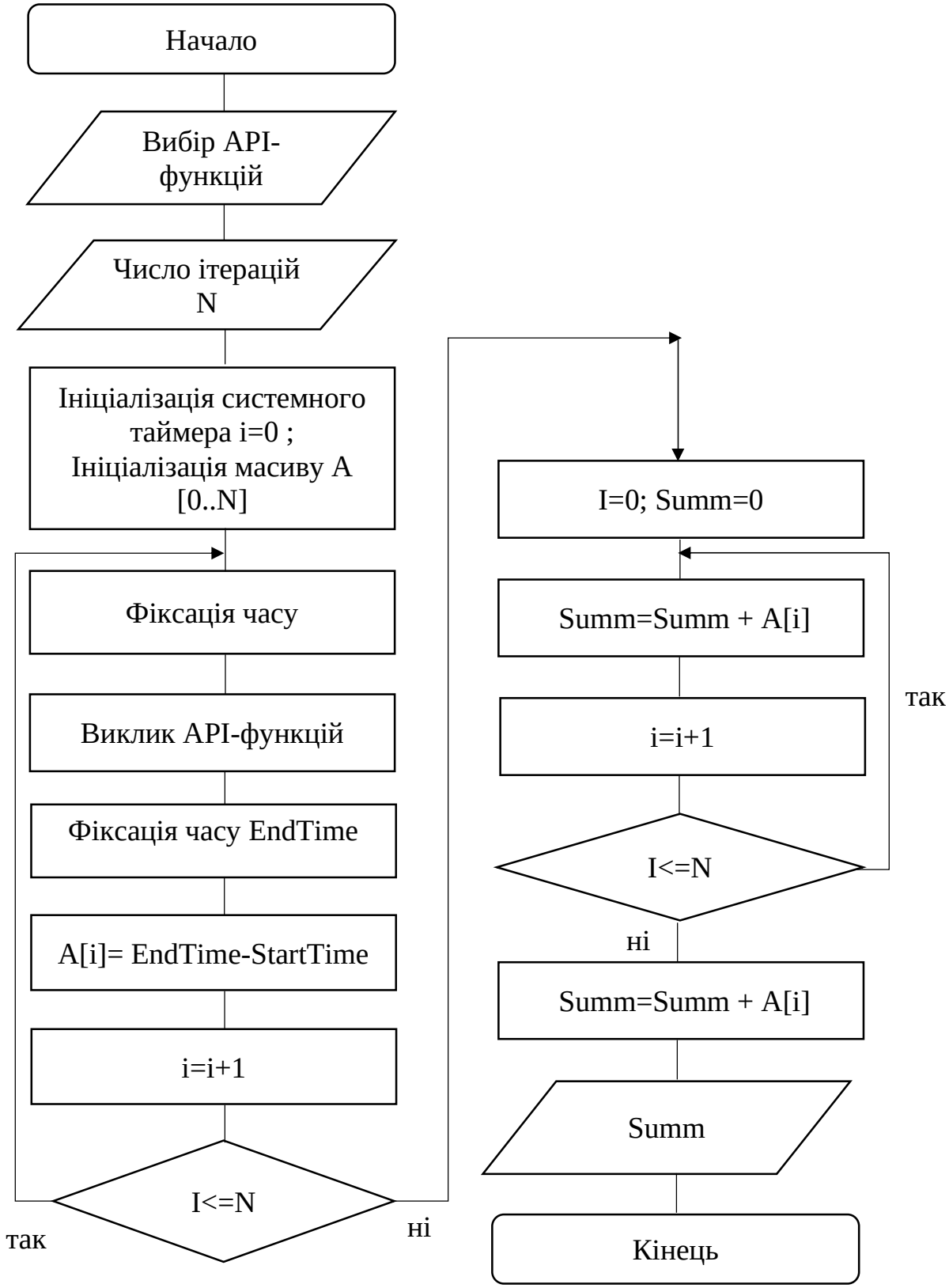
ДОДАТОК А

Блок-схема алгоритма работи програми



ДОДАТОК Б

Графічний матеріал кваліфікаційної роботи

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

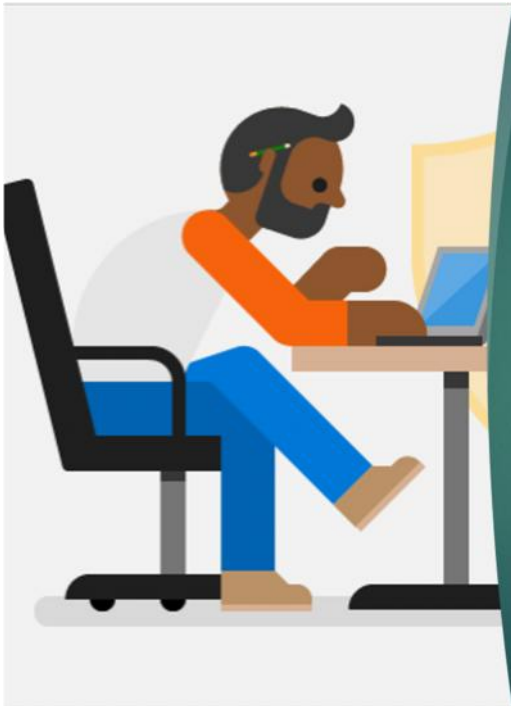
Кафедра ЕОМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: Оцінка впливу вбудованих механізмів безпеки на продуктивність системи

студента групи:
КСМм-20-1
Лобода М.В.

Керівник кваліфікаційної роботи
проф. Горбачов В.О.



2

Мета роботи

Розробити методику оцінки вбудованих механізмів безпеки на продуктивність системи

Актуальність

3

Актуальність роботи полягає у тому, що для збереження важливих та конфіденційних даних, встановлюються системи безпеки, що очікувано негативно впливають на продуктивність системи, що є неменш важливим фактором в сучасності.

Таким чином, виникає необхідність в розробці методики оцінки ступеню впливу засобів розмежування доступу на продуктивність системи

Задачі дослідження

4

- аналіз проблем проектування безпечних систем;
- аналіз моделі розмежування доступу ;
- аналіз методів оцінки впливу систем безпеки на продуктивність;
- методика оцінки впливу системи розмежування доступу на продуктивність системи;
- практична реалізація методи оцінки впливу системи розмежування доступу на продуктивність системи.

Вступ

5

На сьогоднішній день вже положення законів та підзаконних актів в області забезпечення безпеки, інформаційних технологій визначають ряд вимог до механізмів захисту в автоматизованих системах, в тому числі до механізмів логічного розмежування доступу.

Зміни в налаштування вносяться локально, модифікуються невеликі фрагменти правил логічного розмежування доступу. При цьому оцінка впливу таких змін на захищеність та продуктивніть комп'ютерної системи в цілому часто не проводиться.

Аналіз проблем проектування безпечних систем

6

Ефективність засобів захисту від інформаційно-технічних впливів і комп'ютерних атак грає велику роль в адекватному функціонуванні системи. Крім вимог до ефективності виконання захисних функцій, до систем ставиться вимога мінімізації впливу атак на процеси функціонування системи, зокрема, на її продуктивність.

