# Дисциплина «Технологии обеспечения информационной безопасности»

Лекция 4. «Модели управления доступом»

доцент кафедры КБ-4
кандидат педагогических наук, доцент
Пимонов Роман Владимирович

# Учебные вопросы:

1. Понятие стратегий и политик безопасности.
2. Основные модели управления доступом.

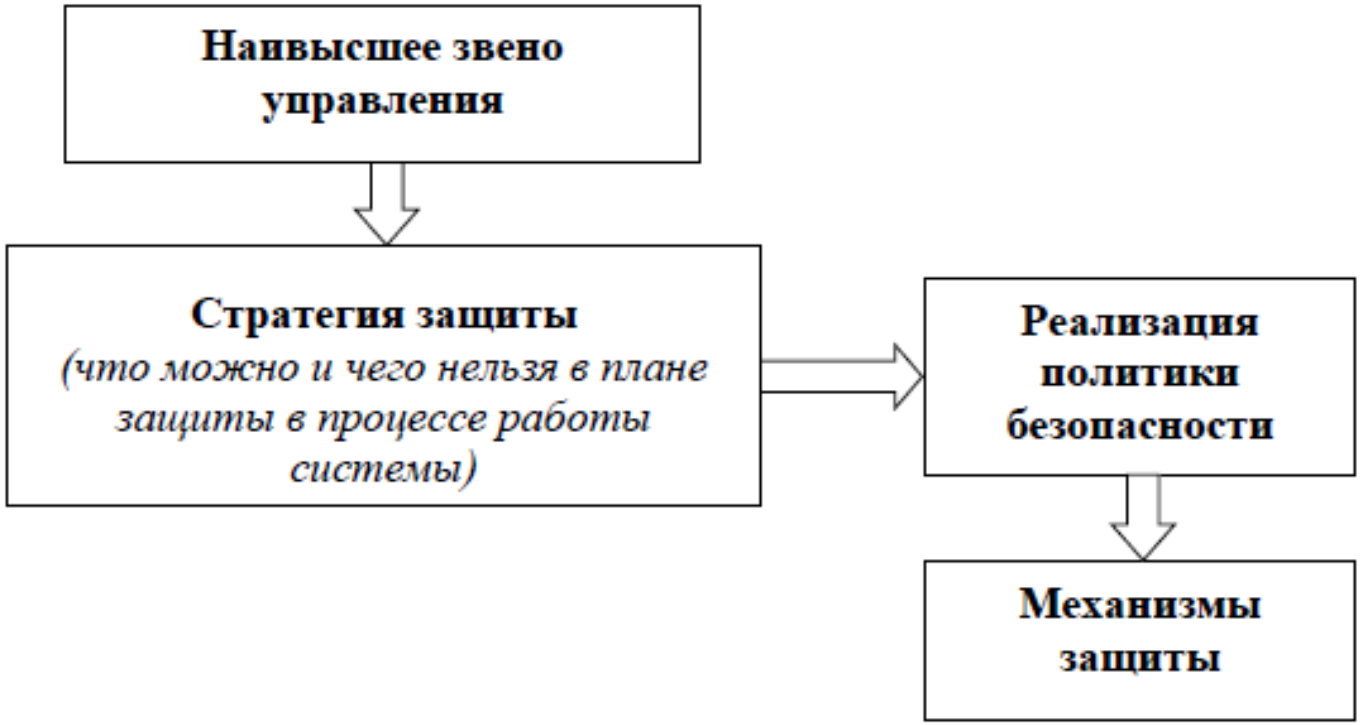
# Нормативные документы


1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / Учебное пособие для вузов. - 3-е изд., перераб. и доп. - Москва: Горячая линия - Телеком, 2023. - 352 с.
2. Модели безопасности компьютерных систем : учеб. пособие / Н. А. Богульская, М. М. Кучеров. – Красноярск : Сиб. федер. ун-т, 2019. – 206 с.
3. https://profsandhu.com/cs6393_s13/
4. Руководящий документ от 30 марта 1992 г. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации.
5. Руководящий документ от 30 марта 1992 г. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации.

# Вопрос 1. Понятие стратегий и политик безопасности.

# Вопрос 1. Понятие стратегий и политик безопасности.

**Стратегия** – план достижения долгосрочной или общей цели [ГОСТ Р ИСО 9000-2015 ].




**Механизм реализации стратегии защиты**

**Стратегии защиты информации**

| Учитываемые угрозы | Влияние на АС | | |
|---|---|---|---|
| | отсутствует | частичное | Полное |
| Наиболее опасные | *Оборонительная стратегия* | | |
| Все известные | | *Наступательная стратегия* | |
| Все потенциально возможные | | | *Упреждающая стратегия* |

# Вопрос 1. Понятие стратегий и политик безопасности.

**Политика безопасности** - набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации [Оранжевая книга 1983 г.].

***Уровень нормативного управления***

**Политика безопасности (информации в организации):** Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [ГОСТ Р 50922-2006].

