**2. Управление логическим доступом**

Дискреционное управление доступом (Discretionary Access Control; DAC), которое подразумевает следующее:

‑ все субъекты и объекты системы должны быть идентифицированы;

‑ права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе матрицы доступа (МД, иногда ее называют матрицей контроля доступа). Такая модель получила название матричной (рисунок 5.1).

|  |
| --- |
| image002  Рисунок 5.1. – Схематичное изображение матрицы доступа |

Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы (О1…Оn) соответствует строка, а субъекту (С1…Сn) ‑ столбец. На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту как «доступ на чтение» (Read Only), «доступ на запись» (Write Only), «доступ на чтение-запись» (Read-Write) и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей дискреционного управления доступом. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата зависимое условие), часы (време-зависимое условие) в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия доступа к объектам обычно используются в системах управления базами данных. Кроме того, субъект с определенными полномочиями может передать их другому субъекту (если это не противоречит правилам политики безопасности).

Решение о доступе субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно избирательное управление доступом реализует принцип «что не разрешено, то запрещено», предполагающий явное разрешение доступа субъекта к объекту.

Матрица доступа (МД) ‑ наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных автоматизированных систем.

Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД. Каждый из этих способов представления МД имеет свои достоинства и недостатки, обуславливающие область их применения. Поэтому в каждом конкретном случае надо знать, во-первых, какое именно представление использует средство защиты и, во-вторых, какие особенности и свойства имеет это представление.

Избирательное управление доступом является основой требований к классам C2 и C1 стандарта США «Критерий оценки безопасности компьютерных систем» (Trusted Computer Systems Evaluation Criteria, известна как «Оранжевая книга»).

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности (accountability), а также имеет приемлемую стоимость и небольшие накладные расходы.

Мандатное управление доступом (Mandatory Access Control; MAC), подразумевает следующее:

‑ все субъекты и объекты системы должны быть однозначно идентифицированы;

‑ каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

‑ каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

В случае, если совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру, и, таким образом, в системе можно реализовать иерархически не исходящий (по ценности) поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Для моделирования полномочного управления доступом используется модель Белла-Лападула (Bell-LaPadulla model), включающая в себя понятия безопасного (с точки зрения политики) состояния и перехода. Для принятия решения на разрешение доступа производится сравнение метки критичности объекта с уровнем прозрачности и текущим уровнем безопасности субъекта. Результат сравнения определяется двумя правилами: простым условием защиты (simple security condition) и \*-свойством (\*-property). В упрощенном виде они определяют, что информация может передаваться только «наверх», то есть субъект может читать содержимое объекта, если его текущий уровень безопасности не ниже метки критичности объекта, и записывать в него, ‑ если не выше (\*-свойство).

Простое условие защиты гласит, что любую операцию над объектом субъект может выполнять только в том случае, если его уровень прозрачности не ниже метки критичности объекта.

Полномочное управление доступом составляет основу требований к классу B1 («Оранжевая книга»), где оно используется совместно с избирательным управлением.

Основное назначение полномочной политики безопасности ‑ регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая требованиям последней иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Изначально полномочная политика безопасности была разработана в интересах МО США для обработки информации с различными грифами секретности. Ее применение в коммерческом секторе сдерживается следующими основными причинами:

‑ отсутствием в коммерческих организациях четкой классификации хранимой и обрабатываемой информации, аналогичной государственной классификации (грифы секретности сведений);

‑ высокой стоимостью реализации и большими накладными расходами.