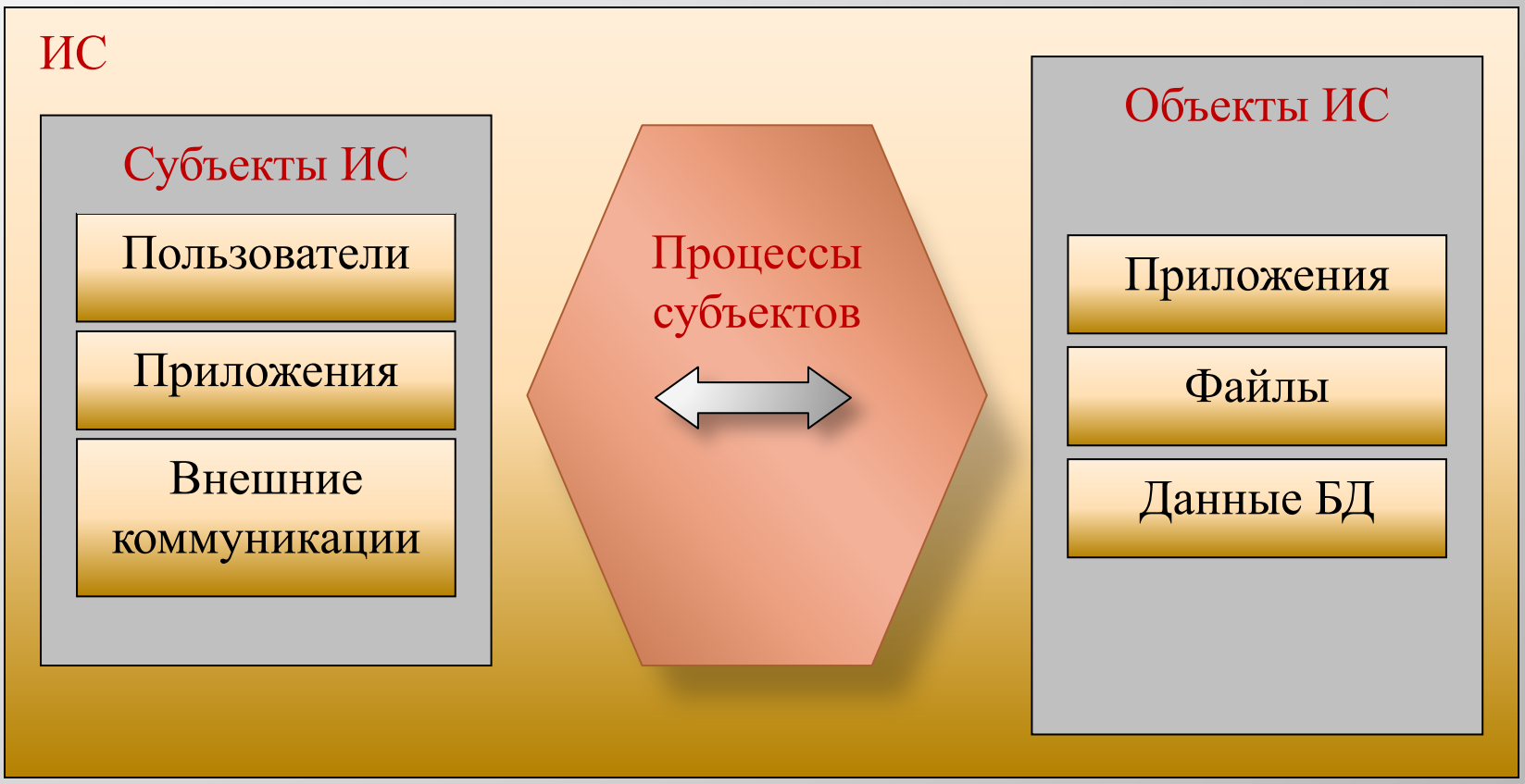
БЕЗОПАСНОСТЬ СИСТЕМ БАЗ ДАННЫХ

3. Модели безопасности

Субъектно-объектная модель доступа

- В общем случае разграничение доступа в ИС основано на использовании *субъектно-объектной модели доступа*.
- В этой модели ИС разделяется на субъекты (активные сущности), объекты (пассивные сущности) и порождаемые действиями субъектов процессы над объектами. При этом субъекты осуществляют доступ к объектам путем порождения процессов над ними.

Субъектно-объектная модель АИС



Модели безопасности

- Субъектно-объектная модель доступа, в свою очередь, реализуется в виде определенной *модели безопасности*.
- ***Модели безопасности*** представляют собой формализацию процедур логического управления доступом. Эти модели позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами).
- ***Модель безопасности*** есть формальное (математическое, схемотехническое, алгоритмическое) выражение и формулирование политики безопасности.

Модели безопасности

- В моделях безопасности реализуются процедуры логического управления доступом, являющиеся основным механизмом многопользовательских систем, (и, прежде всего, БД), который призван обеспечить конфиденциальность, целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Модели безопасности

- Модель безопасности включает:
  - модель АИС;
  - критерии, принципы, ограничения и целевые функции защищенности информации от угроз;
  - формализованные правила, ограничения, алгоритмы, схемы и механизмы безопасного функционирования системы.
- Работа МБ в формальной постановке. Имеется совокупность субъектов и набор объектов. Задача состоит в том, чтобы для каждой пары «субъект-объект» определить множество допустимых операций и контролировать выполнение установленного порядка.

Типы моделей безопасности

- В соответствии с рассмотренными типами политик безопасности, различают следующие типы моделей безопасности (моделей разграничения доступа):
  - ***дискреционные модели;***
  - ***мандатные модели;***
  - ***ролевые модели;***
  - ***модели безопасности информационных потоков;***
  - ***модели изолированной программной среды.***

Дискреционные модели

- Наибольшее развитие и применение получили дискреционные модели контроля доступа (Discretionary Access Control – DAC), основанные на матрице доступа.
- В дискреционных моделях область безопасного доступа строится как прямоугольная матрица (таблица), строки которой соответствуют субъектам доступа, столбцы объектам доступа, а в ячейках матрицы записываются разрешенные операции соответствующего субъекта над соответствующим объектом.
- По принципу организации матрицы доступа в реальных системах используются два подхода – ***централизованный*** и ***распределенный***.

