Інформаційна технологія діагностування мережевих ресурсів та надання рекомендацій для усунення наслідків атак

Магістерська кваліфікаційна робота
122 «Комп’ютерні науки та інформаційні технології»

Виконала: студентка гр. 2КН-16м
Гикава М.В.
Науковий керівник: Суприган О.І.

Мета дослідження – підвищення точності класифікації атаки та формування максимально ефективних рекомендацій усунення наслідків атаки;

Об'єкт дослідження – процес виявлення атаки;

Предмет дослідження – способи класифікації мережевих атак.

Програмний продукт	*Характеристики програм*
BlackICE Defender BID (спеціалізований додаток-агент)	- Видає попередження про атаку; - Повідомляє про спробу несанкціонованого доступу; - Виявляє джерело атаки мережі; **Недолік:** відсутність можливості створення правил для окремих програм.
Intruder Alert (інструментарій детектування мережевих атак)	- Вибирає стратегію захисту мережі. - Завантажує сигнатури хакерських атак. - Вимагає наявність досвідчених спеціалістів для обслуговування. **Недолік:** складний процес управління системою.
Centrax (інструментарій детектування мережевих атак)	- Контролює системи захисту мережі. - Виконує моніторинг трафіку. - Видає попереджувальні повідомлення про мережеву атаку. **Недолік**: не гарантує збереження інформації.
eTrust Intrusion Detection (аналізатор трафіку мережі сегмента)	- Керує стратегіями захисту. - Видає попередження про атаку в режимі реального часу. - Виконує моніторинг трафіку. **Недолік:** не підтримує високий рівень деталізації наборів правил.
Snort (система виявлення атак)	- Ефективно спрацьовує при здійсненні атак на бездротову мережу; - Визначає, який трафік в мережі є шкідливим; - Сканує систему на наявність атаки. **Недолік:** потребує постійного оновлення.

РОЗРОБКА МОДЕЛІ ДІАГНОСТУВАННЯ МЕРЕЖЕВИХ РЕСУРСІВ

Застосування імітаційного моделювання

$$Y=F(X) \quad (1)$$

F – алгоритм імітації, який відтворює функціонування системи;

X– множина вхідних змінних системи;

Y– множина вихідних змінних системи.

$$\mathbf{K=}f\mathbf{(x_1, x_2, m_1, m_2, a,b)} \quad (2)$$

де x_1, x_2 – вхідні параметри системи;

m_1, m_2 – параметри атаки;

a, b – параметри, які визначають наслідки дії атаки;

Дослідження поведінки системи під дією атак

Визначення залежності між фактором ***X*** і показником ***Y*:**

$$Y = a\sqrt{X} + b \qquad (3)$$

де X - атака, яка діє на мережеві ресурси;

a – параметр, який визначає наслідки атаки;

b – характеристика, яка визначає атаку.

Застосування нелінійної динаміки

Для опису стану динамічної системи використовується формула:

$$x = [\boldsymbol{x_1}, \boldsymbol{x_2}, \dots, \boldsymbol{x_n}] \quad (4)$$

де x – характеристика акати, яка діє на мережеві ресурси.

Для встановлення часу виявлення та розпізнавання атаки по характеристикам використовуємо зміну системи, а саме:

$$\frac{\boldsymbol{dx_i}}{\boldsymbol{dt}} = \boldsymbol{F}_{\text{i}}[\boldsymbol{x_1}, \boldsymbol{x_2}, \dots, \boldsymbol{x_n}] \quad (5)$$

де $\boldsymbol{t}$ – час дії атаки, протягом якої буде відбуватися діагностування і розпізнавання;

Модель прогнозування та оцінки можливих наслідків дії атак

$$\mathrm{A}(x_i, m_k) = \sum_{\mathrm{i,k=1}}^{n} a_{ik} \cdot x_i \cdot m_k \qquad (6)$$

$$\mathrm{B}(x_i, m_k) = \sum_{\mathrm{i,k=1}}^{n} b_{ik} \cdot x_i \cdot m_k \qquad (7)$$

$$\mathbf{F} = f(\mathbf{A}, B) \qquad (8)$$

$$\mathbf{F}(\mathbf{A}, B) = \frac{1}{4ab}\left[\left(\frac{\partial A}{\partial x_i} + \frac{\partial A}{\partial x_k}\right)^2 - \left(\frac{\partial B}{\partial x_i} + \frac{\partial B}{\partial x_k}\right)^2\right] + A + B \qquad (9)$$

де А - показник реакції системи на атаку;