***Уровень управления доступом***

**Политика (модель) управления доступом** - совокупность правил, подлежащих реализации средством защиты информации и регламентирующих предоставление доступа между компонентами среды функционирования этого средства защиты информации [ГОСТ Р 59453.1— 2021].

**Традиционно политики безопасности разделяют на *две* категории:**

- *административные*:
- *технические.*

***Административная или организационная ПБ*** обычно *излагается в* документах трех уровней:

1. Первый *уровень* - документы общего характера.
2. Второй *уровень* - необходим в случае структурной сложности организации, наличии специфичных областей деятельности, подразделений, технологий, подсистем и т. п.
3. Третий *уровень* относится к конкретным службам или подразделениям организации и *детализирует верхние* уровни *ПБ.*

**Техническая ПБ (англ. technical security policy)** – это совокупность законов, правил и практических методов, регулирующих обработку чувствительной информации и использование ресурсов ПО и аппаратным обеспечением ИС.

**Техническая ПБ** базируется на *правилах двух* видов.

1. *Первая группа* связана с заданием правил разграничения доступа ко всем ИР организации,
2. *Вторая группа* – основана на правилах анализа сетевого трафика как *внутри* корпоративной ИС, так и при его выходе или входе *из* нее.

В *основе этих правил* лежит **принцип доверия** – пользователям, *приложениям*, процессам, БД, файлам и т. п. Поэтому *определяя техническую ПБ,* нужно установить, насколько можно *доверять людям и* информационным ресурсам.

## Примерное содержание технической политики безопасности:

- сведения о ее целях и области применения;
- цели системы обеспечения безопасности и их соотношение с правовыми и нормативными обязательствами и целями организации;
- требования, предъявляемые к системе обеспечения безопасности с точки зрения обеспечения конфиденциальности, целостности, доступности, достоверности и надежности информации;
- сведения об общем уровне безопасности и остаточном риске, необходимые для осуществления управления;
- сведения об управлении безопасностью, включающие в себя данные об ответственности и полномочиях как организации, так и отдельных лиц;
- вариант подхода к управлению риском, принятый организацией;
- пути и способы определения приоритетов при реализации защитных мер;
- данные о наличии общих правил контроля доступа (контроль доступа при физическом доступе лиц в здания, рабочие помещения, а также к системам и информации);
- сведения о доведении до персонала мер безопасности и обучении лиц, осуществляемом организацией;
- данные об общих процедурах контроля и поддержания безопасности;
- перечень общих проблем обеспечения безопасности, касающихся обслуживающего персонала;
- средства и способы доведения сути политики безопасности информационных технологий до всех заинтересованных лиц;
- обстоятельства для пересмотра ПБ;
- методы контроля изменений, вносимых в ПБ организации.

**При разработке ПБ с более высокой степенью детализации** должны быть дополнительно рассмотрены *следующие вопросы*:

- использование стандартов;
- процедуры внедрения защитных мер;
- модели и процедуры обеспечения безопасности, распространяющиеся на все подразделения организации;
- проверка действенности систем обеспечения безопасности;
- мониторинг использования средств безопасности;
- обработка инцидентов, связанных с нарушением ИБ;
- мониторинг функционирования ИС;
- обстоятельства, при которых требуется приглашение сторонних экспертов по проблемам в сфере ИБ.

# Вопрос 2. Основные модели управления доступом.

# Вопрос 2. Основные модели управления доступом.

**Основная цель создания политики безопасности** системы и описания ее в виде формальной модели - это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Формальное выражение политики безопасности называют ***моделью безопасности*.**

**Политика безопасности включает:**

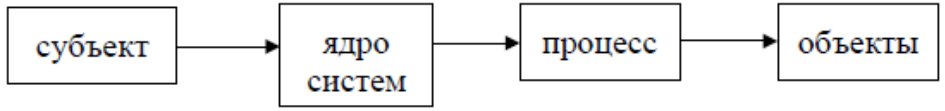
- множество возможных операций над объектами;
- для каждой пары "субъект, объект" (*s*, *o)* множество разрешенных операций, являющееся подмножеством всего множества возможных операций.

***Субъект доступа*** – активная сущность АС, которая может изменять состояние системы через порождение процессов над объектами, в том числе порождать новые объекты и инициализировать порождение новых субъектов.
***Объект доступа*** – пассивная сущность АС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.