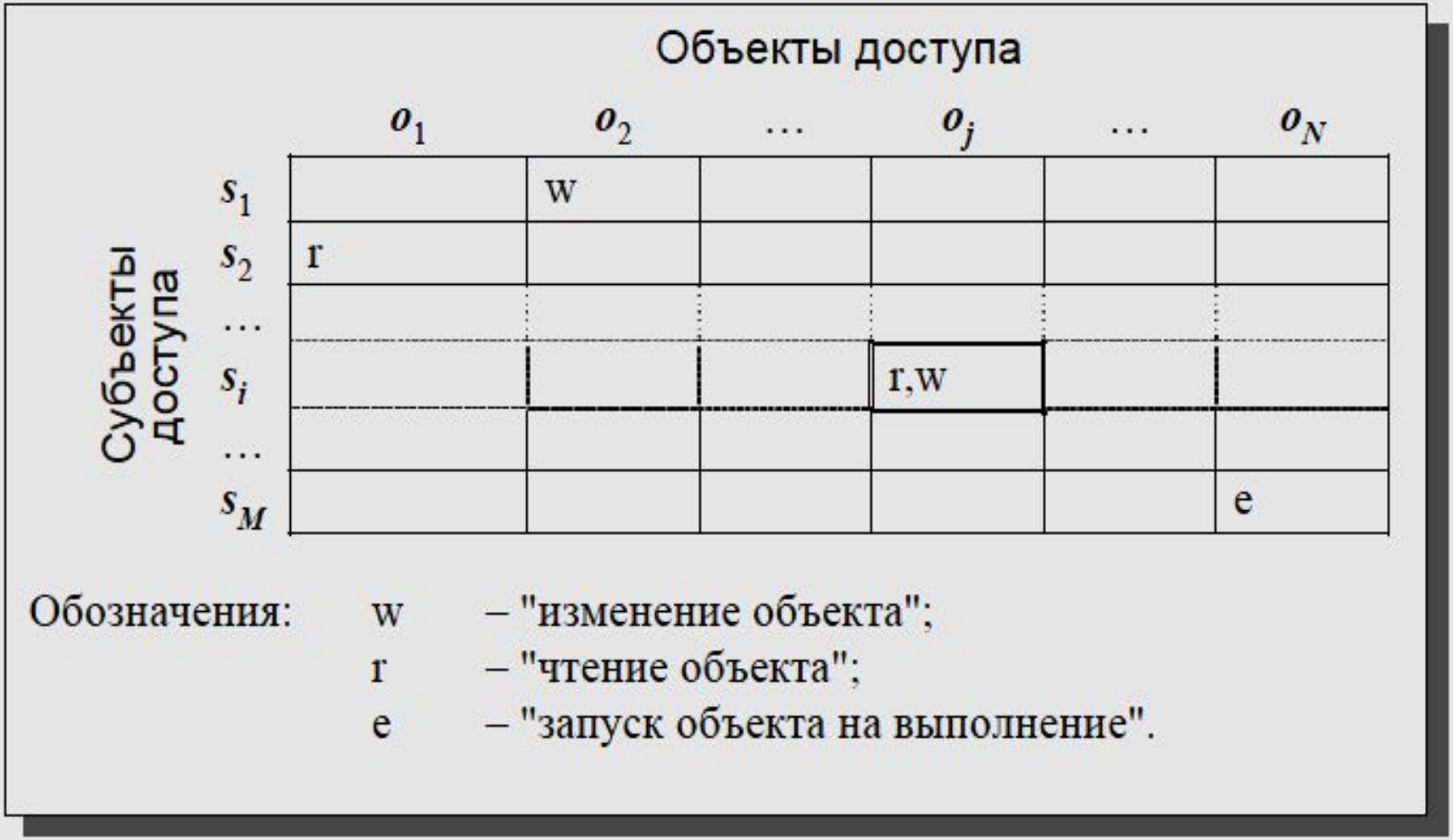
Централизованный подход к МД

- При *централизованном* подходе матрица доступа создается как отдельный самостоятельный объект с особым порядком размещения и доступа к нему.
- Количество объектов доступа и порождаемых пользователями субъектов доступа в реальных КС может достигать очень больших величин, и, кроме того, подвержено динамическому изменению.
- Поэтому при централизованном подходе в большинстве систем строки матрицы доступа характеризуют не субъектов, а непосредственно самих пользователей и их группы, зарегистрированные для работы в системе.

Централизованный подход к МД

- Для уменьшения количества столбцов матрицы, объекты доступа КС могут агрегатироваться в две группы – группу объектов, доступ к которым не ограничен (т. е. разрешен всем пользователям по любым операциям), и группу объектов, собственно, дискреционного доступа.
- Соответственно, в матрице доступа представляются права пользователей только к объектам второй группы, что позволяет существенно уменьшить ее размерность.
- Наличие или создание в матрице доступа столбца (строки) для какого-либо объекта фактически означает его регистрацию в системе дискреционного доступа с соответствующими правами соответствующих пользователей.

Матрица доступа



Обозначения:
- w – "изменение объекта";
- r – "чтение объекта";
- e – "запуск объекта на выполнение".

Пример матрицы доступа

Пользователи	Таблицы				
	1	2	3	4	5
Иванов	Ч, М				
Петров	Ч	Ч	Ч, М, С	Ч, М, С	Ч, М, С
Сидоров	Ч, М, С, У	Ч, М, С, У			
Михайлов	Ч, М, С, У	Ч, М, С, У	Ч, М, С, У	Ч, М, С, У	Ч, М, С, У

Виды доступа:

Ч – чтение

М – модификация

С – создание

У – удаление

Распределенный подход к МД

- При *распределенном* подходе матрица доступа как отдельный объект не создается, а представляется: или т. н. "списками доступа", распределенными по объектам системы, или т. н. "списками возможностей", распределенными по субъектам доступа.
- В первом случае каждый объект системы, помимо идентифицирующих характеристик, наделяется еще своеобразной биркой, представляющей, по сути, соответствующий столбец матрицы доступа.
- Во втором случае своеобразную бирку с перечнем разрешенных для доступа объектов (по сути, строку матрицы доступа) получает каждый субъект при своей инициализации.

Создание и изменение МД

- И централизованный, и распределенный принцип организации матрицы доступа имеет свои преимущества и недостатки.
- По *механизму создания и изменения* матрицы доступа, т. е., фактически по принципу управления доступом, выделяются также два подхода:
  - ***принудительное управление доступом;***
  - ***добровольное управление доступом.***

Принудительное управление доступом

- *Принудительное управление доступом* (ПУД) предусматривает единое централизованное администрирование доступом. Для этого в ИС выделяется специальный доверенный субъект (администратор), который (и только он) определяет разрешения на доступ всех остальных субъектов к объектам ИС.
- ПУД обеспечивает более жесткое централизованное управление доступом, но является менее гибким и менее точным в плане настройки системы разграничения доступа на потребности и полномочия пользователей.

Добровольное управление доступом

- Принцип *добровольного управлении доступом* (ДУД) основывается на парадигме ***«владения» объектами.*** Владельцами объектов являются пользователи, которые создали эти объекты или получили права владения ими.
- Тем самым, в дополнение к основным положениям субъектно-объектной модели вводится специальное отображение множества объектов на множество субъектов доступа, называемое владением, ставящее в каждый фиксированный момент времени каждому объекту системы подмножество субъектов доступа, инициализированных пользователем-владельцем объекта.

Добровольное управление доступом

- ***Правило.*** При ДУД права доступа к объекту определяют их владельцы.
- Из данного правила следует, что заполнение и изменение ячеек матрицы доступа осуществляют субъекты пользователей-владельцев соответствующих объектов.
- В большинстве систем права владения объектами могут передаваться.
- В результате при добровольном управлении доступом реализуется полностью децентрализованный принцип организации и управления процессом разграничения доступа.

Добровольное управление доступом

- ДУД обеспечивает большую гибкость настройки системы разграничения доступа, но затрудняет общий контроль и аудит состояния безопасности данных в системе.
- ДУД ориентировано на те системы, в которых количество объектов доступа является значительным или неопределенным. В этом случае перенос процесса управления доступом на владельцев объектов уменьшает общую мощность множества объектов управления, разделяя его на подмножества объектов управления.
- На практике может применяться комбинированный способ управления доступом, сочетающий полномочия на доступ между администратором ИС и владельцами объектами.

Достоинства и недостатки дискреционной модели

- *Достоинством ДМБ* является относительно простая реализация соответствующих механизмов защиты. Этим обусловлен тот факт, что большинство ИС в настоящее время обеспечивают выполнение положений именно данной модели безопасности.
- *Недостатком ДМБ* является ее статичность. Она не учитывает динамику изменений состояния ИС, не накладывает ограничений на состояния системы. Кроме этого, при использовании дискреционной политики безопасности возникает вопрос – определения правил распространения прав доступа и анализа их влияния на безопасность ИС.

