Модели и методы разграничения доступа в базы данных

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).

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).

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.