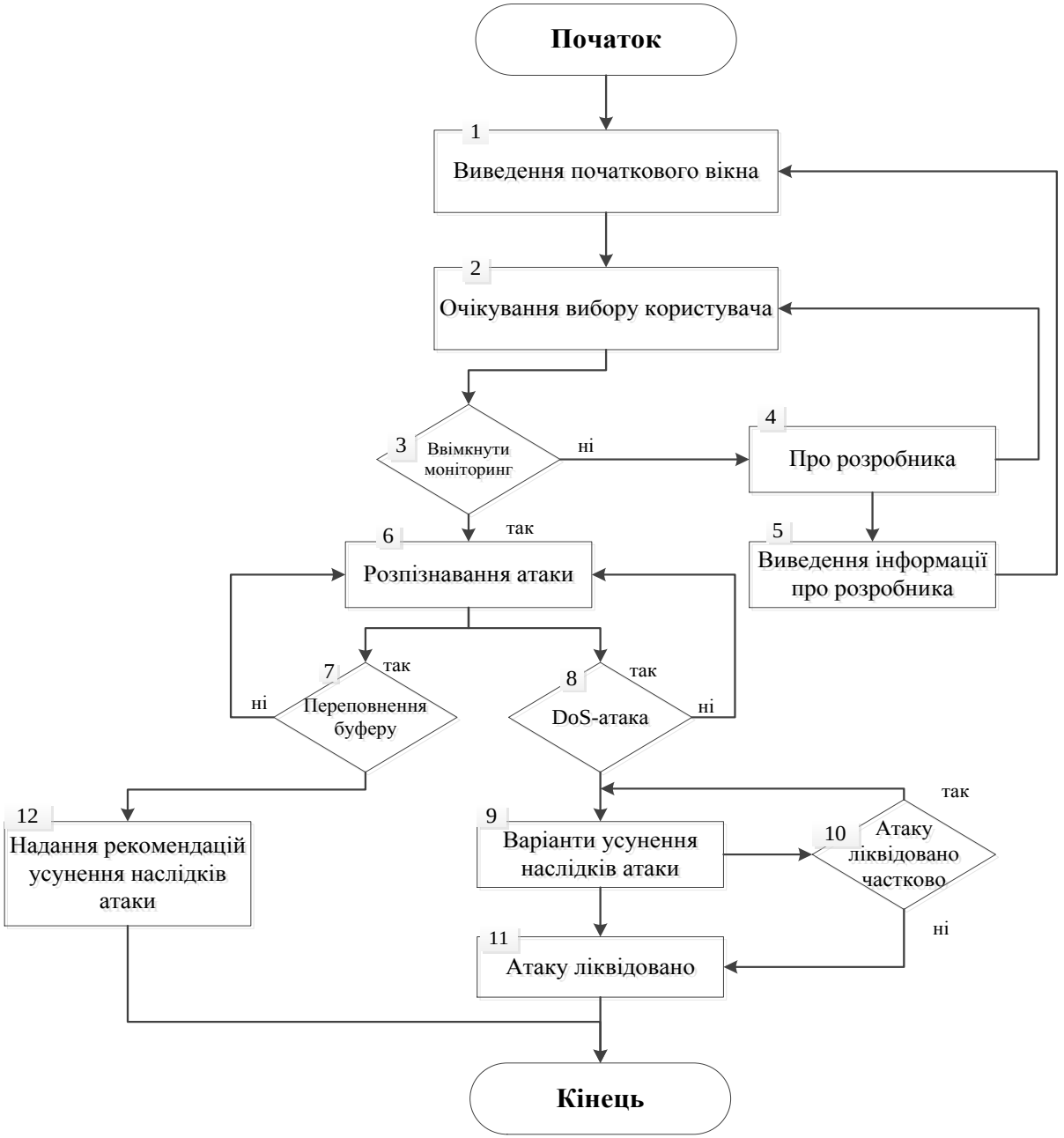
В – показник прогнозування дії системи для усунення наслідків атаки;

i – номер елементу атаки в певний проміжок часу;

