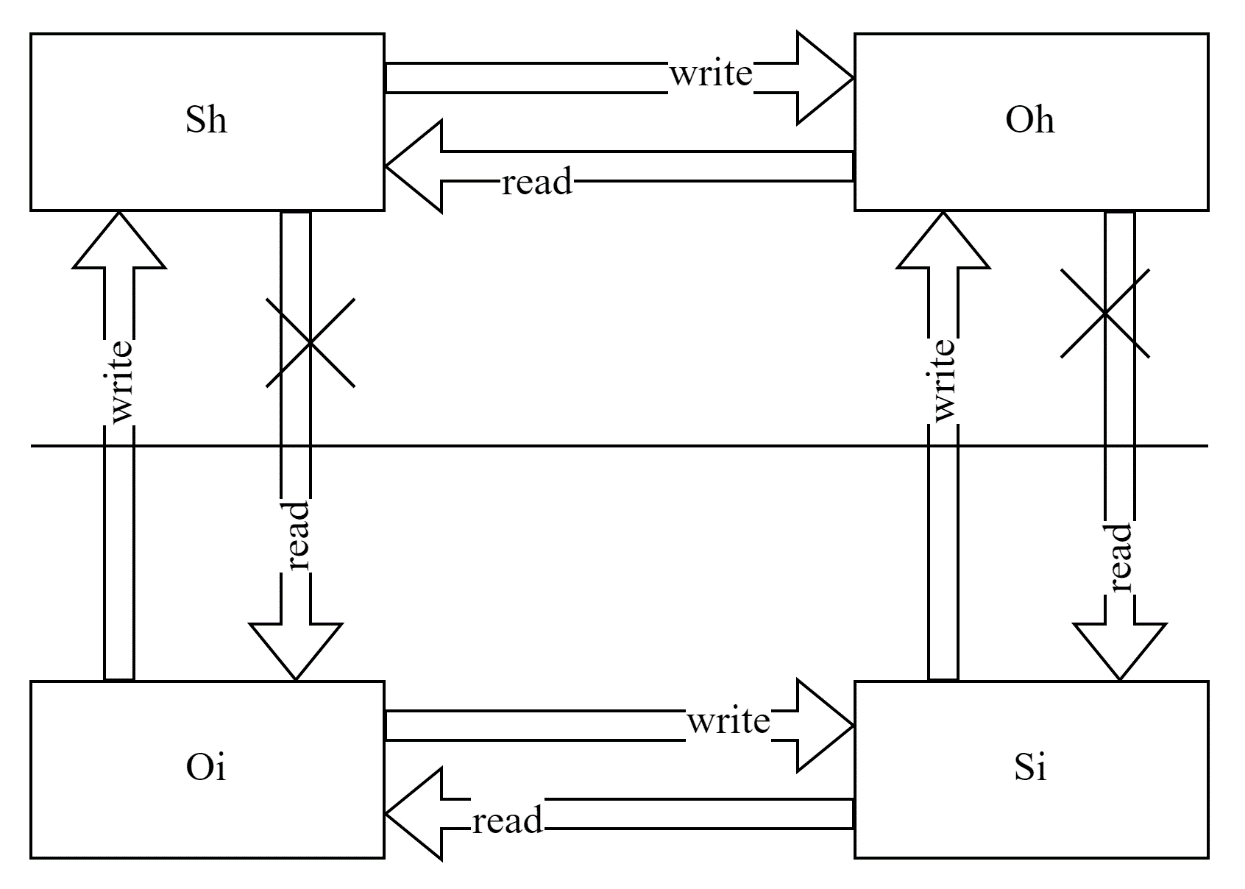
Правило слабого спокойствия – уровни секретности субъектов и объектов никогда не меняются в ходе системной операции таким образом, чтобы нарушить заданную политику безопасности. Это правило может потребовать, что­бы субъекты и объекты воздерживались от действий в период времени, когда меня­ются их уровни секретности.