В ідеальному випадку система (або засоби) захисту не повинні впливати на продуктивність інформаційно-обчислювальної системи. Разом з тим слід зазначити, що створити якусь систему захисту (в тому числі і систему розмежування доступу), яка не впливала б негативно на захищаємий об'єкт, практично неможливо.

Механізми забезпечення безпеки

7

а) До загальних механізмів забезпечення безпеки належать :

- 1) довірча функціональність (trusted functionality);
- 2) позначки безпеки (security lables);
- 3) виявлення подій (event detection);
- 4) контроль безпеки (security audit trail);
- 5) відновлення безпеки (security recovery).

б) До спеціальних механізмів забезпечення безпеки належать такі:

- 1) шифрування (encipherment);
- 2) механізми цифрового підпису (digital signature mechanisms);
- 3) механізми управління доступом (access control mechanisms);
- 4) механізми забезпечення захисту цілісності даних (dataintegrity mechanisms), які включають криптографічні контрольні функції;
- 5) механізми автентифікації (authentication exchange mechanisms);
- 6) механізми заповнення трафіку (padding traffic mechanisms);
- 7) механізми керування маршрутизацією (routing control mechanisms).

Моделі розмежування доступу

8

Одним з критеріїв вибору системи (або засобів) розмежування доступу для захисту будь-якої інформаційно-обчислювальної системи повинен бути критерій мінімуму впливу обраної системи розмежування доступу на продуктивність захищається інформаційно-обчислювальної системи.

З усіх існуючих моделей розмежування доступу найбільшого поширення набули дві основні моделі:

- виборче (дискреційне) розмежування доступу;	- повноважне (мандатний) розмежування доступу.

Дискреційне розмежуванні доступу

9

При дискреційному розмежуванні доступу певні операції над конкретним ресурсом забороняються або вирішуються суб'єктам або групам суб'єктів. Практично всі існуючі операційні системи реалізують саме таку модель доступу.

Мандатне розмежування доступу

10

Мандатне розмежування доступу полягаєв тому, що всі об'єкти доступу мають визначенні рівні секретності, а всі суб'єкти поділяються на групи, що утворюють ієрархію відповідно до рівня допуску до інформації.