Недостатки ДМБ

- Во многих ИС право владения объектом его прежним владельцем может быть передано другому пользователю. Кроме того в ОС декомпозиция системы на субъекты и объекты может меняться в различные моменты времени.
- В результате матрица доступа имеет динамический характер. Права доступа в таких системах могут "гулять", распространяться по субъектам системы.
- В этом случае возникает проблема самого понятия безопасности в смысле главного метода ее обеспечения – разграничения доступа, и требуется исследование условий и процессов распространения прав доступа.

Недостатки ДМБ

- В общем случае, при использовании ДМБ перед монитором безопасности ИС стоит алгоритмически неразрешимая задача: проверить – приведут ли его действия к нарушению безопасности или нет.
- В теоретическом плане впервые данная проблема была исследована Харрисоном, Руззо и Ульманом, которые для этого разработали специальную формальную модель дискреционного доступа, названную по их именам, сокращенно модель ХРУ (англ. – HRU).

Модель Харисона-Руззо-Ульмана

1. КС представляется тройкой сущностей:
   - множеством исходных объектов $\boldsymbol{O} = (o_1, o_2, \ldots, o_M)$;
   - множеством исходных субъектов $\boldsymbol{S} = (s_1, s_2, \ldots, s_N)$, при этом $\boldsymbol{S} \subseteq \boldsymbol{O}$;
   - матрицей доступа **A**, каждая ячейка которой специфицирует права доступа к объектам из конечного набора прав доступа $\boldsymbol{R} = (r_1, r_2, \ldots, r_K)$, т. е. $\mathbf{A}[s, o] \subseteq \boldsymbol{R}$.

- Условие $\boldsymbol{S} \subseteq \boldsymbol{O}$ означает, что в модели HRU субъекты доступа считаются "активизированными" состояниями некоторого подмножества объектов системы.

Модель Харисона-Руззо-Ульмана

2. Функционирование системы рассматривается с точки зрения изменений в матрице доступа **A**, которые определяются шестью примитивными операторами $\boldsymbol{O}_p$:

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

Модель Харисона-Руззо-Ульмана

3. Безопасность системы определяется некоторыми условиями на начальное состояние системы $\mathbf{Q}_0$, а также особенностями системы команд α.

- ***Критерий безопасности в модели*** **HRU**: Система является безопасной относительно права *r*, если для заданного начального состояния $\mathbf{Q}_0 = (\boldsymbol{S}_0, \boldsymbol{O}_0, \mathbf{A}_0)$ не существует применимой к $\mathbf{Q}_0$ последовательности команд, в результате которой право *r* будет занесено в ячейку матрицы $\mathbf{A}[s, o]$, в которой оно отсутствовало в начальном состоянии $\mathbf{Q}_0$.

Модель Харисона-Руззо-Ульмана

- Неформально безопасность системы будет определяться тем, возможно или нет в процессе функционирования системы получение некоторым субъектом определенного права доступа к некоторому объекту, которым он изначально не обладал.
- Для рассмотрения условий, при которых выполняется данный критерий, авторы HRU ввели понятие *монооперационных систем,* в которых каждая команда α выполняет один примитивный оператор, и представили теорему о существовании алгоритма, который проверяет, является ли исходное состояние монооперационной системы безопасным для данного права *r*.

Модель Харисона-Руззо-Ульмана

- К сожалению, теорема доказывает только само существование проверяющего алгоритма, но не дает каких-либо рекомендаций или других оснований для его разработки и построения.
- Вторая теорема авторов ХРУ гласит, что задача определения безопасности для данного права *r* в системах с запросами произвольного вида является алгоритмически неразрешимой.
- Иными словами теорема утверждает, что поведение систем на основе модели HRU с точки зрения безопасности является непредсказуемым!!!

Модель Харисона-Руззо-Ульмана

- Помимо проблем с неопределенностью распространения прав доступа в системах на основе модели HRU была подмечена еще одна серьезная проблема – отсутствие контроля за порождением потоков информации, и, в частности, – за порождением субъектов, следствием чего могут возникать "троянские" программы.
- В модели HRU легитимность инициируемых из объектов-источников субъектов доступа никак не контролируется. В результате, злоумышленник может осуществить неправомерный доступ к информации на основе подмены свойств субъектов доступа.

Другие дискреционные модели

- Результаты по модели HRU стимулировали поиски других подходов к обеспечению проблемы безопасности.
- В частности, для смягчения условий, в которых можно производить формальное доказательство безопасности, а также для введения контроля за порождением объектов были предложены модели:
  - **Типизованной матрицы доступа** (модель Type Access Matrix – TAM);
  - **TAKE-GRANT**.
- Однако и все эти разновидности дискреционной модели полностью не устраняют главных ее недостатков, связанных с сохранением безопасного состояния ИС.

Предпосылки создания мандатной модели безопасности

- Система управления безопасностью, организованная на основе матрицы доступа (МД) может оказаться уязвимой. Так, для рассмотренного выше примера МД, если Иванову удастся выдать себя за Михайлова, то он сможет получить максимальные полномочия в БД.

Субъекты доступа	Объекты доступа				
	1	2	3	4	5
Иванов	Ч, М				
Петров	Ч	Ч	Ч, М, С	Ч, М, С	Ч, М, С
Сидоров	Ч, М, С, У	Ч, М, С, У			
Михайлов	Ч, М, С, У	Ч, М, С, У	Ч, М, С, У	Ч, М, С, У	Ч, М, С, У

Предпосылки создания мандатной модели безопасности

- Очевидно, что одноуровневой модели безопасности данных может оказаться недостаточно для обеспечения надежной защиты от НСД к объектам КС. Необходимы какие-то дополнительные меры, которые бы препятствовали созданию такой ситуации.
- Кроме того, в дискреционных моделях существуют проблемы с контролем распространения прав доступа, и, в особенности, проблема "троянских" программ.
- Исследователи в области моделей безопасности, проанализировали – каким образом подобные проблемы решаются в некомпьютерных сферах и технологиях, в частности, в *секретном делопроизводстве*.

Предпосылки создания мандатной модели безопасности

- Были проанализированы правила и система назначений, изменений, лишений допусков сотрудников к работе с секретными документами, правила создания, уничтожения документов, присвоения или изменения грифов их секретности, в том числе и рассекречивания, а также другие особенности работы с секретными документами.
- В частности было отмечено, что правила получения доступа к документам различаются в зависимости от характера работы с ними – изучение (чтение) или изменение (создание, уничтожение, внесение дополнений, редактирование, т. е. запись в них).

Предпосылки создания мандатной модели безопасности

- На этой основе было "выявлено" два основных правила, гарантирующих безопасность:
- ***Правило 1.*** (no read up (NRU) – нет чтения вверх). Работник не имеет права знакомиться с документом (читать), гриф секретности (уровень безопасности) которого выше его степени допуска (уровня безопасности).
- ***Правило 2.*** (no write down (NWD) – нет записи вниз). Работник не имеет права вносить информацию (писать) своего уровня безопасности в документ с более низким уровнем безопасности (с более низким грифом секретности).

Модель Белла-ЛаПадулы

- Первой формальной моделью мандатного доступа является модель, разработанная в 1972–1975 г. г. американскими специалистами – сотрудниками MITRE Corporation Дэвидом Беллом и Леонардом ЛаПадулой (D. Elliott Bell, Leonard J. LaPadula), названная по их именам и сыгравшая огромную методологическую роль в развитии теории компьютерной безопасности.
- Основные положения модели Белла-ЛаПадулы сводятся к следующему.