**Модели контроля целостности**

1. Модель Биба

В данной модели запись на верхний уровень не нарушает безопасности системы. При рассмотрении мандатной модели контроля целостности запись наверх может представлять угрозу, поэтому можно потребовать, чтобы та­кая запись была запрещена. Следуя подобным аргументам, можно рассматривать чте­ние снизу как поток информации, идущий из объекта нижнего уровня и нарушаю­щий целостность субъекта высокого уровня – **«нет чтения снизу» (No Read Down, NRD) и «нет записи наверх» (No Write Up, NWU)**.

Правило NRD мандатной модели целостности Биба определяется как запрет субъектам на чтение информации из объекта с более низким уровнем целостности. NRD является полной противоположностью правила NRU модели Белла и Лападу­ла, за исключением того, что здесь используются уровни целостности, а не секрет­ности, как в модели Белла и Лападула.



2. Модель понижения уровня субъекта (вариация модели Биба с ослаблением правила чтения снизу)

В данной модели субъекту разрешается осуществлять чтение снизу, но в результате такого чтения уровень целостности субъекта понижается до уровня целостности объекта.

Одной из характеристик этой модели является то, что она не накладывает никаких ограничений на то, что субъект может прочитать.

Модель подразумевает монотонное изменение уровней целостности субъектов. То есть уровни целостности субъектов или остаются неизменными, или снижаются. В этой модели не предусмотрено никаких механизмов для повышения уровня целостности объекта.

3. Модель понижения уровня объекта (вариация модели Биба с ослаблением правила записи наверх)

Вместо полного запрета на запись наверх эта модель разрешает такую запись, но снижает уровень целостности объекта до уровня целостности субъекта, осуществлявшего запись.

Данная модель не накладывает никаких ограничений на то, что субъект может читать или писать.

В данной модели происходит монотонное снижение уровня целостности объ­ектов. В этой модели не предусмотрено никаких механизмов для повышения уровня целостности объекта.

**Критика модели Биба**

Однако модель Биба также обладает многими проблемами, присущими модели Белла и Лападула:

* Использование модели Биба в распределенных систе­мах может привести к двунаправленному потоку информации при удаленном чте­нии.
* Слишком сильно полагается на понятие доверенных процессов, т. е. проблема необходимости создания доверенных процессов для повышения или понижения це­лостности субъектов или объектов является весьма существенной.
* Не предусматривает механизмов повышения целостности, что ведет к монотонному снижению целостности системы.
* Использует целостность как некую меру, и ставили под сомнение то, что понятие «большей целостности» имеет какой-либо смысл. м

**Объединение моделей безопасности**

Существует 2 подхода для рассмотрения вопросов об объединении 2-х моделей:

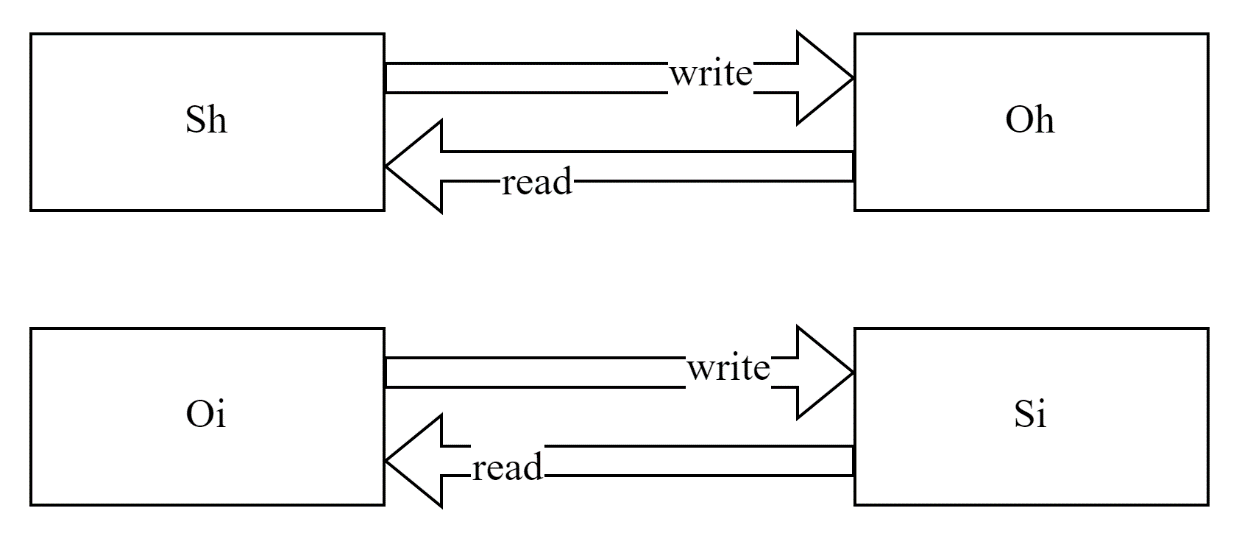
1. Различные модели могут быть выражены одной универсальной структурой так, что их правила работают в пределах одной модели безопасности.
2. Модели могут использоваться отдельно, и может быть проведен неформальный анализ соответствующих подходов к реализации каждой модели.

