# Лабораторна робота №5

# дискреційна модель

***Мета роботи***: Ознайомитися з проблемами реалізації політик безпеки в комп'ютерних системах на прикладі дискреційної моделі.

***Теоретичні відомості до лабораторної роботи***

Під політикою безпеки розуміють набір норм, правил і практичних прийомів, що регулюють управління, захист і розподіл цінної інформації. Політика безпеки задає механізми управління доступу до об'єкту, визначає як дозволені, так і заборонені доступи.

Політика безпеки реалізується через адміністративно−організаційні заходи, фізичні і програмно−технічні засоби та визначає архітектуру системи захисту. Для конкретної організації політика безпеки повинна носити індивідуальний характер і залежати від конкретної технології обробки інформації і тих програмних і технічних засобів, що використовуються.

Політика безпеки визначається способом управління доступом, який задає порядок доступу до об'єктів системи. Розрізняють два основних види політики безпеки: виборчу і повноважну.

*Виборча політика*безпеки заснована на виборчому способі керування доступом. Виборче (або дискреційне) керування доступом характеризується заданою адміністратором безліччю дозволених відносин доступу (наприклад, у вигляді трійок об'єкт − суб'єкт − тип доступу). Зазвичай для опису властивостей виборчого керування доступом застосовують математичну модель на основі матриці доступу**.**

Матриця доступу є матрицею, в якій стовпчик відповідає об'єкту системи, а рядок − суб'єкту. На перетині шпальти і рядка матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» і т.п.

*Повноважна політика* безпеки заснована на повноважному (мандатному) способі керування доступом. Повноважне (або мандатне) керування доступом характеризується сукупністю правил надання доступу, визначених на множині атрибутів безпеки суб'єктів і об'єктів, наприклад, в залежності від мітки конфіденційності інформації та рівня допуску користувача. Повноважне керування доступом передбачає, що:

* 1. всі суб'єкти і об'єкти системи однозначно ідентифіковані;
  2. кожному об'єкту системи привласнена мітка конфіденційності інформації, яка визначає цінність даних, що містяться в ньому;
  3. кожному суб'єкту системи присвоєно певний рівень допуску, який визначає максимальне значення мітки конфіденційності інформації об'єктів, до яких суб'єкт має доступ.

Чим важливіше об'єкт, тим вище його мітка конфіденційності. Тому найзахищеними виявляються об'єкти з найбільш високими значеннями мітки конфіденційності.

Основне призначення повноважної політики безпеки − регулювання доступу суб'єктів системи до об'єктів з різними рівнями конфіденційності, запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливих проникнень з нижніх рівнів на верхні.

При виборі і реалізації політики безпеки в комп'ютерній системі, як правило, працюють наступні кроки:

1. В інформаційну структуру вноситься структура цінностей (визначається цінність інформації) і проводиться аналіз загроз і ризиків для інформації та інформаційного обміну.
2. Визначаються правила використання для будь−якого інформаційного процесу, права доступу до елементів інформації з урахуванням даної оцінки цінностей.

*Математична модель* дискреційної  *політики безпеки*

Нехай О − множина об'єктів, U − множина користувачів, S − множина дій користувачів над об'єктами. Тоді дискреційна політика визначає відображення O → U (об'єктів на користувачів − суб'єктів). Згідно з даним відображенням, кожен об'єкт *Oj∈O* оголошується власністю відповідного користувача *Uk∈U*, який може виконувати над ними певну сукупність дій *Si∈S*, в яку можуть входити декілька елементарних дій (читання, запис, модифікація і т.д.). Користувач, який є власником об'єкта, іноді має право передавати частину або всі права іншим користувачам (володіння адміністраторськими правами).

Зазначені права доступу користувачів−суб'єктів до об'єктів комп'ютерної системи записуються у вигляді так званої матриці доступу. На перетині *i*−го рядка та *j*−ого стовпчика даної матриці розташовується елемент *Sij* – множина дозволених дій *j*−ого користувача над *i*−м об'єктом.

*Приклад*. Нехай є множина з трьох користувачів {Адміністратор, Гість, Користувач \_1} і множина з чотирьох об'єктів {Файл\_1, Файл\_2, CD−RW, Flash−карта}. Множина можливих дій включає наступні: {Читання, Запис, Передача прав іншому користувачеві}. Дія «Повні права» дозволяє виконання всіх трьох дій, дія «Заборона» забороняє виконання всіх перерахованих дій. В даному випадку, матриця доступу, що описує дискреційну політику безпеки, може виглядати наступним чином (табл. 7.1).

Таблиця 7.1 − Приклад матриці доступу

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Об’єкт / Суб’єкт | Файл\_1 | Файл\_2 | Flash−карта | CD−RW |
| 1. Адміністратор | Повні права | Повні права | Повні права | Повні права |
| 2. Гість | Заборона | Читання | Читання | Заборона |
| 3. Користувач\_1 | Читання,  передача прав | Читання,  запис | Повні права | Заборона |

Наприклад, Користувач \_1 має права на читання і запис в Файл\_2. Передавати ж свої права іншому користувачеві він не може.