Модель Белла-ЛаПадулы

1. Модель системы $\Sigma(v_0, \mathbf{Q}, F_T)$ представляется совокупностью:
   - множества объектов O доступа;
   - множества субъектов S доступа;
   - множества прав доступа R (в т. н. "классической" модели Белла-ЛаПадулы) всего два элемента – *read*-чтение и *write*-запись);
   - матрицы доступа $\mathbf{A}[s, o]$;
   - решетки Λ_L уровней безопасности L субъектов и объектов системы;
   - функции $F_L: S \cup O \rightarrow L$, отображающей элементы множеств S и O на множество L;

Модель Белла-ЛаПадулы

- множества состояний системы V, которое определяется множеством упорядоченных пар (F_L, **A**);
- начального состояния $v_0 \in V$;
- набора запросов **Q** субъектов на доступ (осуществление операций) к объектам, выполнение которых переводит систему в новое состояние;
- функции переходов $F_T(V \times \mathbf{Q}) \rightarrow V^*$, которая переводит систему из одного состояния V в другое V^* при выполнении запросов из **Q**.

Модель Белла-ЛаПадулы

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

$$\forall\ s \in \boldsymbol{S},\ \forall\ o \in \boldsymbol{O},\ \text{read} \in \mathbf{A}[s, o] \rightarrow \boldsymbol{F}_L(s) \geq \boldsymbol{F}_L(o)\ .$$

Модель Белла-ЛаПадулы

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

$$\forall\ s \in \boldsymbol{S},\ \forall\ o \in \boldsymbol{O},\ \text{write} \in \mathbf{A}[s, o] \rightarrow \boldsymbol{F}_L(o) \geq \boldsymbol{F}_L(s)\ .$$

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

Модель Белла-ЛаПадулы

- На основе введенных понятий, которые, как нетрудно видеть, выражают правила NRU и NWD политики мандатного доступа, авторы модели сформулировали следующий критерий безопасности.
- ***Определение* 4.** (*Критерий безопасности в модели Белла-ЛаПадулы*). Система $\Sigma(v_0, Q, F_T)$ безопасна тогда и только тогда, когда ее начальное состояние v_0 безопасно и все состояния, достижимые из v_0 путем применения конечной последовательности запросов из Q, безопасны.

Модель Белла-ЛаПадулы

- На основе данного критерия Белл и ЛаПадула доказали теорему, получившую название "***основной теоремы безопасности***" (ОТБ). Суть ее в следующем.
- На функцию переходов накладываются 4 ограничения, которые фактически выражают требования соблюдения в каждом состоянии системы правил NRU и NWD независимо от предыстории доступов.
- Иначе говоря, при переходах системы в новое состояние в матрице доступа не должно возникать никаких новых, и не должно сохраняться никаких старых отношений доступа, которые были бы небезопасны в смысле правил NRU и NWD.

Мандатная модель безопасности

- Основу ***мандатной*** (полномочной) модели безопасности (ММБ) составляет мандатное управление доступом (Mandatory Access Control – MAC), которое подразумевает, что:
  - Все субъекты и объекты системы должны быть однозначно идентифицированы;
  - Задается линейно упорядоченный набор меток конфиденциальности;
  - Каждому объекту системы присваивается метка конфиденциальности, определяющая его уровень секретности в КС;

Мандатная модель безопасности

- Каждому субъекту системы присвоена метка конфиденциальности, определяющая уровень доверия к нему в ИС. Значение метки конфиденциальности субъекта указывает на максимальное значение метки конфиденциальности объектов, к которым данный субъект имеет доступ. Метка конфиденциальности субъекта называется еще его уровнем доступа.

- Основная цель ММБ – предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т.е. противодействие возникновению в ИС информационных каналов сверху вниз.

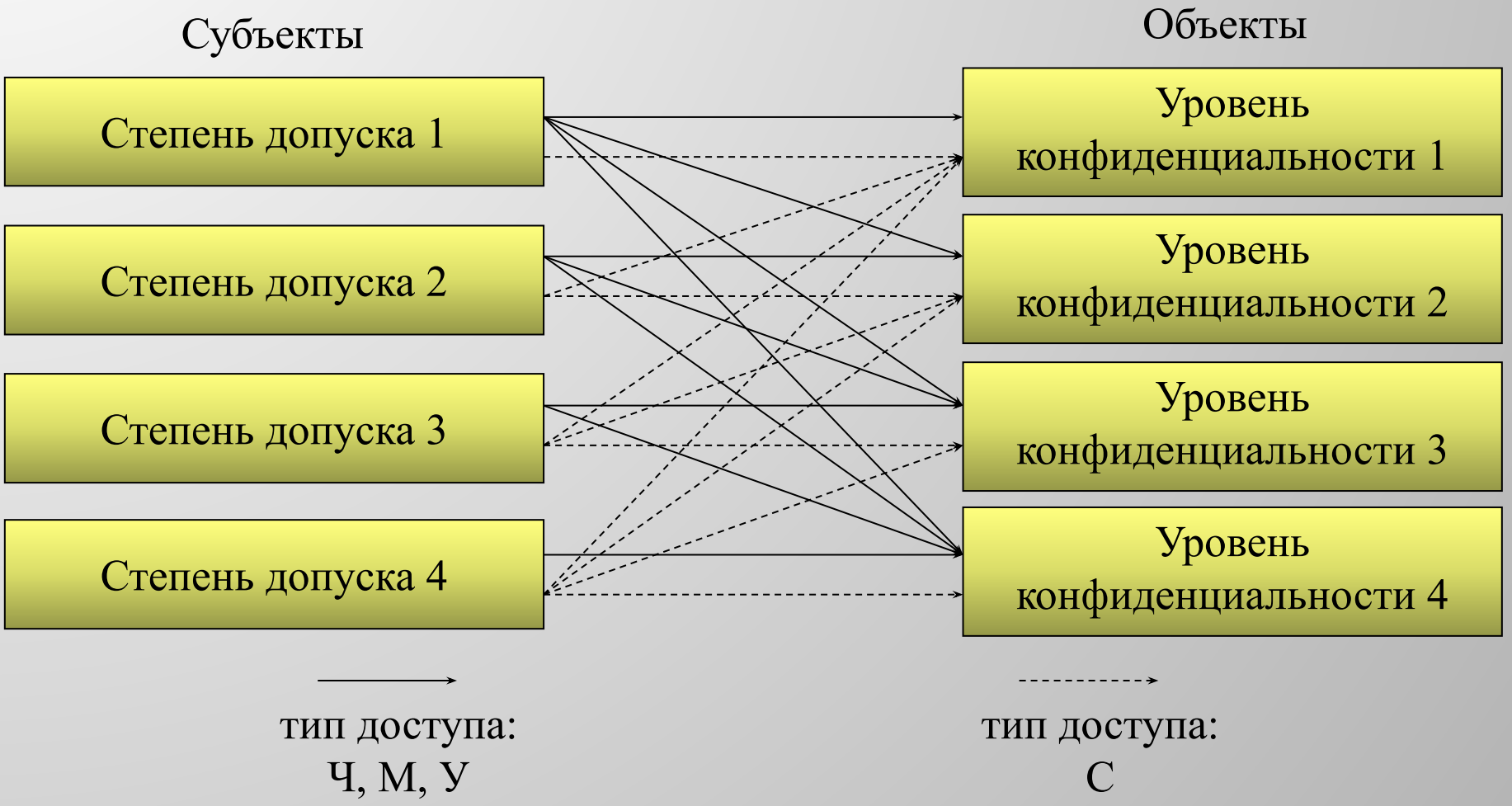
Реализация мандатной модели безопасности

- Реализуется ММБ. Все информационные ресурсы ИС классифицируются по степени конфиденциальности на ряд классов (уровней). Так, в военных ведомствах США применяется 4-х уровневая иерархия классов конфиденциальности информационных ресурсов:
  - совершенно секретно – СС;
  - секретно – С;
  - конфиденциально – К;
  - несекретно – Н.
- В отечественных силовых структурах применяется 5-уровневая иерархия классов конфиденциальности информационных ресурсов: ОВ; СС; С; ДСП; Н.