**Объединение модели Белла и Лападула и модели Биба**

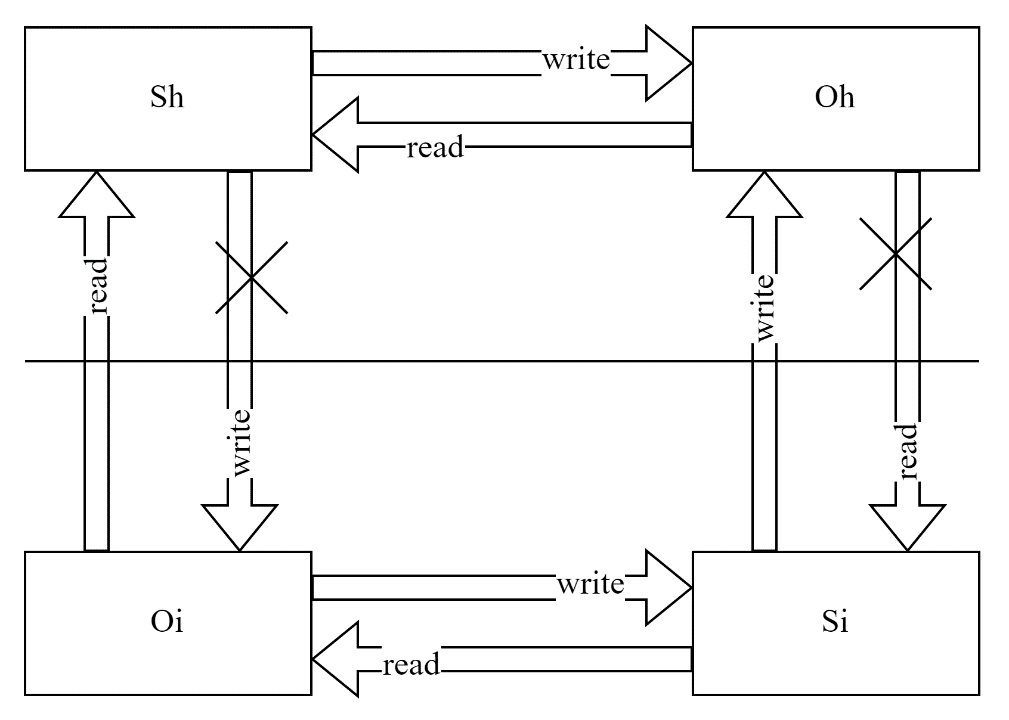
Данная политика включает в себя правила из обеих моделей. Для этого потребуется, чтобы субъектам и объектам были назначены различные уровни секретности и целостности, что позволит проводить оценку каждой модели отдельно.