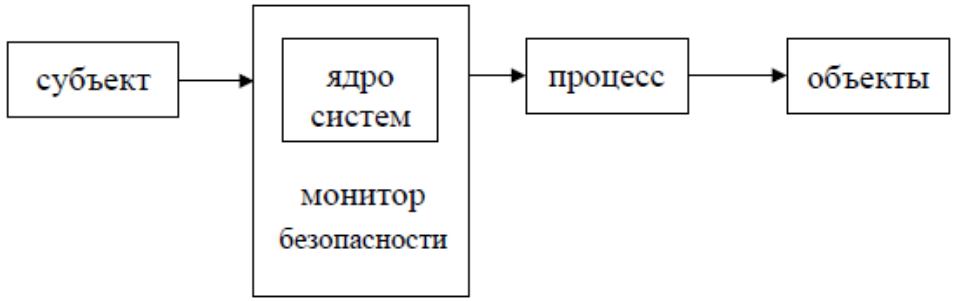
**Система безопасна тогда и только тогда, когда субъекты не имеют возможностей нарушать (обходить) установленную в системе политику безопасности.**

# Вопрос 2. Основные модели управления доступом.

**Монитор безопасности** – механизм реализации политики безопасности в автоматизированной системе, совокупность аппаратных, программных и специальных компонент системы, реализующих функции защиты и обеспечения безопасности (общепринятое сокращение – ТСВ – Trusted Computing Base).




*Незащищенная система*




*Защищенная система*

**Требования к реализации монитора безопасности:**

1. Полнота.
2. Изолированность.
3. Верифицируемость.
4. Непрерывность.

# Вопрос 2. Основные модели управления доступом.

# Вопрос 2. Основные модели управления доступом.

**Дискреционная политика безопасности или дискреционная модель управления доступом** (Discretionary access control – DAC) – разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

***Свойства* DAC :**

- все субъекты и объекты идентифицированы;
- права доступа субъектов на объекты системы определяются на основании некоторого внешнего по отношению к системе правила.

Основным элементом систем дискреционного разграничения доступа является **матрица доступов.**

| | $O_1$ | $O_2$ | $O_3$ | ... | $O_j$ |
|---|---|---|---|---|---|
| $S_1$ | 0 | 0 | 1 | - | 0 |
| $S_2$ | 1 | 1 | 0 | - | 0 |
| ... | - | - | - | - | - |
| $S_i$ | 1 | 1 | 1 | - | 1 |

# Вопрос 2. Основные модели управления доступом.

**Модель Харрисона–Руззо–Ульмана**
Модель безопасности Харрисона–Руззо–Ульмана (HRU), реализует произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа.

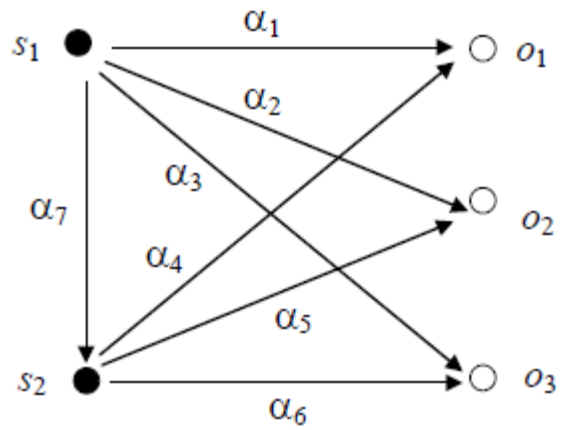
В рамках этой модели система обработки информации представляется **в виде совокупности:**
• активных сущностей - субъектов (множество *S)*, которые осуществляют доступ к информации;
• пассивных сущностей - объектов (множество *O*), содержащих защищаемую информацию;
• конечного множества прав доступа *R* = (*r*1, …rn), означающих полномочия на выполнение соответствующих действий (например, чтение, запись, выполнение).

**Правила организации матрицы прав доступа**:
• создает ресурсы (объекты) владелец;
• владелец объекта произвольно ограничивает доступ субъектов к своему объекту;
• права доступа не зависят от каких-либо факторов. Для каждой тройки субъект–объект–метод доступ определен однозначно и не меняется со временем;
• существует привилегированный пользователь (администратор), который может обратиться к любому объекту с помощью любого метода доступа.

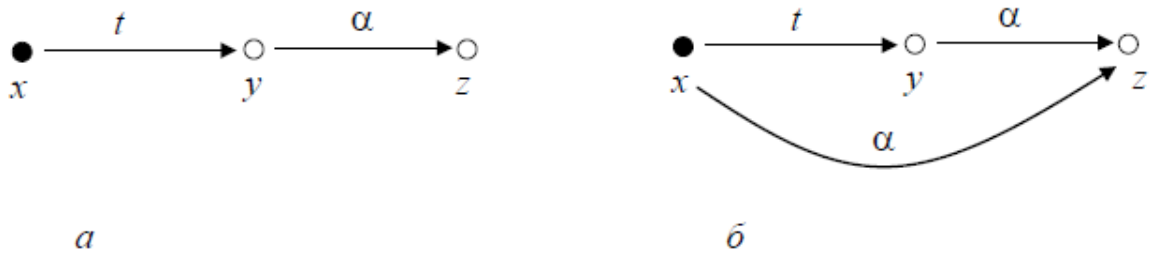
***Модель распространения прав доступа TAKE-GRANT***

АС рассматривается как граф *G* (*O, S, E*), в котором множество вершин представлено:

- множеством объектов *O* ($o_1$, $o_2$, …, $o_n$) доступа;
- множеством субъектов *S* ($s_1$, $s_2$, …, $s_m$) доступа, причем $S \subset O$.