Реализация мандатной модели безопасности

- Соответственно субъекты доступа категорируются по соответствующим уровням доверия, путем получения т.н. допуска (допуск степени 1, степени 2 и т. д.). Уровни доверия субъектов соответствуют классам конфиденциальности информационных ресурсов АИС.
- Так, для иерархии классов, принятой в США, работник с допуском степени 1, имеет право работать с любой информацией уровней «СС», «С», «К» и «Н». Работник с допуском степени 2 имеет право работы с любой информацией уровней «С», «К» и «Н». Работник с допуском степени 3 имеет право работать с любой информацией уровней «К» и «Н». Наконец, работник с допуском степени 4 имеет право работать с любой информацией только уровня «Н».

Реализация мандатной модели безопасности



Функционально-зональный принцип разграничения доступа

- Внутри уровней ММБ может дополняться дискреционным принципом разграничением доступа.
- ММБ может дополняться элементами ***функционально-зонального*** принципа разграничения доступа, в соответствии с которым защищаемые сведения, помимо категории конфиденциальности, получают ***признак функциональной тематики*** (зоны). Соответственно, каждый работник, имеющий определенный уровень допуска к конфиденциальным сведениям, по своим функциональным обязанностям имеет определенный ***профиль деятельности,*** который предоставляет допуск или уточняет сферу допуска к категорированным сведениям только соответствующей тематики.

Достоинства мандатной модели безопасности

- В рамках ММБ доказывается важное утверждение, принципиально отличающее ее от ДМБ:
- **Если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушают ограничений, сформулированных политикой безопасности, то любое последующее состояние системы безопасно.**
- Кроме того для ИС с ММБ характерна более высокая степень надежности. Это связано с тем, что монитор безопасности такой системы должен отслеживать, не только правила доступа субъектов системы к объектам, но и состояния самой ИС. Таким образом, каналы утечки в системах данного типа не заложены в нее непосредственно (что наблюдается ДМБ), а могут появиться только при практической реализации системы.

Дополнение мандатной модели дискреционным доступом

- При мандатном доступе, разграничение осуществляется до уровня классов безопасности сущностей системы. Т.е. любой объект определенного уровня безопасности доступен любому субъекту соответствующего уровня безопасности (с учетом правил NRU и NWD).
- Нетрудно видеть, что это приводит к избыточности прав доступа для конкретных субъектов в пределах соответствующих классов безопасности, что противоречит самому понятию разграничения доступа.
- Для устранения данного недостатка мандатный принцип разграничения доступа часто дополняется дискреционным внутри соответствующих классов безопасности.

Расширения модели Белла-ЛаПадулы

- При практической реализации модели Белла-ЛаПадулы в реальных ИС возник ряд трудностей, послуживших основанием для многочисленных работ по ее критическому анализу. Основные из этих трудностей:
  - проблемы переходных процессов, изменяющих доверительные характеристики (уровни безопасности) субъектов и объектов доступа;
  - невозможность ограничиться в реальных ИС процессами, сопровождающимися только однонаправленными информационными потоками.

Расширения модели Белла-ЛаПадулы

- В частности, МакЛин привел концептуальное описание **Z-системы**, удовлетворяющей условиям ОТБ (основная теорема безопасности Белла-ЛаПадулы), но, вместе с тем, обеспечивающей возможность получения доступа любым субъектом к любому объекту по любому методу (read и write). МакЛин построил несколько расширений модели Белла-ЛаПадуллы, преодолевающих некоторые ее недостатки и приближающих ее к канонической модели.
- Альтернатива уполномоченным субъектам, избавляющая процессы безопасности от субъективного фактора, была реализована в мандатной модели **Low-Watermark (LWM).**

Расширения модели Белла-ЛаПадулы

- Еще одним расширением модели Белла-ЛаПадулы, имеющим важное прикладное значение, является введение методологии и техники совместного (группового) доступа. Для этого в мандатной модели добавляется функция группового доступа. Соответственно в матрице доступа A[s, o] системы добавляются строки, соответствующие субъектам группового доступа.
- Помимо дополнения матрицы доступа групповыми субъектами, вводятся механизмы реализации для них правил NRU и NWD, поскольку в состав субъекта группового доступа, могут входить субъекты с различным уровнем безопасности.

Расширения модели Белла-ЛаПадулы

- Таким образом, расширения модели Белла-ЛаПадулы обеспечивают устранение многих недостатков исходной модели, но не снимают всех ее недостатков .
- В частности, мандатный доступ снимает проблему "троянских программ", но только с точки зрения опасных потоков "сверху вниз". Однако в пределах одного класса безопасности, вопросы доступа решаются, как и в дискреционных моделях, на основе матрицы доступа, и, следовательно, для полного устранения проблемы "троянских программ" и в системах мандатного доступа требуется более тщательный и детализированный контроль информационных потоков.

Общие недостатки дискреционных и мандатных моделей

- При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Поэтому потребовались новые решения, способные эту сложность понизить.
- В основе рассмотренных ранее политик безопасности лежат отношения между отдельным пользователем (субъектом) и объектом доступа, определяемые либо внешним фактором (дискреционный доступ), либо уровнем безопасности (мандатный доступ), либо тематикой информации (тематический доступ).

Ролевые модели управления

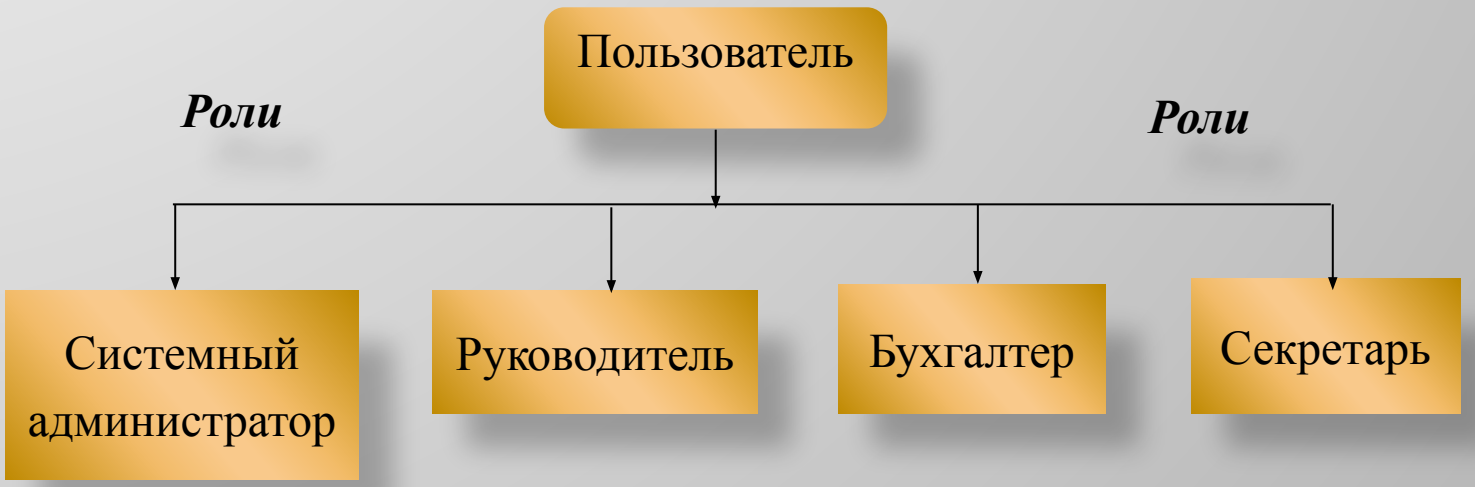
- Анализ различных организационно-управленческих схем показывает, что в реальной жизни сотрудники организаций выполняют определенные функциональные обязанности не от своего личного имени, а в рамках некоторой должности.
- Должность можно трактовать как определенную роль, которая представляет некоторую абстрактную, точнее обобщенную сущность, выражающую определенный тип функций и тип положения работника (подчиненность, права и полномочия).
- То есть, права и полномочия предоставляются конкретному сотруднику не лично, а через назначение его на определенную должность (роль), с которой он и получает некоторый типовой набор прав и полномочий.