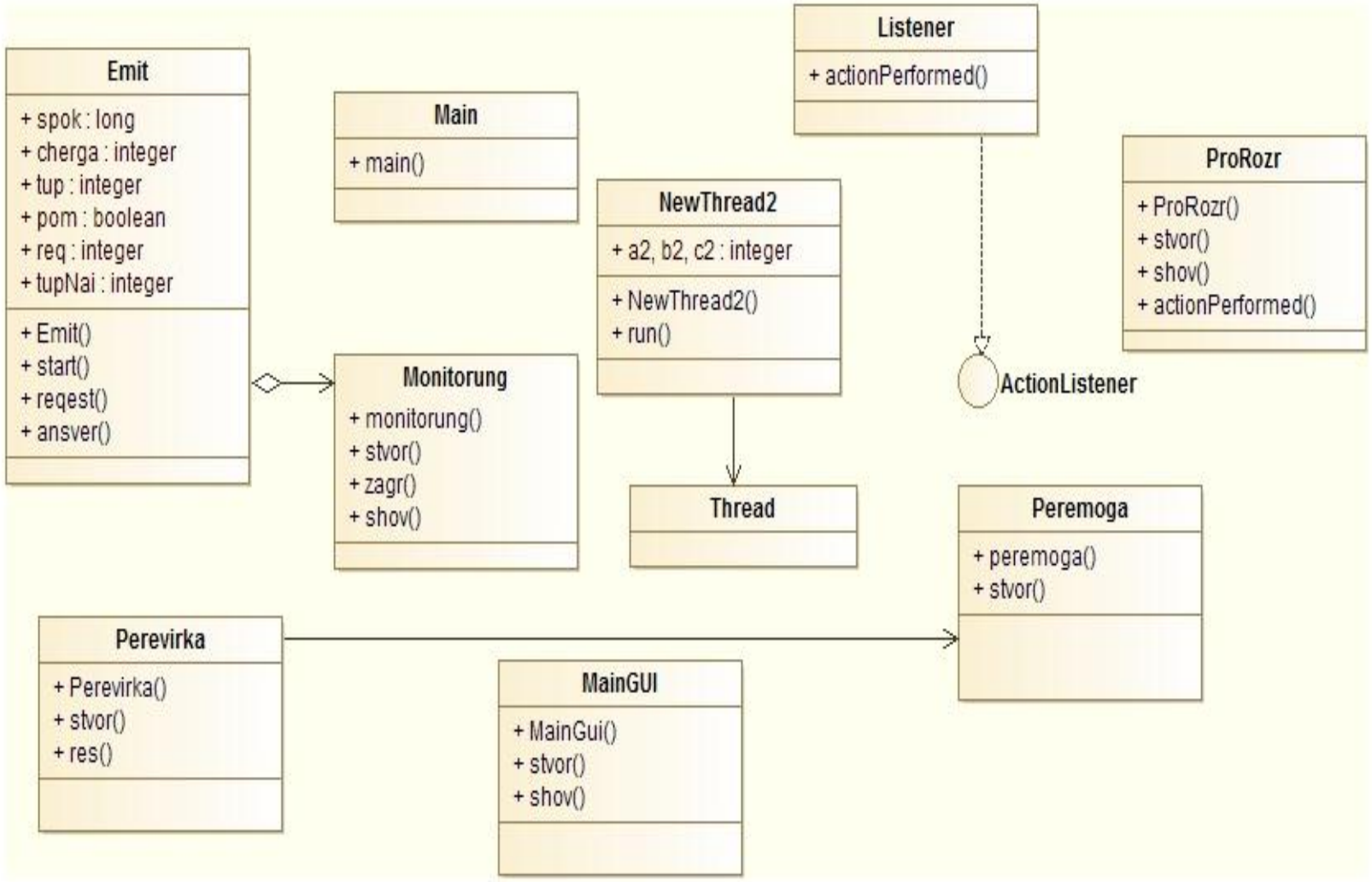
k – показник кількості атак.