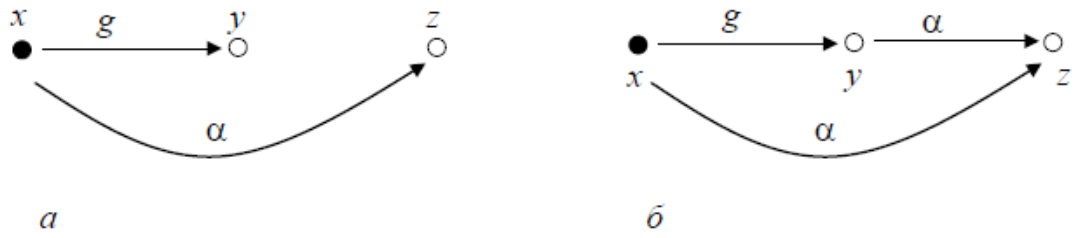



Граф доступа *G* в модели TAKE-GRANT




*а* *б*

Изменение подграфа доступа по команде take:
а - подграф до применения команды,
б – после применения команды



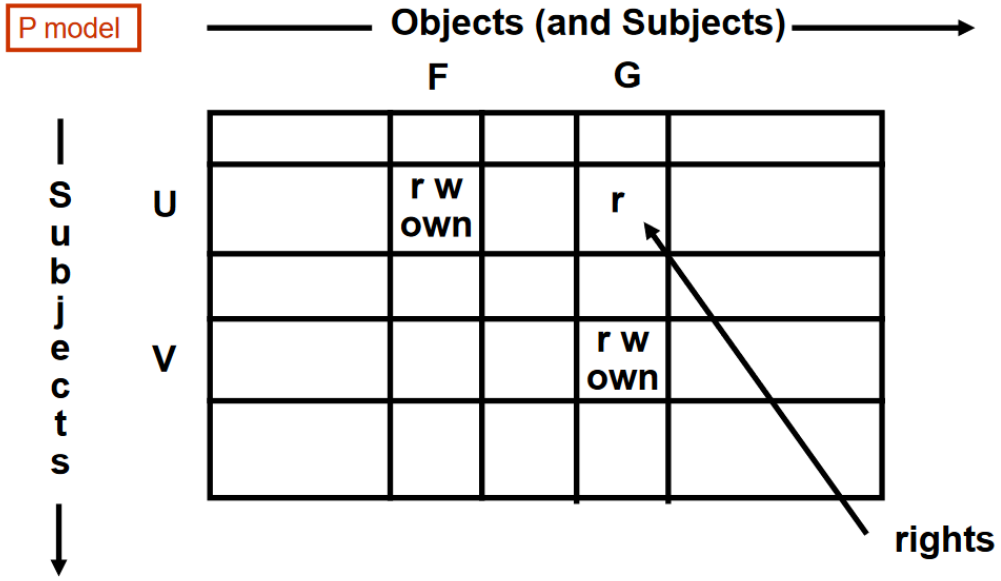

*а* *б*

Изменение подграфа доступа по команде *grant:*
*а* - подграф до применения команды,
*б* – после применения команды

# Вопрос 2. Основные модели управления доступом.

## DAC: ACCESS MATRIX MODEL

P model




## CAPABILITY LISTS

E model

U F/r, F/w, F/own, G/r

V G/r, G/w, G/own

## ACCESS CONTROL LISTS (ACLs)

E model

F

| |
|---|
| U:r |
| U:w |
| U:own |

G

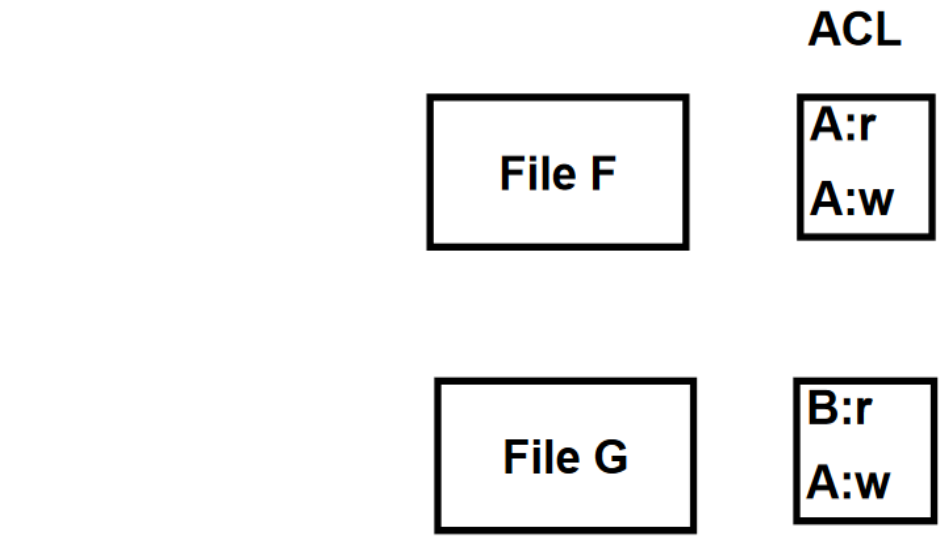
| |
|---|
| U:r |
| V:r |
| V:w |
| V:own |