Ролевое управление доступом

- В 2001 г. Институт стандартов и технологий США предложил стандарт ролевого управления доступом (РУД).
- Основой РУД является введение в субъектно-объектную модель дополнительной категории активных сущностей – ***ролей***.
- РУД приводит к тому, что права доступа субъектов системы к объектам группируются с учетом специфики их применения, образуя роли. В настоящее время РУД является составляющей многих современных систем и применяется в системах защиты СУБД и сетевых ОС.

Ролевое управление доступом

- Суть ***ролевого разграничения доступа*** состоит в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.



Ролевое управление доступом

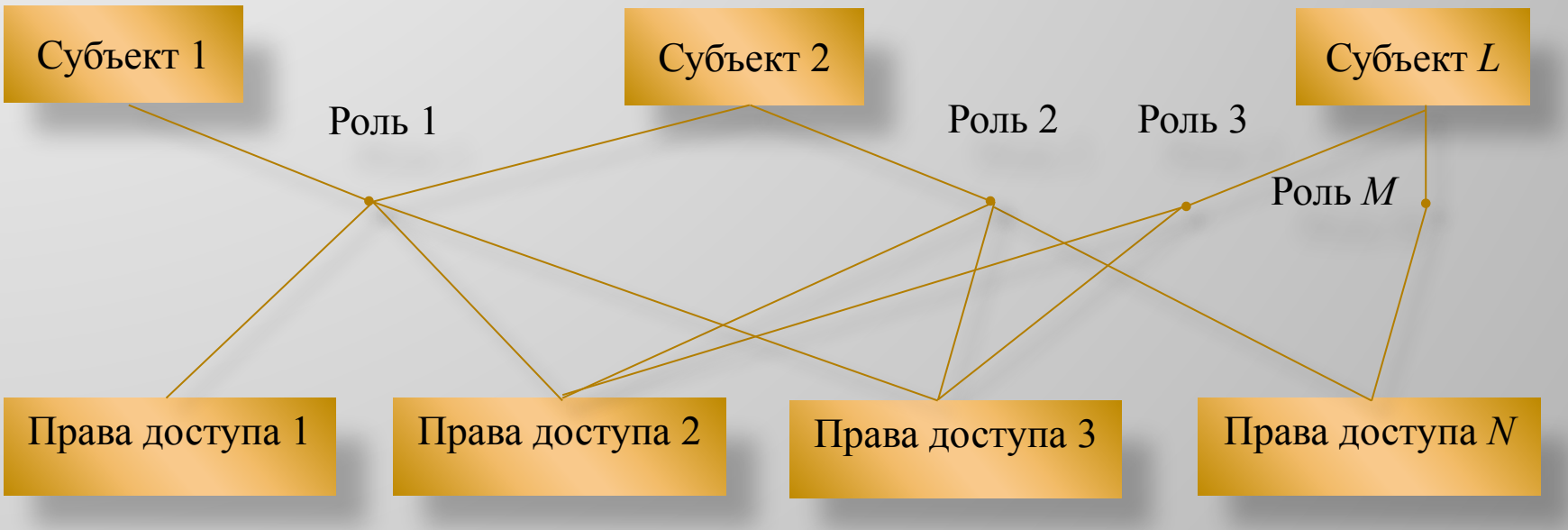
- Можно представить формирование ролей как иерархию, начиная с минимума прав (и максимума пользователей), приписываемых роли «сотрудник», с постепенным уточнением состава пользователей и добавлением прав («Секретарь», «Бухгалтер», «Руководитель подразделения», «Директор», «Системный администратор».
- Однако любая иерархия ролей не абсолютная. Предоставление прав осуществляется в соответствии с принципом минимизации привилегий. Каждой роли целесообразно разрешить только то, что необходимо для выполнения определенных служебных обязанностей.

Ролевое управление доступом

- ***Определение* 1.** Ролью называется активно действующая в ИС абстрактная сущность, обладающая логически взаимосвязанным набором полномочий, необходимых для выполнения определенных функциональных обязанностей пользователями системы.
- Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование. Он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей.

Ролевое управление доступом

- Ролей всегда значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.



Ролевое управление доступом

- РУД оперирует следующими основными понятиями:
  - ***пользователь*** (человек, автономный агент и т.п.);
  - ***сеанс работы пользователя***;
  - *роль* (определяется организационной структурой);
  - ***объект*** (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
  - ***операция*** (зависит от объекта: для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п.; для прикладных объектов операции могут быть более сложными);
  - ***право доступа*** (разрешение выполнять определенные операции над определенными объектами).

Ролевое управление доступом

- Ролям приписываются пользователи и права доступа; можно считать, что роли специфицируют отношения «многие ко многим» между пользователями и правами. Одной роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям.
- Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, и он становится обладателем объединения прав этих ролей.
- Одновременно пользователь может открыть несколько сеансов.
- Между ролями может быть определено отношение частичного порядка, называемое ***наследованием***.

Ролевое управление доступом

- Введение ролей приводит к двухэтапной организации системы разграничения доступа:
  - Создание ролей и определение их полномочий (прав доступа к объектам);
  - Назначение ролей пользователям системы.
- Соответственно формальные спецификации ролевых моделей должны регламентировать тем или иным способом (точнее в рамках той или иной политики) и определение полномочий ролям и назначение ролей пользователям.

Ролевое управление доступом

- Управление доступом в ролевых системах требует разбиения процесса функционирования системы и работы пользователя на сеансы, в каждом из которых, в свою очередь, выделяется две фазы:
  1. Авторизация в данном сеансе пользователя с одной или несколькими разрешенными для него ролями;
  2. Разрешение или запрещение субъектам пользователя доступа к объектам системы в рамках полномочий соответствующих ролей, с которыми авторизован в данном сеансе пользователь.

Ролевое управление доступом

- РУД сочетает:
  - мандатный подход к организации доступа через определенную агрегацию субъектов и объектов доступа, и тем самым обеспечивают жесткость правил разграничения доступа,
  - дискреционный подход, обеспечивающий гибкость в настройке системы разграничения доступа на конкретные функционально-организационные процессы предметной области КС.
- Эти особенности РУД позволяют строить системы с хорошей управляемостью в сложных системах при большим количестве пользователей и объектов.

Формальная спецификация ролевой модели

1. КС представляется совокупностью следующих множеств:
   - множества пользователей U;
   - множества ролей $\mathcal{R}$;
   - множества полномочий P;
   - множества сеансов C работы пользователей с системой.
- Множество полномочий P в общем виде задается специальными механизмами, объединяющими операции доступа и объекты доступа, например, запросами на обработку данных в СУБД, или иными именованными процедурами обработки данных, в том числе возможно высокого логического уровня.

Формальная спецификация ролевой модели

- 2. Ролевые отношения устанавливаются следующими отображениями множеств сущностей системы:

  $F_{P\mathfrak{R}} : P \times \mathfrak{R}$ – отображение множества полномочий на множество ролей;

  $F \cup \mathfrak{R} : U \times \mathfrak{R}$ – отображение множества пользователей на множество ролей.

