УДК 004.056:061.68

ДИСКРЕЦІЙНА МОДЕЛЬ РОЗМЕЖУВАННЯ ДОСТУПУ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Ігнатьєв І.В.[1)], Касянчук М.М.[2)], Лисий Н.В.[3)], Осадчук О.Й.[4)]

Тернопільський національний економічний університет

[1)] інженер; [2)] к.ф.-м.н., доцент; [3)] магістрант

[4)]Тернопільський обласний онкологічний диспансер, лікар УЗД

I. Постановка проблеми

В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу [1], що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Захист інформації має серйозні завдання, адже у випадку витоку інформації організація може понести непоправні збитки, а саме, фінансові втрати, які в підсумку можуть привести до деструкції організації. Але найбільш суттєві наслідки у випадку витоку інформації, власником якої є держава, оскільки в результаті будуть страждати інтереси самої держави.

З урахуванням майбутнього розвитку інформатизації, проникнення інформаційних технологій у найважливіші сфери життя суспільства необхідно передбачити перехід від принципів гарантування безпеки інформації до принципів інформаційної безпеки.

II. Мета роботи

Метою дослідження є розробка дискреційної моделі розмежування доступу в системах захисту інформації.

III. Побудова дискреційної моделі розмежування доступу в системах захисту інформації

Для реалізації дискреційної моделі розмежування доступу необхідно розробити дискреційний принцип розмежування. Ресурси, що підлягають захисту, розташовуються на файловому сервері, відповідно необхідно розглянути структури каталогів, в яких розташовуються ресурси. Всі ресурси чітко розділені по окремих каталогах, до яких мають доступ відповідні користувачі. Структура каталогів повторює організаційну структуру підприємства, що спрощує процес побудови моделі.

Програмний засіб управління доступом повинен відповідати таким вимогам:

1) робота в середовищі ОС Windows;
2) високий рівень надійності призначення прав доступу;
3) неперервність роботи;
4) простота в користуванні;
5) використання мінімальних ресурсів комп’ютера;
6) можливість конфігурування;
7) мінімальні затрати на розробку.

Найбільш високий рівень надійності призначення прав можна досягнути, використовуючи їх на рівні файлової системи. Це подібне до способу розмежування доступу в автоматизованих системах.

Згідно розробленого алгоритму, програмний засіб працює таким чином: спочатку встановлюється час запуску програми, після чого вона очікує значення встановленого часу. Далі програма робить запит списку каталогів, розташованих на файловому сервері. При першому запуску створюється файл, який містить список каталогів на сервері. Вміст даного файлу порівнюється з отриманим результатом запиту. У випадку появи нових каталогів проводиться додавання в файл списку каталогів. Далі здійснюється запит для отримання списку користувачів і груп. Після цього проводиться зіставлення каталогів і користувачів. Результат зіставлення записується в окремий файл. Використовуючи результати зіставлення, записані в окремий файл, проводиться редагування списків.

Процес зіставлення і призначення прав доступу користувачам і групам здійснюється згідно розробленої дискреційної моделі розмежування прав доступу.

Висновок

У роботі розроблено дискреційну модель розмежування доступу в системах захисту інформації.

Список використаних джерел

1. Домарев В.В. Безопасность информационных технологий. Системный поход / Домарев В.В. – К.: ООО ТИД Диа Софт, 2008. –992 с.