Для реалізації мандатної моделі розмежування доступу, як правило, необхідні додаткові програмні засоби, що вбудовуються в операційну систему.

При цьому слід зазначити, що мандатна модель розмежування доступу при реалізації її в операційних системах не замінює дискреційну модель розмежування доступу, а доповнює її, вносячи додатковий рівень перевірки прав доступу суб'єктів, при їх запитах на будь-які дії з об'єктами.

11

Загальна схема методики

Визначення переліку системних функцій операційної системи, що підлягають контролю та вагових коефіцієнтів значущості системних функцій.

12

Етап 1. Для обраних API-функцій при виконанні завдань загального призначення (редагування текстових документів та електронних таблиць,робота з архівами документів тощо) протягом 7 хвилин був здійснений підрахунок кількості викликів цих функцій (використовувалася програмна утиліта Process Monitor). Після чого був визначений коефіцієнт значості. Результати цього експерименту наведено у таблиці .

$$w_i = \frac{x_i}{X}$$

де xi – кількість викликів і-й системної функції за контрольований проміжок часу ($i = \overline{1;N}$; N -число системних функцій, що підлягають оцінці);

X - загальна кількість всіх системних викликів за керуємий проміжок часу, визначається як

Назва API-функцій	Кількість викликів API-функцій	Вагових коефіцієнт значості
CreateFile	452	0.204
CopyFile	84	0.038
DeleteFile	24	0.011
MoveFile	19	0.009
ReadFile	895	0.405
WriteFile	734	0.332

Визначення коефіцієнтів уповільнення виконання системних функцій операційної системи, що підлягають оцінці

13

Етап 2. Для вибраних api-функцій булизроблено оцінки часу виконання функцій без контролю їх засобами розмежуваннядоступу та під контролем засобів розмежуваннядоступу – по 30 викликів кожної функції з фіксацією часу виконання кожного виклику. Результати вимірювань середнього часу виконаннясистемних функцій, а також розраховані коефіцієнти уповільнень роботи системних функційнаведено у таблиці.

$$k_i = \frac{\overline{t_i^*}}{\overline{t_i}}$$

де $\overline{t_i}$ – середній час виконання і-ї системної функції без контролю її засобами розмежування доступу;

$\overline{t_i^*}$ – середній час виконання і-ї системної функції під контролем її засобами розмежування доступу.

Назва api-функцій	Час роботи функції без контролю t_i (сек.)	Час роботи функції під контролем t_i^* (сек.)	Коефіцієнт уповільнення роботи функцій k_i
Createfile	0,000816	0,001225	1,502
Copyfile	0,002614	0,003219	1,231
Deletefile	0,000429	0,000952	2,219
Movefile	0,000440	0,000973	2,211
Readfile	0,000082	0,000145	1,768
Writefile	0,000207	0,000371	1,792

Визначення певного інтегрального показника зниження продуктивності системи внаслідок впливу засобів розмежування доступу.

14

Даний показник визначається як адитивна згортка коефіцієнтів уповільнення роботи кожної системної функції з урахуванням вагового коефіцієнта значущості цієї функції: $K = \sum_{i=1}^{N} k_i w_i$.

Етап 3.

З урахуванням даних, отриманих на етапах 1 та 2, загальний коефіцієнт уповільнення роботи системи при введенні до її складу засобів розмежування доступу зі складу комплексу засобів інформаційної безпеки secret net буде дорівнювати

$$K = \sum_{i=1}^{6} k_i w_i = 1.502 * 0.204 + 1.231 * 0.038 + 2.219 * 0.011 + 2.211 * 0.009 + 1.768 * 0.405 + 1.792 * 0.332 = 1.707$$

ВИСНОВОК

В процесі написання кваліфікаційної роботи на тему: «Оцінка впливу вбудованих механізмів безпеки на продуктивність системи». Були підняті та проаналізовані такі питання:

1. аналіз проблем проектування безпечних систем
2. моделі систем розмежування доступу
3. аналітична оцінки впливу на систему монітора безпеки

Результатом роботи є створена методика оцінки впливу системи розмежування доступу на продуктивність системи та програмний застосунок, для розрахування часу виконання API-функцій, що використовується у методиці. В результаті використання методики були отримані результати вимірювань, які були занесені в таблиці 1 та 2 та був розрахований загальний коефіцієнт уповільнення роботи системи K = 1.707.

Таким чином, запропонована методика та її програмна реалізація дозволяють оцінити вплив системи розмежування доступу до об'єктів доступу на продуктивність інформаційно-обчислювальної системи та при цьому при оцінці вагових коефіцієнтів значимості приватних показників використовувати розрахунковий метод без використання експертних оцінок.