- Отображение $F \cup \mathfrak{R}$ может реализовываться:
  - матрицей «пользователи-роли»;
  - на основе соотношения степеней допуска пользователей и грифов конфиденциальности ролей;
  - на основе соотношения разрешенных тематик пользователей и тематики ролей.

Формальная спецификация ролевой модели

3. Управление доступом в системе осуществляется на основе введения следующих функций:

fuser: C→U – значением функции u = fuser(c) является пользователь u ∈ U, реализующий данный сеанс работы;

froles: C→R – значением функции R = froles (c) является набор ролей R ⊆ ℜ из доступных пользователю, по которым пользователь работает в данном сеансе c ∈ C;

fpermissions: C→ P – значением функции P = fpermissions (c) является набор полномочий P ⊆ P, доступных по всем ролям, задействованным пользователем в данном сеансе c ∈ C.

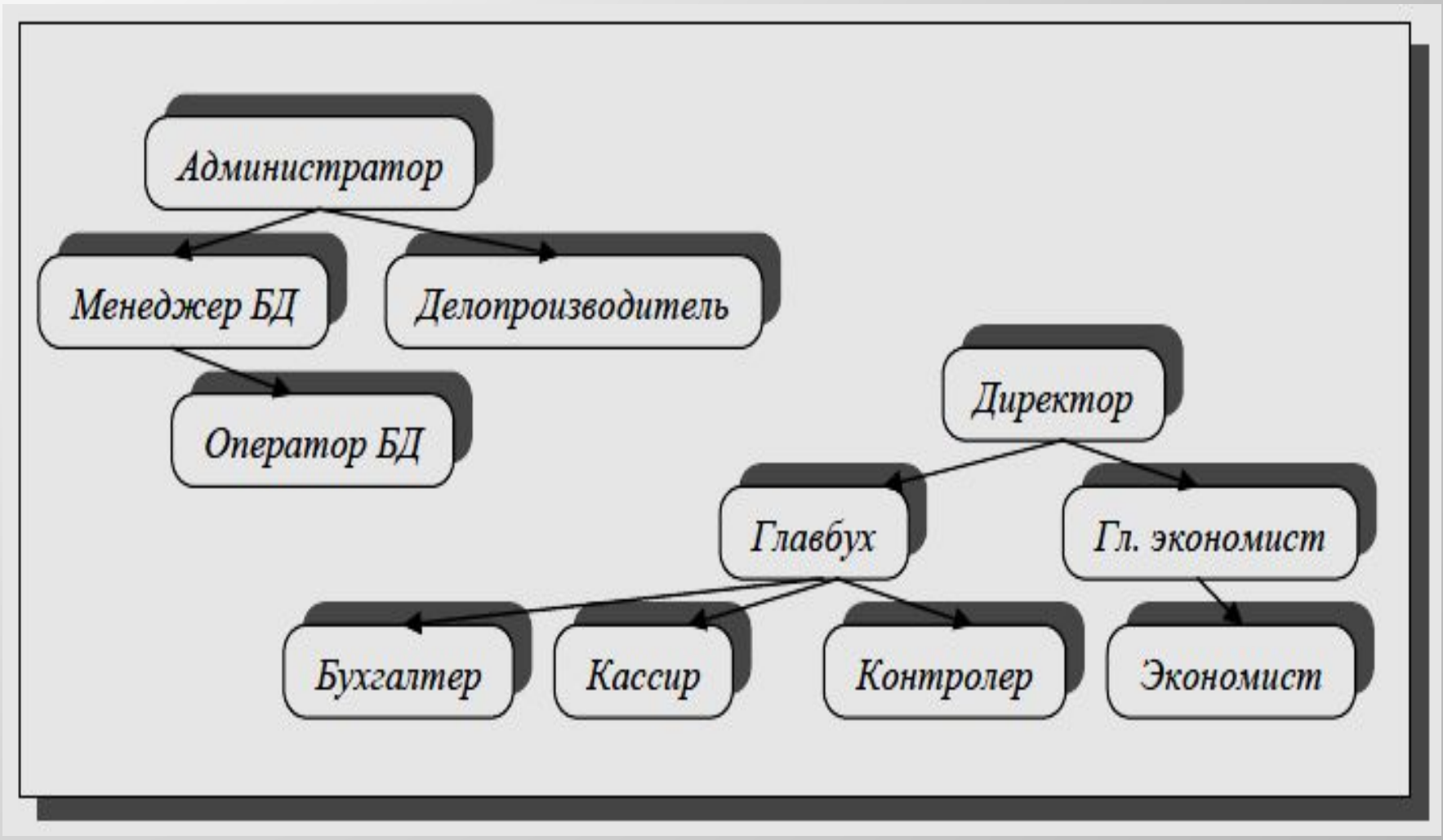
Формальная спецификация ролевой модели

- 4. Основное правило (критерий безопасности) ролевого доступа определяется следующим образом.
- ***Правило 1.*** Система функционирует безопасно, если и только если любой пользователь $u \in U$, работающий в сеансе $c \in C$, может осуществлять действия (операции, процедуры) в рамках полномочия $p \in P$, при условии: $p \in P$, где $P = f_{permissions}(c)$.
- Нетрудно видеть, что основной акцент в РУД заключается в особенностях отображения множества пользователей на множество ролей $F \cup \mathcal{R}$ и ограничений, накладываемых на функцию авторизации f_{roles}(c) пользователя в данном сеансе с разрешенными ему ролями.

Ролевая модель безопасности

- В зависимости от особенностей разрешения данных вопросов выделяют несколько разновидностей ролевых моделей:
  - с иерархической организацией системы ролей;
  - с взаимоисключающими на любые (все) сеансы ролями (модель статического распределения обязанностей);
  - с взаимоисключающими на один сеанс ролями (модель динамического распределения обязанностей);
  - с количественными ограничениями по ролям;
  - с группированием ролей и полномочий.

Иерархическая система ролей



Ролевая модель статического распределения обязанностей

- Особенностью некоторых предметных областей является запрет на предоставление определенного набора прав или полномочий в совокупности одному работнику.
- Подобные ограничения призваны усилить безопасность путем уменьшения вероятности злоумышленных действий по наборам связанных критических процессов и процедур.
- Если такие действия будут выполняться только разными работниками, то для осуществления злоумышленных действий потребуется сговор соответствующих работников. Вероятность злоумышленного развития ситуации в этом случае уменьшается.

Ролевая модель динамического распределения обязанностей

- Во многих организационно-управленческих и организационно-технологических структурах работникам приходится совмещать выполнение определенных групп обязанностей или подменять других работников на определенное время.
- В этом случае распределение функциональных или служебных обязанностей имеет динамический характер и организуется на определенный временной период.
- При этом часть полномочий, групп процедур также может иметь критический с точки зрения безопасности характер в плане одновременного их выполнения одним работником.

Ролевая модель с количественными ограничениями

- Отдельным направлением идеологии исключения потенциально опасных ситуаций, связанных с набором критических по безопасности прав и полномочий, является возможность наложения количественных ограничений на права и полномочия, агрегируемые одной отдельно взятой ролью.
- В других ситуациях требуется предоставление определенных полномочий как можно меньшему или строго ограниченному количеству сотрудников, скажем допуск к определенным опасным работам, право ознакомления с определенной информацией и т. п.