Другим подходом может быть логическое объединение правил этих моделей в одну модель безопасности, основанную на одном уровне как для безопасности, так и для целостности.

Данное объединение приведет к правилам равного чтения и равной записи, которые удовлетворяют обеим моделям, но значительно снизит гибкость операций чтения и записи в реальной системе.



Еще один подход основан на использовании одного уровня как для целостности так идля безопасности. Этот прием подразумевает размещение субъектов и объектов с высокой целостностью на нижней ступени иерархии безопасности.



**Выводы**

Данная схема обеспечивает защиту системных файлов и администраторов от троянских коней. Если троянский конь находится на одном из верхних уровней, он никогда не сможет исказить системные файлы за счет правила NWD. Таким образом, осуществляется защита целостности от троянских коней. Очевидно, такое объединение моделей осуществляет защиту секретности для верхних уровней определенной иерархии и защиту целостности для нижних уровней.

# **Лекция №10. Модели**

**Теоретико-информационные модели**

Одной из самых трудно решаемых проблем безопасности в АС – проблема скрытых каналов утечки информации.

Скрытым каналом утечки информации называется механизм, посредством которого в АС может осуществляться информационный поток (передача информации) между сущностями в обход политики разграничения доступа.

В моделях дискреционного доступа критерием безопасности является невозможность осуществления доступа субъектов к объектам вне явных разрешений, прописанных в матрице доступа. В моделях мандатного доступа недопустимыми являются потоки, нарушающие правила NRU и NWD.

**Понятие и классификация скрытых логических каналов утечки информации**

Под скрытым каналом понимается (ГОСТ Р 53113.2-2009) непредусмотренный разработчиком информационной системы коммуникационный канал, который может быть применен для нарушения политики безопасности. Факт существования такого канала невозможно выявить штатными средствами, так как он не предусмотрен разработчиками, для формирования используются не предназначенные для передачи данных инструменты.

Возникают риски:

* внедрения вредоносных программ, осуществляющих съем информации;
* модификации данных;
* подачи команд нарушителем политик безопасности, вносящих изменения в регламент работы информационной сети;
* утечки паролей и криптографических ключей.

При использовании скрытого канала нарушитель получает контроль над линией передачи данных или команд от уполномоченного лица к информационной системе. Получение контроля часто реализуется при помощи установки закладных устройств и их взаимодействия с вредоносными программами, скрытно установленными на компьютер.

Классификация скрытых каналов производится по разным критериям, выделяются (ГОСТ Р 53113.1-2008):

* скрытые каналы по памяти;
* скрытые каналы по времени;
* скрытые статистические каналы.

**Информационные модели**

**1. Модель невмешательства**

Модель, основанная на принципе невмешательства. В данной модели система является безопасной, если группы субъектов не вмешиваются в работу друг друга. Система в данной модели представлена как машина состояний, описанная следую­щим образом: *S= {s1 ,…, sn}* —множество субъектов, расположенных на различных уровнях секретности, Σ = {σо, σ,,...} — множество состояний, *О* = {о1, о2, ...} — множество выходов и Z= *{z1, z2,….}* —множество команд. Множество команд изме­нения состояний можно записать как *С = S × Z* на основании того, что уровень секрет­ности субъекта оказывает влияние на выполняемую команду. Тогда можно ввести следующее определение.

**Опр**. Функция изменения состояний *Т: С* х Σ *—>* Σ описывает эффект выполнения команды *с* в состоянии σ. Функция выхода *Т: С* х Σ —> *О* описывает выход машины при исполнении команды *с* в состоянии σ. Начальное состояние сис­темы обозначается как σ0. Выход системы может быть описан как функция выполне­ния команд и начального состояния.

Модель, основанная на принципе невмешательства, разработана для:

* разрешения проблемы скрытых каналов утечки информации;
* определения разрешенных доступов по чтению;
* определения разрешенных доступов по записи.