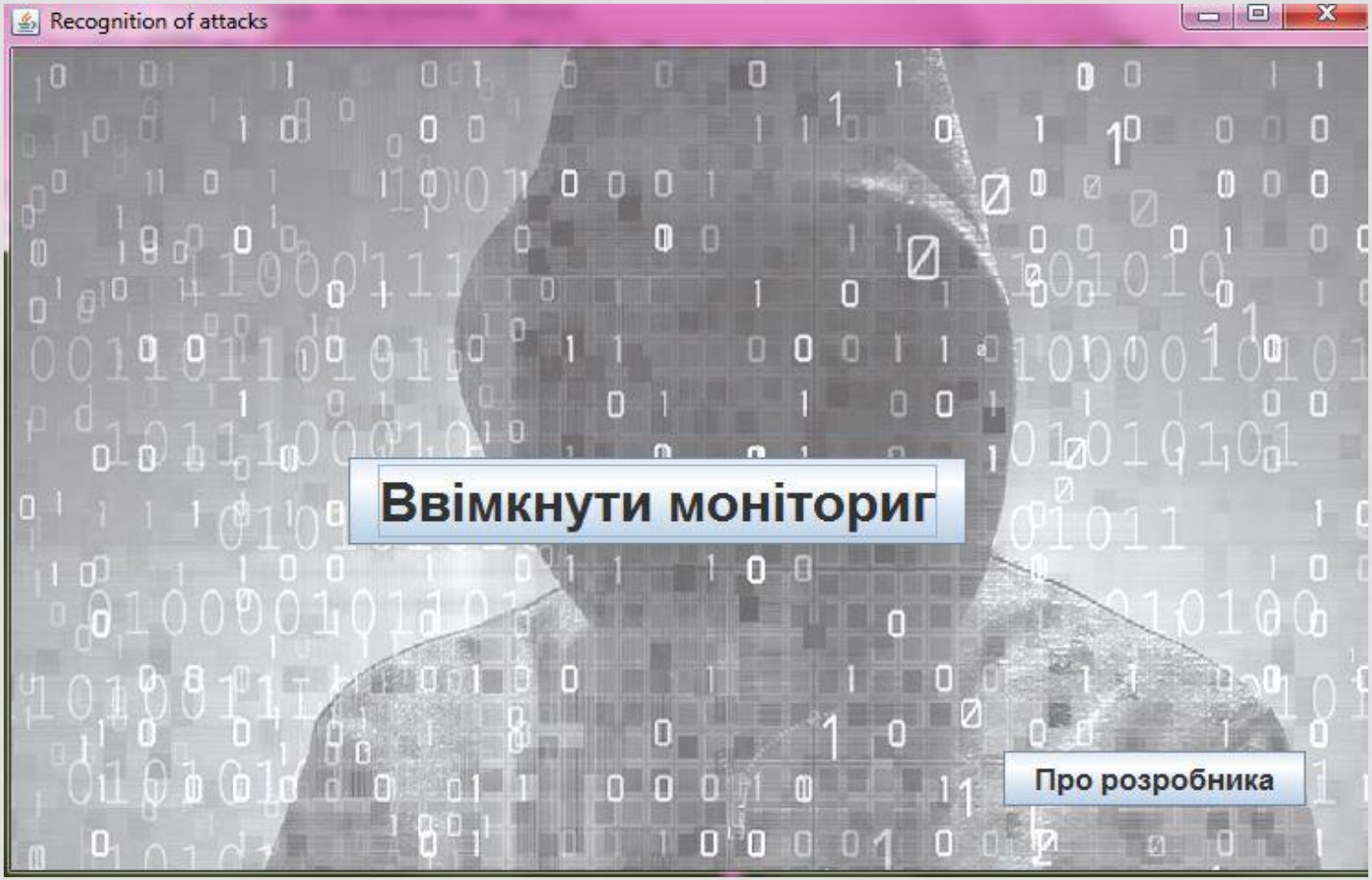
СТРУКТУРНА СХЕМА ДІАГНОСТУВАННЯ МЕРЕЖЕВИХ РЕСУРСІВ ТА НАДАННЯ РЕКОМЕНДАЦІЙ УСУНЕННЯ НАСЛІДКІВ АТАК