## ACCESS CONTROL TRIPLES

E model

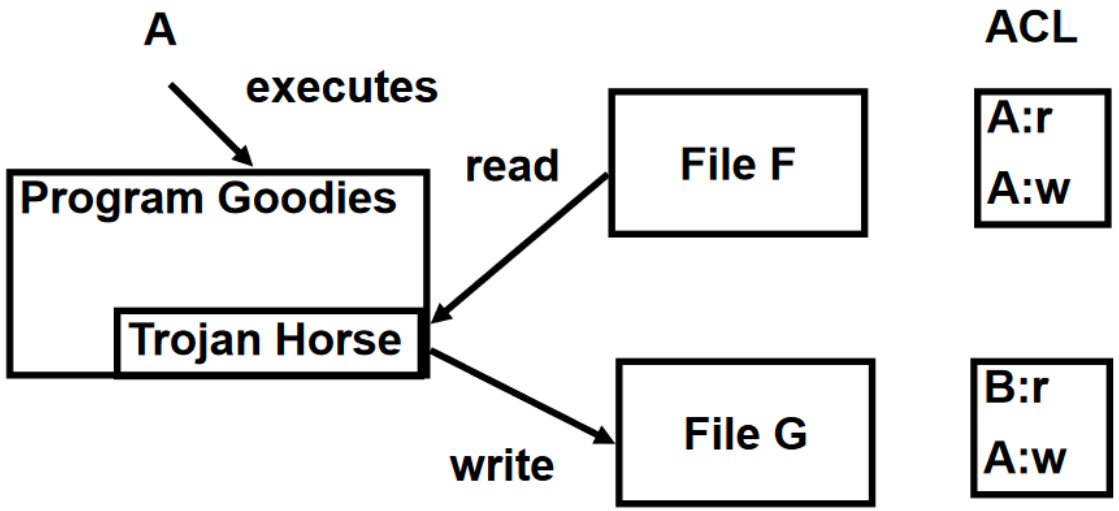
| Subject | Access | Object |
|---|---|---|
| U | r | F |
| U | w | F |
| U | own | F |
| U | r | G |
| V | r | G |
| V | w | G |
| V | own | G |

## DAC: TROJAN HORSE EXAMPLE




**B cannot read file F**

## DAC: TROJAN HORSE EXAMPLE




B can read contents of file F copied to file G

**Мандатная политика безопасности** или мандатное разграничение доступа (Mandatory Access Control – MAC) – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

**Контроль доступа** осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух правил:

1. *No read up (NRU)* – нет чтения вверх: субъект имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.
2. *No write down (NWD)* – нет записи вниз: субъект имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

## *Модель Белла–ЛаПадулы*

**Формальное описание**

1. S - множество субъектов
2. O - множество объектов
3. L - решетка уровней безопасности с линейным отношением преобладания уровня секретности ≥.
4. $F : S \cup O \rightarrow L$ - функция, применяемая к субъектам и объектам, данная функция определяет уровни безопасности своих аргументов в данном состоянии;
5. V - множество состояний - множество упорядоченных пар (F, M), где M - матрица доступа субъектов системы к объектам.

