Дискреционная модель

Субъекты – те, кто выполняют действия. Объекты – те, над кем выполняют действия.

Модель реализована в установке, на ее основе и будем разбираться

|  |  |  |  |
| --- | --- | --- | --- |
|  | Файл | Реестр | Процесс |
| Пользователь 1 | В | 0 | С |
| Пользователь 2 | Ч | В | З |
| Пользователь 3 | Ч | 0 | В |

Элементы матрицы доступа могут иметь ссылки на специальные процедуры, результат которых позволяет принимать решение о праве доступа

Есть несколько вариантов задания матрицы доступа:

- листы возможностей: для каждого субъекта создается лист (файл) , в котором указывается все объекты, к которым он имеет доступ

- листы контроля доступа: для каждого объекта создается лист, в котором указаны все субъекты, которые имеют доступ

Размерность матрицы доступа мб очень большой. Следовательно, ее надо как-то уменьшить. Варианты решения:

- установление группы субъектов с одинаковыми правами, называются кликами

- группировка объектов по уровням категорий

Достоинства:

- простая в понимании и реализации

Недостатки:

- проблема контроля распространения прав доступа.

При передаче содержание файла происходит передача прав собственника на этот файл.

Многоуровневая

Объекты могут передавать между субъектами, находящимися на одном уровне или на уроне ниже

Пример в методичке говорит о том, что если вы каким-то чудом записали в файл информацию, то прочитать вы ее не сможете – прав не хватит

Структура система контроля

В виндовс нт каждый объект имеет свои атрибуты безопасности, определяемые в дескрипторе безопасности. Дескриптор содержит информацию о владельце объекта, а также список управления доступом ACL, в котором описываются права группы или пользователей к данному объекту

Существует 2 вида списка управления доступом:

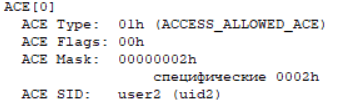
- дискреционный

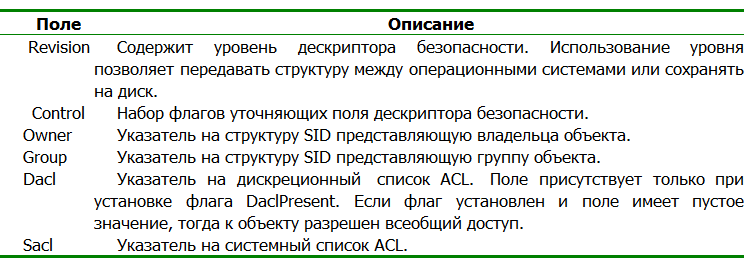
Управляется самим объектом и описывает права отдельных пользователей или групп

- системный

Задается админом и позволяет применить к объекту политику безопасности на уровне системы

Дальше рассказ про то, что себя представляет элемент списка





Субъекты – те, которые выполняют действия. Объекты – те, над кем выполняют действия.

Дискреционная модель доступа

Создается таблица – матрица доступа. В ней указываются все субъекты, все объекты. На пересечении субъекта и объекта указывается вид права.

Есть несколько вариантов задания матрицы доступа:

- листы возможностей: для каждого субъекта создается лист (файл), в котором указывается все объекты, к которым он имеет доступ

- листы контроля доступа: для каждого объекта создается лист, в котором указаны все субъекты, которые имеют доступ

Размерность матрицы доступа мб очень большой. Следовательно, ее надо как-то уменьшить. Варианты решения:

- установление группы субъектов с одинаковыми правами, называются кликами

- группировка объектов по уровням категорий

Многоуровневая модель

У объектов появляется уровень секретности, а у субъектов уровень доступа.

Каждый объект О имеет метку с информацией о классе c(O). Каждый субъект также имеет метку, содержащую информацию о том, какой класс доступа c(S) он имеет. Мандатный контроль сравнивает метки и удовлетворяет запрос субъекта S к объекту О на чтение, если c(S) > c(0) и удовлетворяет запрос на запись, если c (S) < c(0)

Модель Белла-Лападулы