АЛГОРИТМ РОБОТИ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

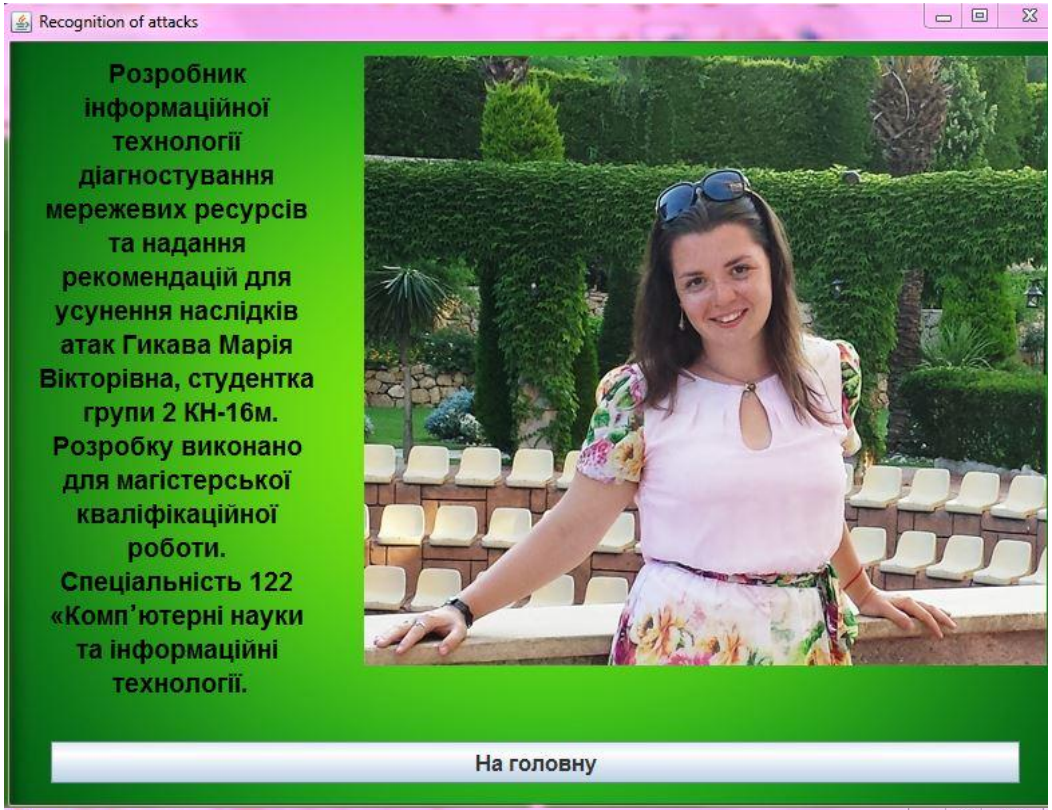


СТРУКТУРА ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

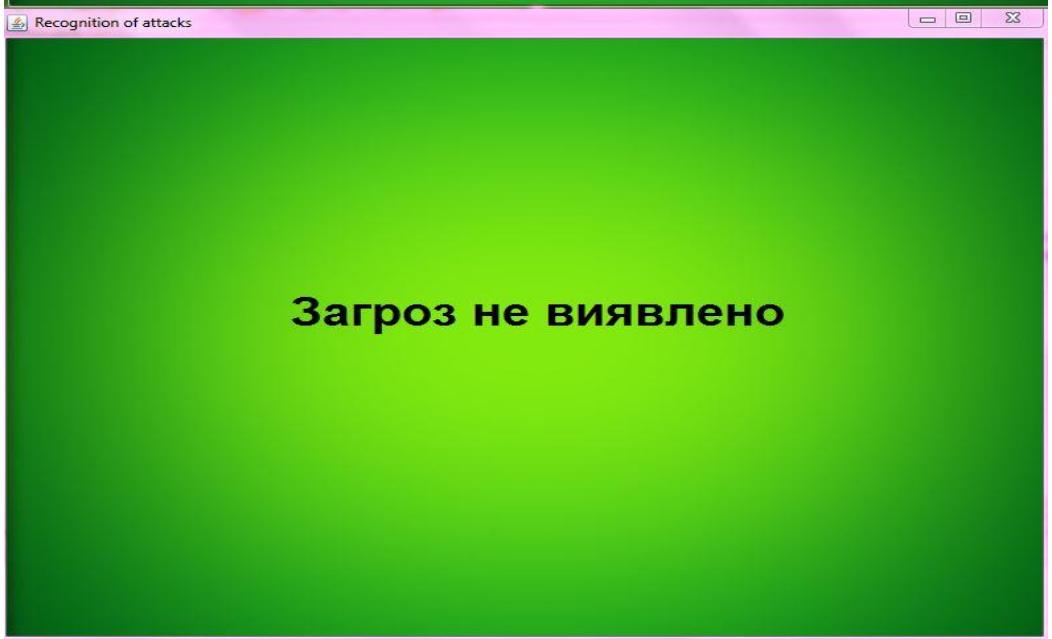




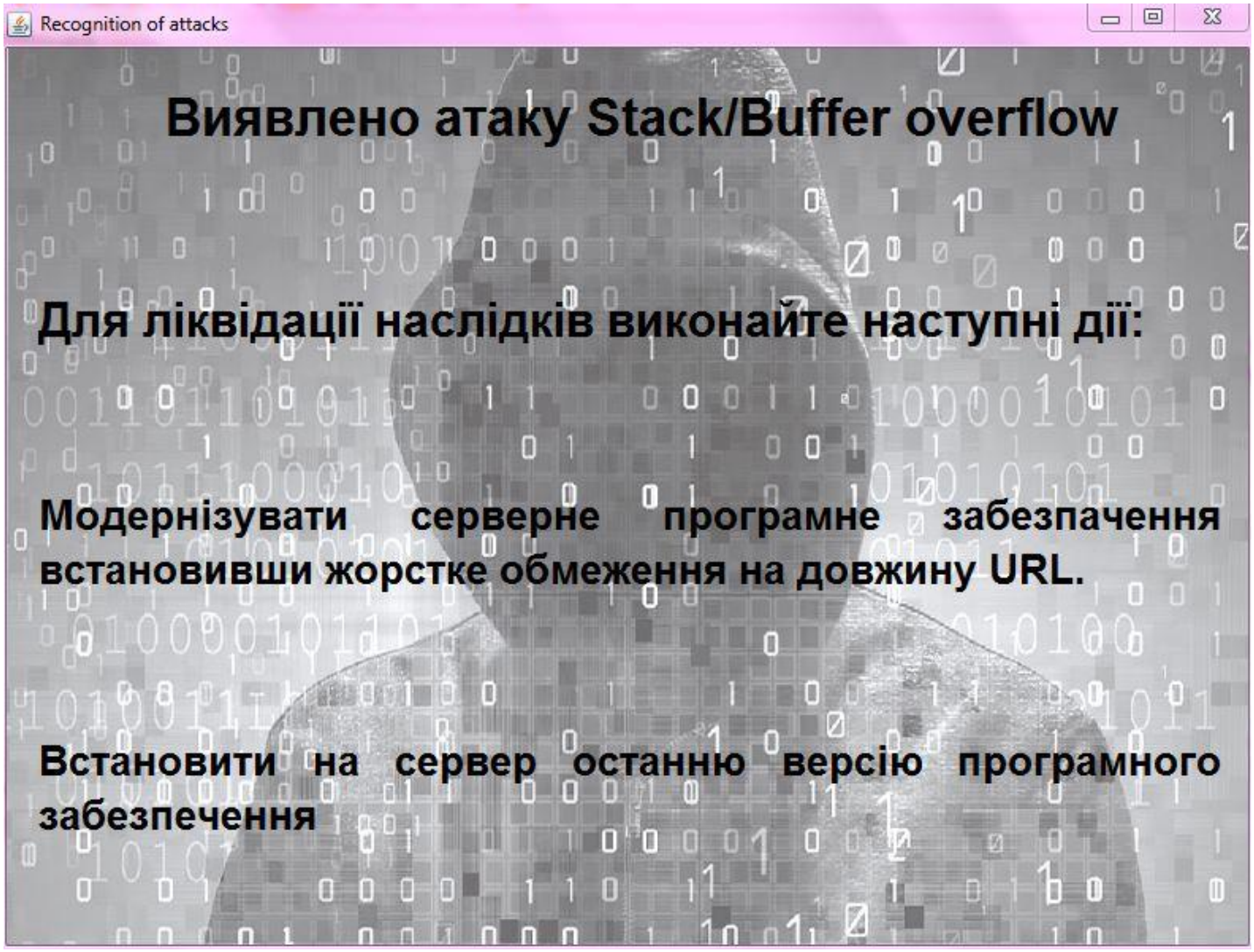
Головне вікно роботи користувача



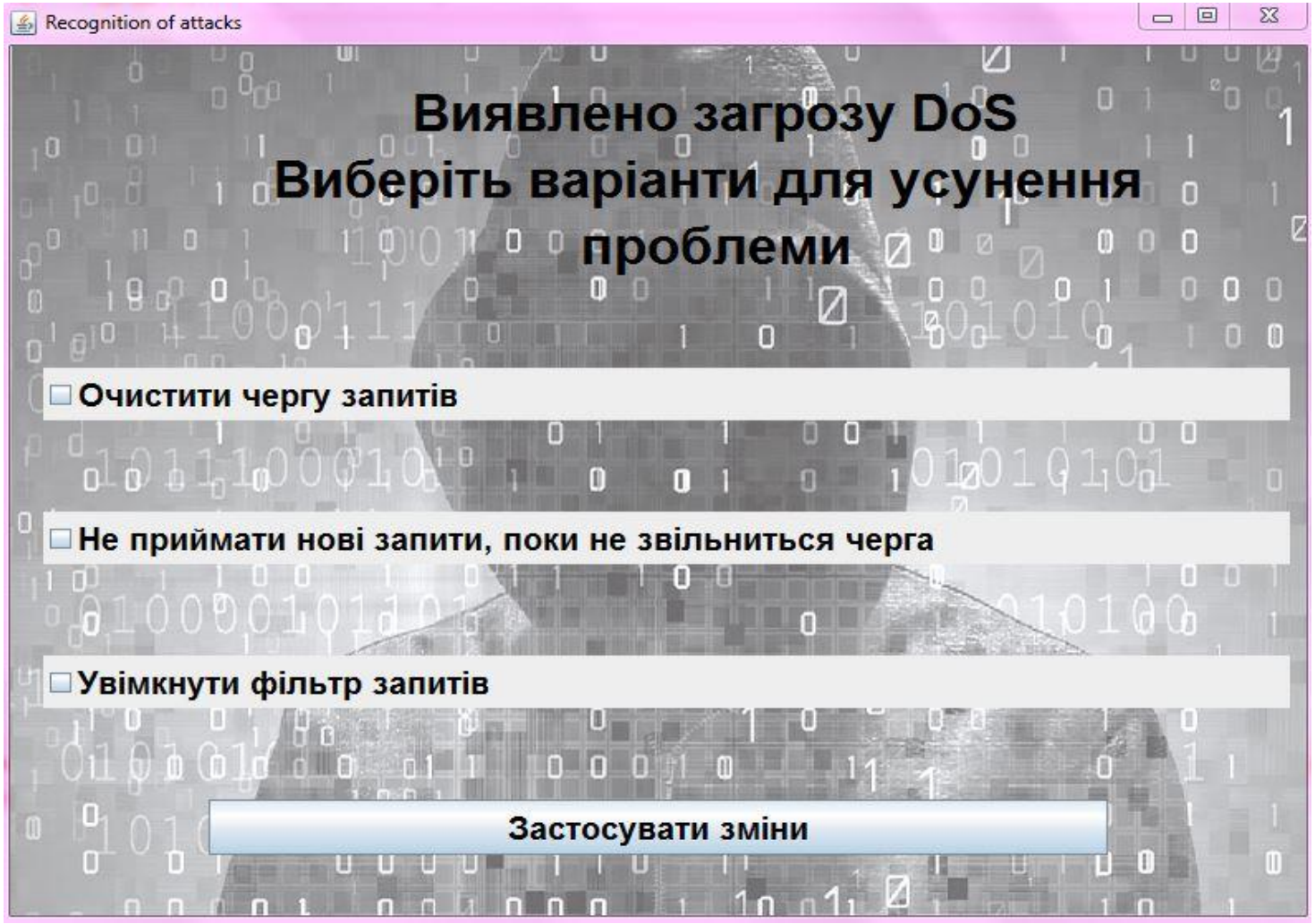
Інформація про розробника програми



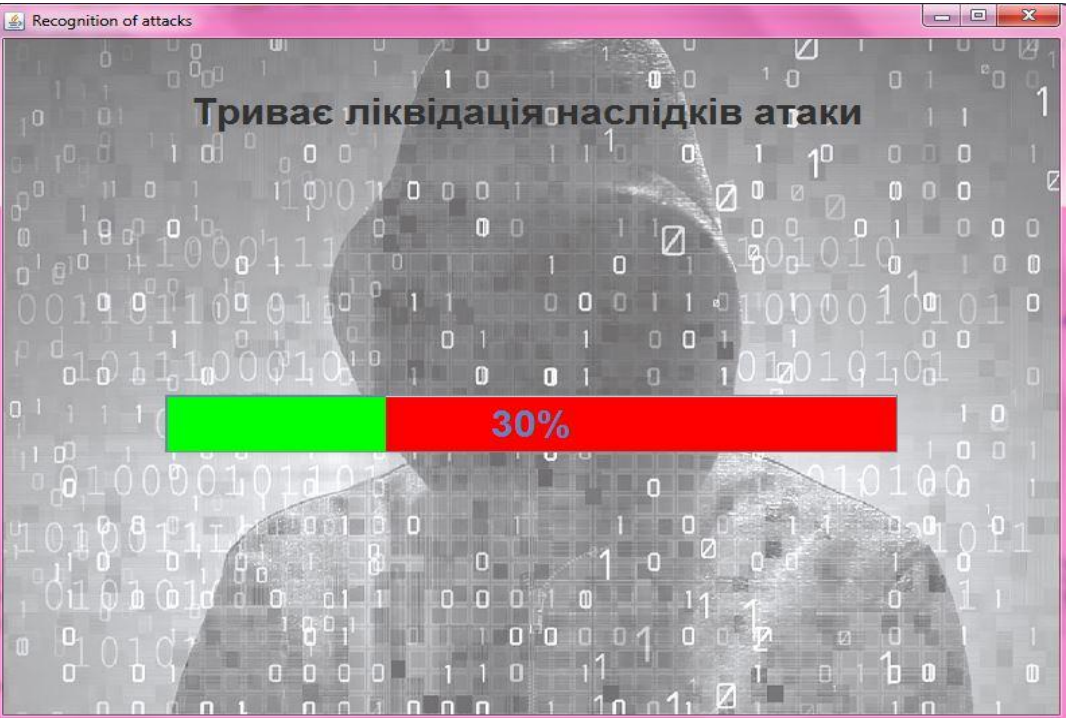
Початкова робота програми



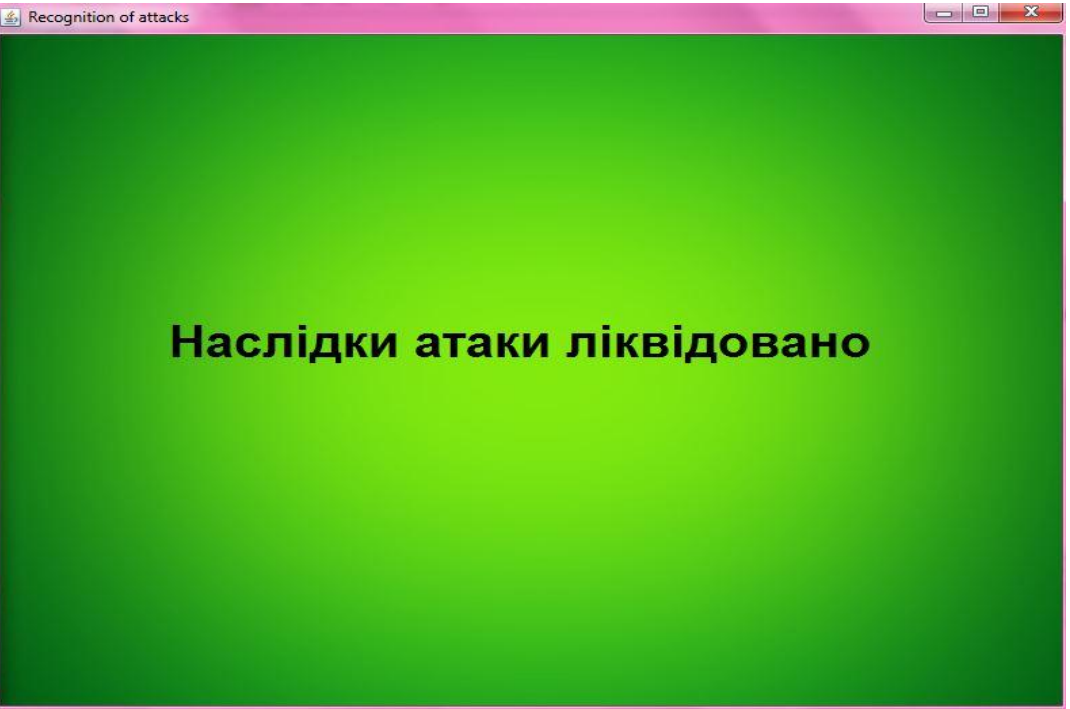
Надання рекомендацій при виявленні атаки переповнення буфера



Варіанти усунення наслідків атаки