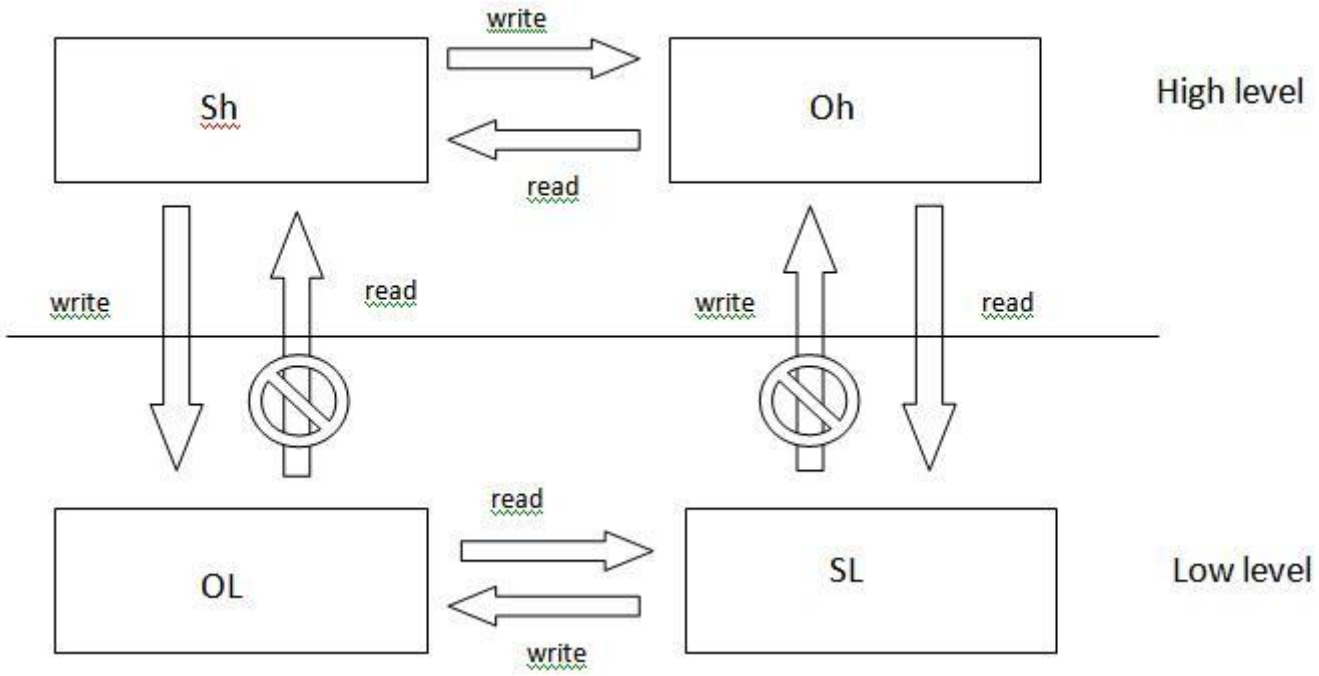
Система представляется начальным состоянием $v_0$, определенным множеством запросов к системе R и функцией переходов $T : (V \times R) \rightarrow V$ такой, что система переходит из состояния в состояние после исполнения запроса.

Система Σ (V0, Q, FT) безопасна тогда и только тогда, когда ее начальное состояние V0 безопасно и все состояния, достижимые из V0 путем применения конечной последовательности запросов из Q, безопасны.