Ролевая модель с группировкой ролей и полномочий

- В некотором смысле противоположным по отношению к количественным ограничениям является группирование ролей и полномочий.
- По смыслу и определению роль представляет группирование прав и полномочий в отдельную логически обособленную их совокупность, имеющую самостоятельное значение в предметной области КС.
- Поэтому, прежде всего, устанавливается механизм, контролирующий агрегирование в одну роль некоторых логически связанных прав и полномочий

Комплексное использование ролевых моделей

- На практике могут использоваться комплексные подходы, сочетающие рассмотренные разновидности ролевых моделей, что позволяет существенно упростить системы разграничения доступа в КС, автоматизирующих сложные, нетривиальные организационно-технологические и управленческие схемы и процессы.
- Вместе с тем, в ролевых моделях нет строгих доказательств безопасности системы в соответствии с определенными формализованными критериями. Поэтому их безопасность основывается на контрольных механизмах дискреционных или мандатных моделей, средствами которых регулируется доступ ролевых субъектов к объектам системы.

Индивидуально-групповое разграничение доступа

- Это упрощенная, но наиболее широко применяемая разновидность РУД. Основные положения модели:

1. КС представляется совокупностью наборов сущностей:
   - множества объектов доступа $\boldsymbol{O}(o_1, o_2,\ldots, o_M)$;
   - множества пользователей $\boldsymbol{U}(u_1, u_2,\ldots, u_N)$;
   - множества рабочих групп пользователей $\boldsymbol{G}(g_1, g_2,\ldots, g_K)$;
   - множества прав доступа и привилегий $(r_1, r_2,\ldots, r_J)$;
   - матрицей доступа **A** размерностью $((N + K) \times M)$, каждая ячейка которой специфицирует права доступа и привилегии пользователей или их рабочих групп к объектам из конечного набора прав доступа и привилегий $\boldsymbol{R}$ $(r_1, r_2,\ldots, r_J)$, т. е. $\mathbf{A}[u, o] \subseteq \boldsymbol{R}$, $\mathbf{A}[g, o] \subseteq \boldsymbol{R}$.

Индивидуально-групповое разграничение доступа

- ***Определение***. Рабочей группой называется совокупность пользователей КС, объединенных едиными правами доступа к объектам и (или) едиными привилегиями (полномочиями) выполнения определенных процедур обработки данных.
- Рабочая группа представляет упрощенный аналог некоторой роли, которая формируется "на основе агрегирования в одну общую сущность пользователей, потребности в доступе которых к объектам системы подобны или близки.
- При этом у пользователей сохраняются и индивидуальные права доступа, которые не охватываются правами рабочей группы.

Индивидуально-групповое разграничение доступа

2. Групповые отношения в системе устанавливаются отображением множества пользователей на множество рабочих групп: $\boldsymbol{F}_{UG}$: $\boldsymbol{U} \times \boldsymbol{G}$ – такое, что одна рабочая группа объединяет нескольких пользователей, а один пользователь может входить в несколько рабочих групп (связи «многие-ко-многим»).

- При этом, в отличие от классической ролевой политики, разделение процесса функционирования системы на сеансы не является принципиальным, т. к. пользователь, входя в систему, всегда приобретает помимо своих индивидуальных прав одновременно и права доступа всех рабочих групп, в которые он включен по отношению $\boldsymbol{F}_{UG.}$

Индивидуально-групповое разграничение доступа

3. Функционирование системы основывается на введении и использовании следующих функций:

- f_{groups}: $\boldsymbol{U} \rightarrow \boldsymbol{G}$ – значением функции $f_{groups}(u) = G$ является набор рабочих групп $\boldsymbol{G} = \{g_{u1}, g_{u2}, \ldots\} \subseteq \boldsymbol{G}$, в которые пользователь u включен по отображению F_{UG};
- f_{users}: $\boldsymbol{G} \rightarrow \boldsymbol{U}$ – значением функции $\boldsymbol{U} = f_{users}(g)$ является набор пользователей $\boldsymbol{U} = \{u_{g1}, u_{g2}, \ldots\} \subseteq U$, которые рабочая группа g включает по отношению $\boldsymbol{F}_{UG}$.
- В практическом плане реализация функций f_{groups} и f_{users} производится посредством построения бинарной матрицы «пользователи-рабочие группы", ячейки которой заполняются при установлении отношения $\boldsymbol{F}_{UG}$.

Индивидуально-групповое разграничение доступа

- Управление индивидуально-групповым доступом в системе осуществляется на основе следующего правила (критерия безопасности) индивидуально-группового доступа.
- ***Правило.*** Система функционирует безопасно, если и только если любой пользователь $\boldsymbol{u} \in \boldsymbol{U}$ по отношению к любому объекту $\boldsymbol{o} \in \boldsymbol{O}$ может осуществлять доступ с правами $\boldsymbol{R}$, не выходящими за пределы совокупности индивидуальных прав $\mathbf{A}[\mathbf{u}, \mathbf{o}]$ и прав рабочих групп $\mathbf{A}[\boldsymbol{g}^{(u)}_i, \boldsymbol{o}]$, в которые пользователь входит по отношению $\boldsymbol{F}_{UG}$:

$$\boldsymbol{R} \subseteq \{\mathbf{A}[\boldsymbol{u}, \boldsymbol{o}] \cup \mathbf{A}[\boldsymbol{g}_{u1}, \boldsymbol{o}] \cup \mathbf{A}[\boldsymbol{g}_{u2}, \boldsymbol{o}] \cup \ldots\},$$

где $\{\boldsymbol{g}_{u1}, \boldsymbol{g}_{u2}, \ldots\} = \boldsymbol{f}_{groups}(\boldsymbol{u})$.

Индивидуально-групповое разграничение доступа

- Таким образом, права доступа пользователя к объекту складываются из его индивидуальных прав и прав всех рабочих групп, в которые он включен по отношению $\boldsymbol{F}_{UG}$.
- Следует отметить, что рабочие группы в полном смысле слова не являются ролями, т. к. они не реализуются в виде отдельных самостоятельно действующих субъектов доступа.
- Т. е. в системе не инициализируются отдельные субъекты доступа, действующие от имени рабочих групп, а действуют только субъекты пользователей, права которых в процессах доступа к объектам определяются на основе совокупности индивидуальных и групповых прав.

Индивидуально-групповое разграничение доступа

- В данной модели, как и в других разновидностях ролевых моделей, нет доказательства безопасного функционирования системы при выполнении правил разграничения доступа. Т. е. РУД в смысле безопасности идентична ДМБ.
- Но применение этой модели позволяет существенно упростить проектирование и управление системы при большом числе пользователей и объектов доступа.
- Недостатки модели: слабость защитных свойств, избыточность и дублирование в предоставлении прав доступа, проблемы проектирования системы рабочих групп.

РУД в реляционных СУБД

- В РУД не вводятся отдельные механизмы спецификации полномочий, а используется традиционный набор элементарных методов доступа (чтение, запись, и т. д.).
- Основу обработки данных в реляционных СУБД составляют запросы, обособляющие в отдельные именованные сущности, операции над данными (SELECT, INSERT, UPDATE, DELETE), объекты данных (таблицы) и результаты обработки.
- Сконструированные в SQL запросы хранятся в БД вместе с данными и составляют отдельную группу сущностей БД.
- Пользователям системы предоставляются права запускать определенные запросы.

Выводы по разделу

- Общая теория моделей безопасности (МБ) подразумевает выполнение всех предусмотренных требований, но существующие реализации МБ выполняют только часть из них, что значительно ограничивает возможные области их применения.
- С течением времени эта тенденция усиливается, и в настоящее время модели фактически разрабатываются специально под определенные реализации.
- МБ, как и большинство технологий безопасности, все больше переходят из области военных разработок в область коммерческого и общего использования, что в значительной мере связано с развитием сетевых ИТ.