Користувач, що володіє правами передачі своїх прав доступу до об'єкта іншому користувачеві, може зробити це. При цьому, користувач, який передає права, може вказати безпосередньо, які зі своїх прав він передає іншому.

Якщо Користувач \_1 передає право доступу до Файлу\_1 на читання користувачеві Гість, то у користувача Гість з'являється право читання з Файла\_1.

***Порядок виконання роботи***

Нехай множина S можливих операцій над об'єктами комп'ютерної системи задана трьома станами:

*S* = {«Доступ на читання», «Доступ на запис», «Передача прав»}.

Для заданої множини S виконати наступне

1. Отримати дані про кількість користувачів і об'єктів комп'ютерної системи з таблиці 7.2 (відповідно до варіанту).

Таблиця 7.2 − Варіанти завдань до лабораторної роботи

|  |  |  |
| --- | --- | --- |
| Варіант | Кількість суб’єктів  доступу (користувачів) | Кількість об’єктів  доступу |
| 1 | 3 | 3 |
| 2 | 4 | 4 |
| 3 | 5 | 6 |
| 4 | 6 | 5 |
| 5 | 7 | 6 |
| 6 | 3 | 5 |
| 7 | 4 | 6 |
| 8 | 5 | 3 |
| 9 | 6 | 4 |
| 10 | 7 | 4 |
| 11 | 3 | 4 |
| 12 | 4 | 5 |
| 13 | 5 | 5 |
| 14 | 6 | 6 |
| 15 | 7 | 3 |
| 16 | 3 | 6 |
| 17 | 4 | 3 |
| 18 | 5 | 4 |
| 19 | 6 | 5 |
| 20 | 7 | 5 |

1. Реалізувати програмний модуль, що створює матрицю доступу користувачів до об'єктів комп'ютерної системи, який виконує наступне:
   1. вибрати ідентифікатори користувачів, що використовуватимуться при вході в комп'ютерну систему (по одному ідентифікатору для кожного користувача, кількість користувачів вказано для варіанту). Наприклад, множина з трьох ідентифікаторів користувачів {Ivan, Sergey, Boris}. Один з даних ідентифікаторів повинен відповідати адміністратору комп'ютерної системи (користувач, що володіє повними правами доступу до всіх об'єктів);
   2. реалізувати програмне заповнення матриці доступу, що містить кількість користувачів і об'єктів відповідно до варіанта.
      1. При заповненні матриці доступу необхідно враховувати, що один з користувачів повинен бути адміністратором системи (припустимо, Ivan). Для нього права доступу до всіх об'єктів повинні бути виставлені як повні.
      2. Права інших користувачів для доступу до об'єктів комп'ютерної системи повинні заповнюватися випадковим чином за допомогою датчика випадкових чисел. При заповненні матриці доступу необхідно враховувати, що користувач може мати кілька прав доступу до деякого об'єкту комп'ютерної системи, мати повні права, або зовсім не мати прав.
      3. Реалізувати програмний модуль, який демонструє роботу в дискреційній моделі політики безпеки.
2. Даний модуль повинен виконувати наступні функції:
   1. При запуску модуля повинен запитуватися ідентифікатор користувача (проводиться ідентифікація користувача), при успішній ідентифікації користувача повинен здійснюватися вхід в систему, при неуспішній − виводитися відповідне повідомлення.
   2. При вході в систему після успішної ідентифікації користувача на екрані повинен друкуватися список всіх об'єктів системи із зазначенням переліку всіх доступних прав доступу ідентифікованого користувача до даних об'єктів.
   3. Після виведення на екран переліку прав доступу користувача до об'єктів комп'ютерної системи, необхідно організувати очікування вказівок користувача на здійснення дій над об'єктами в комп'ютерній системі. Після отримання команди від користувача, на екран необхідно вивести повідомлення про успішність або неуспішності операції. При виконанні операції передачі прав повинна модифікуватися матриця доступу. Програма повинна підтримувати операцію виходу з системи, після якої йде запит ідентифікатору користувача.
3. Виконати тестування розробленої програми, продемонструвавши реалізовану модель дискреційної політики.
4. Оформити звіт до лабораторної роботи.

***Вимоги до звіту:***

1. Титульний лист
2. Вступ (про політики безпеки в захисті інформації);
3. Основний розділ, в якому описати таке:

− алгоритм формування матриці доступу користувачів до об'єктів комп'ютерної системи;

− організацію заповнення матриці доступу;

− роботу модуля з дискреційною моделлю політики безпеки

− навести програмний код розробки з коментарями;

− відобразити отримані результати, навести копії екранів.

1. Сформулювати висновки.

***Питання для самоконтролю***

1. Що розуміється під політикою безпеки в комп'ютерній системі?
2. В чому полягає модель дискреційної політики безпеки в комп'ютерній системі?
3. Що розуміється під матрицею доступу в дискреційній політиці безпеки? Що зберігається в даній матриці?
4. Які дії проводяться над матрицею доступу в тому випадку, коли один суб'єкт передає іншому суб'єкту свої права доступу до об'єкта комп'ютерної системи?