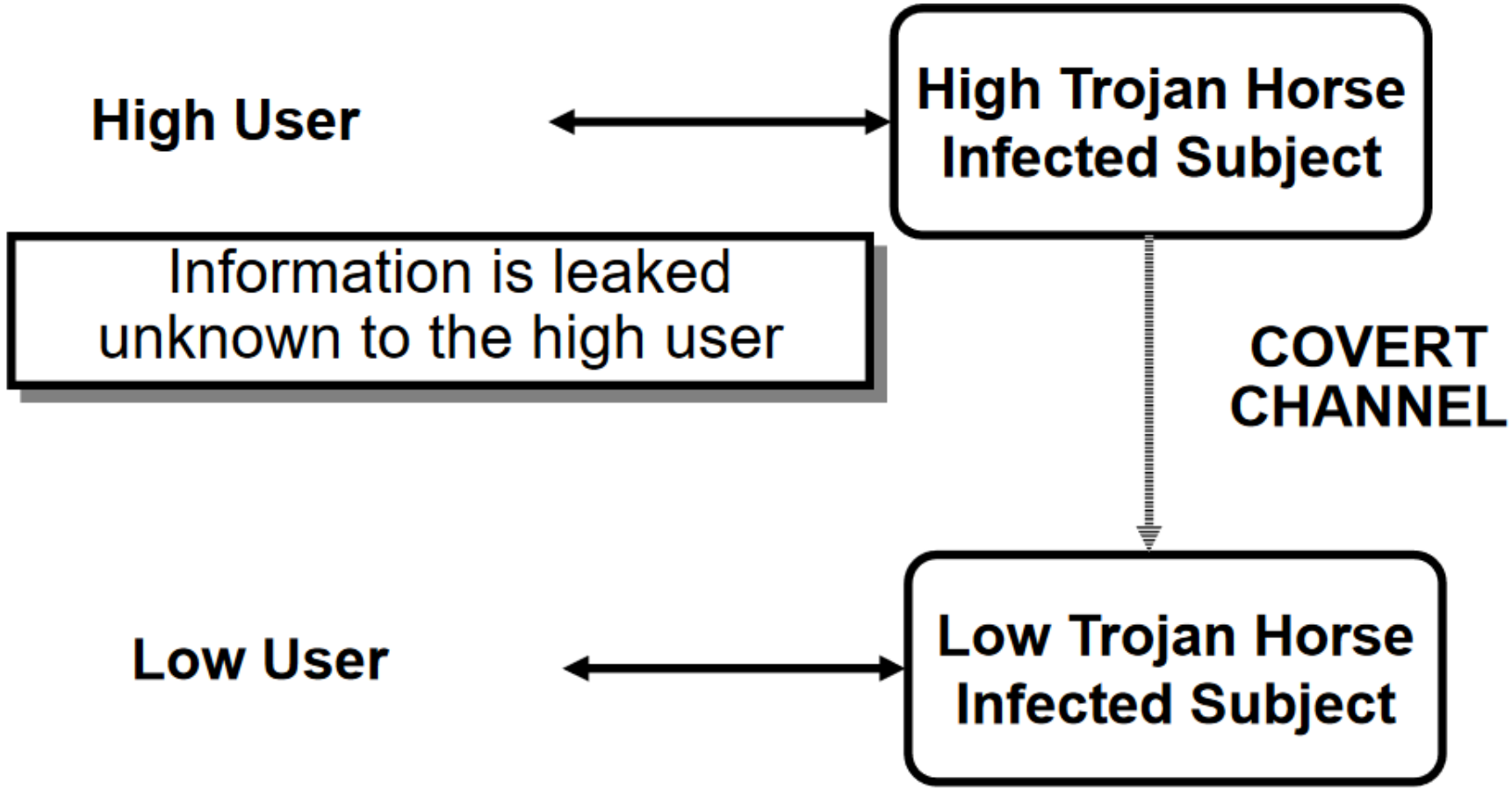
## Модель Биба

**Определены:**

1. Уровни целостности для объектов и субъектов в системе
2. Правило No Read Down.
3. Правило No Write Up.



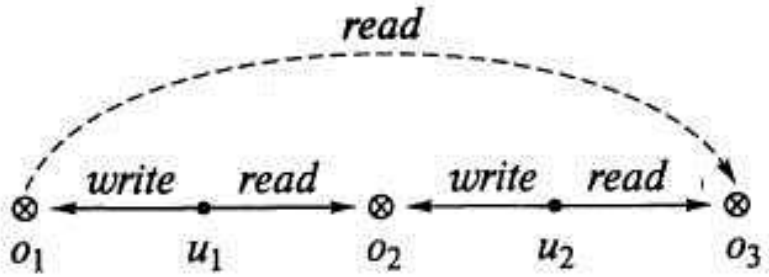
## LBAC: LATTICE STRUCTURES



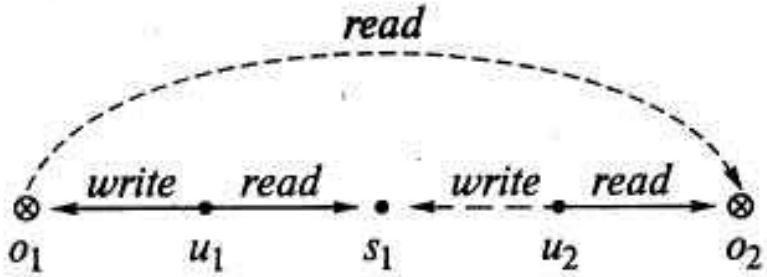
# Вопрос 2. Основные модели управления доступом.

**Политика безопасности информационных потоков** – основана на разделении всех возможных информационных потоков между объектами системы на два непересекающихся множества: благоприятных и неблагоприятных информационных потоков.

**Цель реализации политики безопасности информационных потоков** - обеспечить невозможность возникновения в компьютерной системе неблагоприятных информационных потоков.




Информационный поток по памяти




Информационный поток по времени

## Политика изолированной программной среды (ИПС)

**Цель** реализации ***политики изолированной программной среды*** - определение порядка безопасного взаимодействия субъектов системы, обеспечивающего невозможность воздействия на систему защиты и модификации ее параметров или конфигурации, результатом которых могло бы стать изменение реализуемой системой защиты политики разграничения доступа.

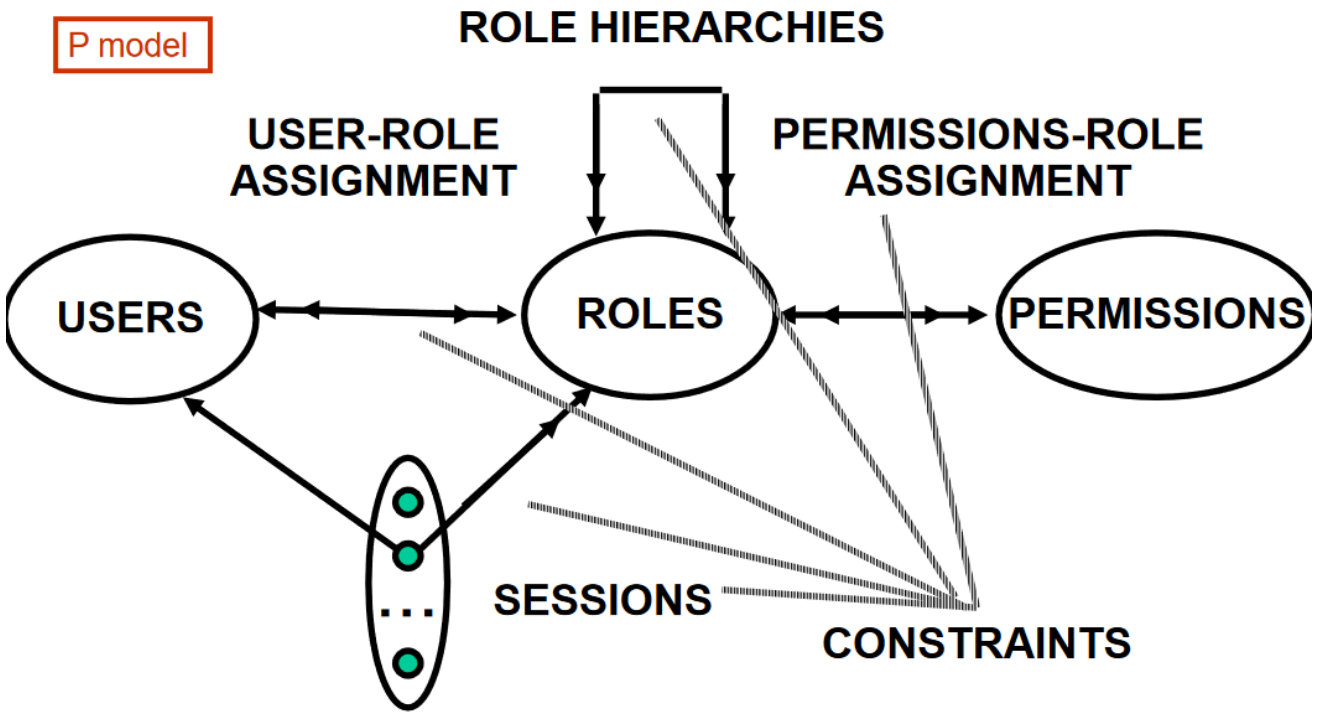
# Вопрос 2. Основные модели управления доступом.

