**Лаба1**

**Политика безопасности** — это индивидуальный для каждой организации набор правил и средств для защиты информации.

Она реализует управление доступом через два основных вида:

1. **Избирательная (Дискреционная) политика**
   * **Суть:** Доступ определяет администратор, задавая, кто (субъект) и к каким данным (объектам) имеет право обращаться.
   * **Модель:** Проще всего представляется в виде **матрицы доступа** (строки — пользователи, столбцы — файлы, ячейки — права: чтение, запись и т.д.).
   * **Применение:** Широко используется в коммерческих организациях, так как гибкая и соответствует требованиям по разграничению прав.
2. **Полномочная (Мандатная) политика**
   * **Суть:** Доступ определяется **метками конфиденциальности** у данных и **уровнями допуска** у пользователей.
   * **Правило:** Пользователь может получить доступ только к тем данным, чья метка конфиденциальности не превышает его уровень допуска.
   * **Главная цель:** Жёстко предотвратить утечку информации «сверху вниз» (от более секретных данных к менее секретным пользователям).

**Ключевой вывод:** Выбор политики безопасности зависит от технологии и потребностей организации. Её реализация должна быть тщательно продумана, чтобы не заблокировать доступ к нужной информации, формально соблюдая правила.

**1. Основной принцип:**

* Каждый объект (файл, устройство) имеет **владельца** (пользователя).
* **Владелец** имеет полные права над своим объектом, включая право **передавать права** доступа другим пользователям.

**2. Механизм реализации:**

* Права доступа описываются с помощью **матрицы доступа**.
* **Строки** матрицы — это пользователи (U).
* **Столбцы** — это объекты (O).
* **Ячейка на пересечении** строки и столбца содержит **множество разрешённых действий** (S) данного пользователя с данным объектом (например, {Чтение, Запись}).

**3. Суть на примере:**

* В приведённом примере **Администратор** имеет полные права на все объекты.
* **Гость** может только читать "Файл\_1" и использовать CD-RW.
* **Пользователь\_1** является владельцем "Файла\_2" (имеет на него полные права) и может читать "Файл\_1".

**Главный вывод:** Дискреционная политика основана на воле владельца объекта, который сам решает, кому и какие права на него предоставить. Матрица доступа — это наглядное представление этой политики.

**Лаба2**

Подсистемы идентификации и аутентификации выполняют роль "переднего края обороны" в системах защиты информации, поскольку именно они первыми подвергаются атакам злоумышленников. Парольные системы, остающиеся наиболее распространенным методом аутентификации, требуют комплексного подхода к обеспечению безопасности.

К паролям предъявляются три основных требования: минимальная длина не менее 6 символов; использование различных групп символов (строчные и прописные буквы, цифры, специальные символы); запрет на использование реальных слов и имен собственных. К подсистеме аутентификации также выдвигаются требования: установка максимального срока действия паролей; ограничение количества попыток ввода (обычно не более трех); введение временной задержки при ошибочном вводе.

**Ключевой аспект:** Количественная оценка стойкости парольной защиты основана на вероятностной модели. Вероятность подбора пароля злоумышленником вычисляется по формуле P = (V·T)/Aᴸ, где V - скорость перебора, T - срок действия пароля, A - мощность алфавита, L - длина пароля. Для обеспечения заданного уровня безопасности необходимо определить минимальное количество возможных паролей S\* = [V·P/T] и подобрать такие параметры A и L, чтобы выполнялось условие S\* ≤ Aᴸ.

**Практическое применение:** Например, при вероятности подбора P=10⁻⁶, сроке действия пароля T=7 дней и скорости перебора V=10 паролей в минуту, требуемая стойкость обеспечивается паролем из 8 символов латинского алфавита (A=26) или 6 символов, включающих буквы и цифры (A=36). Это демонстрирует, как теоретические расчеты непосредственно влияют на практические рекомендации по составлению паролей.