В модели, основанной на принципе невмешательства, система является безопасной, если:

* группы субъектов не вмешиваются в работу друг друга;
* группы субъектов связаны скрытыми каналами утечки информации;
* группы объектов не вмешиваются в работу друг друга.

**Опр**. Допустим, *T\*{cs, и)* — последовательность переходов состояний системы, а *Р\*(сs, σi)* — соответствующий ей выход системы. Тогда *proj (s,сs, σi*.) — множество выходов *P\*{cs, σi),* которые субъект s авторизован видеть (в том же по­рядке, в котором они появляются в Р\*(*cs, σi)*.

**Опр**. Допустим, *G* ⊆ *S* — группа субъектов, а *А*⊆Z — множество команд. Определим *πG(cs)* как последовательность команд ct, полученную удалением всех элементов *(s, z)* в *сз* для *s∈G.* Определим *πA(cs)* как последовательность команд сs полученную удалением всех элементов (s, z) в с8 для z ∈ *А.* Определим *πG,A(cs)* как последовательность команд с, полученную удалением всех элементов (s, z) в *сs* для *s∈ и* z∈*A,*

**Опр.** Допустим, G ⊆S и G’⊆ S — группы субъектов, A⊆Z — множество команд. Тогда пользователи из множества G, исполняя команды из мно­жества A, не вмешиваются в работу пользователей из множества *G'* (*A, G* :| G'), если и только если для всех последовательностей *сs,* состоящих из элементов в С\* и для всех *s* ∈ *G' proj(s, cs, σ)****=*** *proj(s, πG,A(cs), σ).*

**Опр.** Политика безопасности есть множество ограничений невмеша­тельства, приведенных в определении выше.

**Опр**. Допустим, *r* — рефлексивное отношение, определенное на *D×D,* Тогда г определяет политику безопасности для *X.*

Отношение г определяет возможные потоки информации в системе. Если *di rdj* выполняется, то возможен поток информации между доменами *di* и *dj.* Если данное отношение не выполняется, то поток информации между доменами запрещен. В свя­зи с тем, что *di rdj,* поток информации внутри домена разрешен. Это определение ниче­го не говорит о содержании политики безопасности. Оно показывает только то, что есть политика безопасности.

**Опр.** Допустим *d∈D,c∈*С и с∈С\*. Тогда *πd(ν)* = ν, где ν — пустая последовательность.

Если *dom(c)rd,* то *πd(сs,* с) = *πd(сs)с,* иначе *πd(сs*,*с)=πd(сs).*

**2. Модель невыводимости**

Базируется на описании инфор­мационных потоков в системе. Модель невыводимости выражается в терминах пользо­вателей и информации, связанных с одним из двух возможных, уровней секретности (высокий и низкий).

Под системой в модели невыво­димости понимается четверка *(Е, I, О,* T), где *Е* — множество событий, I∈*Е* — мно­жество событий ввода, О∈Е- множество событий вывода, *Т* — множество всех возможных конечных последовательностей событий. Множество *Е* разделяется на мно­жество высокоуровневых *(H)* и низкоуровневых *(L)* событий *(Е* = *H* ∪ *L, H* ∩ *L* = 0). Тогда можно определить высокоуровневый ввод *Highj=Н*∩I, высокоуровневый вывод *High0 = Н ∩ О,* низкоуровневый ввод *Low1* = *L ∩ I,* низкоуровневый вывод *Low0 =L ∩ О.*

Допустим, *TL0W* содержит множество всех возможных конечных последователь­ностей низкоуровневых событий. Тогда можно определить функцию *πL*: *Т* —> *Т****LOW****,* удаляющую все высокоуровневые вводы из трассы событий. При этом низкоуровне­вый субъект не сможет сделать выводов высокоуровневом вводе на основании трассы t**0∈** *Т****LOW***

Система является безопасной по отношению к свойству выводимости, если для любой трассы *t****LOW***∈*Т****LOW***соответствующее множество высокоуровневых трасс содержит все воз­можные трассы *t* e *T,* для которых *πL(t)= tww.*