**Ролевое управление доступом (RBAC)** – является развитием дискреционной политики разграничение доступа субъектов к объектам, но права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли.

**Свойства:**
1. Пользователи не могут передавать права на доступ к информации другим пользователям.
2. Распределение полномочий роли зависит только от выбранной политики безопасности.

**Достоинства:**
• Контроль доступа осуществляется над всей информацией обрабатываемой в АС организации.
• Простота процедуры добавления и удаления роли у пользователя.

**Недостатки:** – назначение привилегий ролям не влечет обновления привилегий для отдельных пользователей.



# Вопрос 2. Основные модели управления доступом.

**Модель управления доступом на основе атрибутов (Attribute-Based Access Control, ABAC)** – это метод управления доступом, который опирается на атрибуты пользователей, ресурсов и контекста для принятия решений о предоставлении доступа к информации и ресурсам.

Ключевые характеристики и описание ABAC:

**Атрибуты:** ABAC учитывает атрибуты, которые могут быть присвоены пользователям, ресурсам и контексту.

**Политики доступа:** В ABAC определяются политики доступа, которые опираются на атрибуты.

**Условия:** ABAC позволяет определять условия, которые должны выполняться, чтобы разрешить доступ. Эти условия могут включать в себя логические операции, сравнения атрибутов и временные ограничения.

**Автоматизация:** ABAC часто реализуется с использованием программных решений и автоматизации, что позволяет системе самостоятельно принимать решения о доступе на основе атрибутов и политик.

**Гибкость и точность:** Эта модель обладает большой гибкостью и позволяет определить точные и детализированные правила доступа на основе множества атрибутов и условий. Она может быть адаптирована к различным сценариям и требованиям безопасности.

**Централизованный и децентрализованный подходы:** ABAC может быть реализована в централизованных системах управления доступом или в децентрализованных приложениях, где атрибуты и политики доступа хранятся и управляются на разных уровнях.

# Вопрос 2. Основные модели управления доступом.

## Общая схема модели ABAC:

1. **Атрибуты пользователя:**
   - Роль (Role)
   - Должность (Position)
   - Отдел (Department)
   - Уровень доступа (Security Clearance)
   - Время доступа (Time of Access)
   - Местоположение (Location)
2. **Атрибуты ресурса:**
   - Тип ресурса (Resource Type)
   - Классификация (Classification)
   - Владелец ресурса (Resource Owner)
   - Группа ресурсов (Resource Group)
   - Доступные действия (Allowed Actions)
3. **Атрибуты контекста:**
   - Текущее время (Current Time)
   - Сетевая среда (Network Environment)
   - Текущее местоположение пользователя (User Location)
   - Состояние системы (System State)
4. **Политики доступа:**
   - Определение прав доступа с использованием атрибутов пользователей, ресурсов и контекста.
   - Пример: "Если Роль пользователя = 'Администратор' и Тип ресурса = 'Финансовые документы', то Разрешить Доступ."
5. **Условия:**
   - Условия, которые определяют, когда применяются политики доступа.
   - Пример: "Если Текущее время равно Рабочему времени (9:00 - 18:00), то применить политику доступа."
6. **Автоматизация:**
   - Принятие решений о доступе автоматически на основе атрибутов, политик и условий.

Результат: Разрешение или запрет доступа к ресурсам.

# Дисциплина «Технологии обеспечения информационной безопасности»

Лекция 4. «Модели управления доступом»

доцент кафедры КБ-4
кандидат педагогических наук, доцент
Пимонов Роман Владимирович