Процес ліквідації наслідків атаки



Представлення вдалого усунення наслідків атаки

ЕФЕКТИВНІСТЬ РОБОТИ ПРОГРАМИ

Аналоги / Параметри	Розроблена інформаційна технологія	Snort (система виявлення атак)	Centrax (інструментарій детектування мережевих атак)
Діагностування характеристик атаки, яка діє на мережеві ресурси	Діагностує характеристики атаки	Виявляє дію атаки	Виявляє дію атаки
Класифікація атаки	Класифікує атаки	Розпізнає	–
Надання рекомендацій, щодо усунення наслідків атаки	Надаються рекомендації	Не надає рекомендацій	Попереджає про мережеву атаку
Час виявлення атаки (t), с	0,3	0,35	0,5
Забезпечення збереження цілісності інформації	забезпечує	забезпечує	не гарантує збереження
Усунення наслідків атак	Усуває наслідки атаки	Блокує атаку одразу при виявленні	–
Точність класифікації атаки	95% точності класифікації (DoS-атаки)	50%	–

Наукові публікації:

1) XLV науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії (м. Вінниця, 2016 р.);

2) XLVI науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії (м. Вінниця, 2017 р.) ;

3) VI міжнародна науково-практична конференція «Методи та засоби кодування, захисту й ущільнення інформації» та опубліковано тези у збірнику доповідей даної конференції

Акт впровадження

ТОВ «ЮК РАДНИК ПЛЮС»

Україна, 21009 м. Вінниця, вул. Лялі Ратушної, 22 А

19 грудня 2017 року

Довідка дана студентці Вінницького національного технічного університету групи 2КН-16м Гикавій Марії Вікторівні в тому, що результати магістерської кваліфікаційної роботи «Інформаційна технологія діагностування мережевих ресурсів та надання рекомендацій для усунення наслідків атак» буде використовуватися компанією ТОВ «ЮК РАДНИК ПЛЮС».

Директор ТОВ «ЮК РАДНИК ПЛЮС» Міровський В.А.

М.П.

Товариство з обмеженою відповідальністю «ЮК РАДНИК ПЛЮС» 41079192 Україна Вінниця

Дякую за увагу!