

## **АНАЛІЗ ДЕСКРИПТОРІВ БЕЗПЕКИ ТА СПИСКІВ КОНТРОЛЮ ДОСТУПУ**

Гудзь В.В. ст. гр. 13І – 06  
Науковий керівник - к.т.н, доцент, Войтович О.П.

Основною проблемою при захисті та оцінці вразливих місць в операційних системах є контроль доступу, який реалізується на рівні користувачів. В залежності від задач, що потрібно вирішувати за допомогою обчислювальної системи, обирається тип контролю доступу, який буде впроваджений в інформаційну систему. Помилка в питанні розмежування прав між користувачами може призвести до витоку цінної інформації або її повної втрати.

Списки контролю доступу є одним з можливих методів захисту інформаційних ресурсів в операційній системі. Оскільки число користувачів різних автономних систем невідомо зростає, тому гостро постає питання розмежування їхніх повноважень в інформаційній системі. Існує два типи списків контролю доступу. Перший працює на рівні користувачів та являю собою механізм захисту ресурсів таких як файли та папки. Другий тип контролю доступу – це системний список управління доступом та механізм контролю над повідомленнями аудиту які пов'язані з інформаційним ресурсом, тобто кількість успішних та невдалих спроб доступу.

Робота списків контролю доступу основана на створенні записів контролю доступу, в яких поєднується ідентифікатор безпеки користувача разом із маскою доступу. Запис контролю доступу може як дозволяти так і забороняти право на використання певного ресурсу. Кожен запис зберігається в базі даних, яка знаходиться в метафайлі \$Secure файлової системи NTFS.

Для розробки програми, за допомогою якої буде реалізовуватись призначення прав доступу для ресурсів операційної системи необхідно використати API-функції та бібліотеку класів .NET Framework, що містить простір імен System.Security.AccessControl.

Класи, що відносяться до даного простору імен, дозволяють програмним способом створювати і змінювати системні та користувацькі списки контролю доступом для різних захищених ресурсів.

В подальшому планується розглянути можливості забезпечення безпеки управління доступом Windows для розділів реєстру за допомогою класу імен RegistrySecurity, а також роботу мережевих списків доступу як методу захисту інформації на мережевому рівні.