Методика дослідження кібербезпеки розумного будинку. Частина 1. Тести на проникнення

Виконав:
студент групи 1БС-17м
Вишньовський Владислав
Керівник:
к. т. н., доцент каф. ЗІ
Войтович О. П.

Актуальність теми комплексної магістерської кваліфікаційної роботи пов’язана із зростанням кіберзагроз та вразливостей розумного будинку.

Метою комплексної магістерської кваліфікаційної роботи є покращення кібербезпеки шляхом розробки методів проведення тестування на проникнення розумного будинку.

Об’єкт дослідження – методи дослідження кібербезпеки розумного будинку.

Предмет дослідження – методи тестування на проникнення системи розумного будинку.

Постановка задачі:

1) виконати огляд літературних джерел;
2) провести аналіз основних методів зламу та захисту розумного будинку;
3) розробити методи тестування безпеки;
4) обґрунтувати вибір мови програмування для досягнення поставленої мети;
5) виконати програмну реалізацію на основі розроблених методів;
6) провести тестування розроблених методів;
7) провести обґрунтування економічної доцільності розробки.

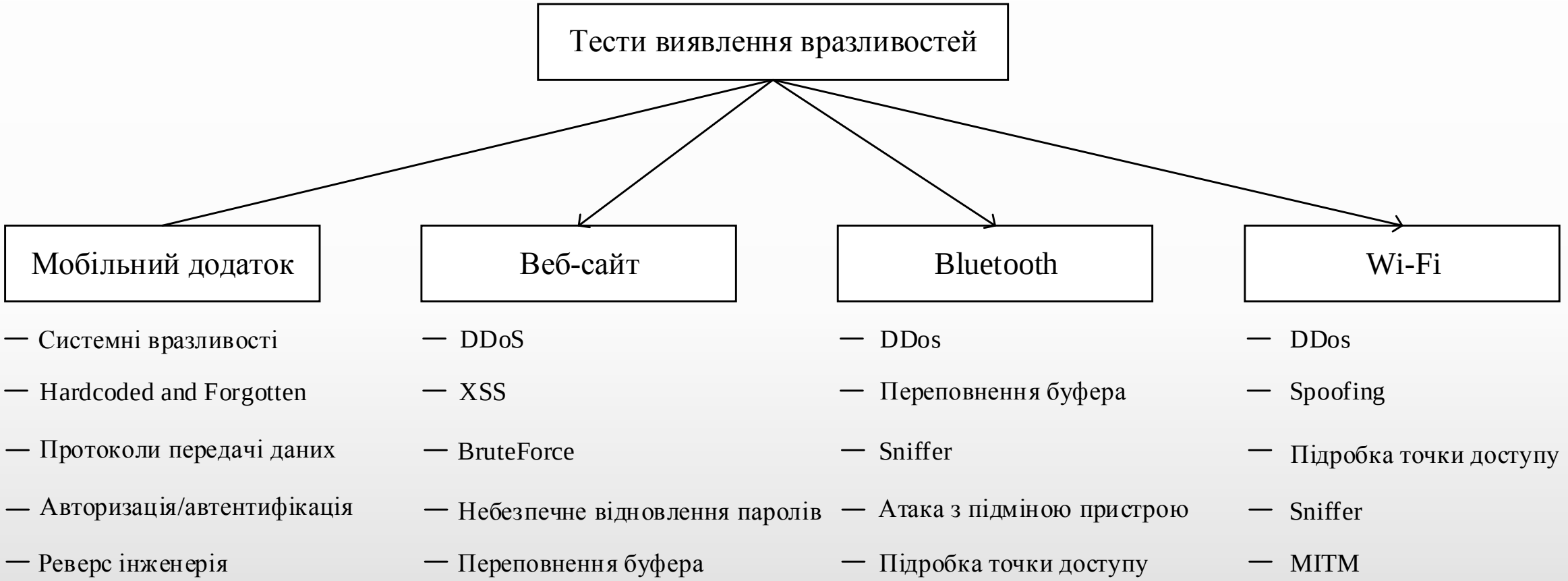
Аналіз сучасних методик

Методика	Недоліки
OSSTMM	Формалізація і відсутність додаткового опису до вимог.
BSI	Використання платного ПЗ, яке можна використовувати для тестування об'єктів, описаних в методиці.
PTEST	Деякі посилання документа ведуть на неіснуючі сторінки. Містить опис тільки процедур зовнішнього тестування.
ISSAF	Методика частково не завершена, не скрізь є приклади та опис.

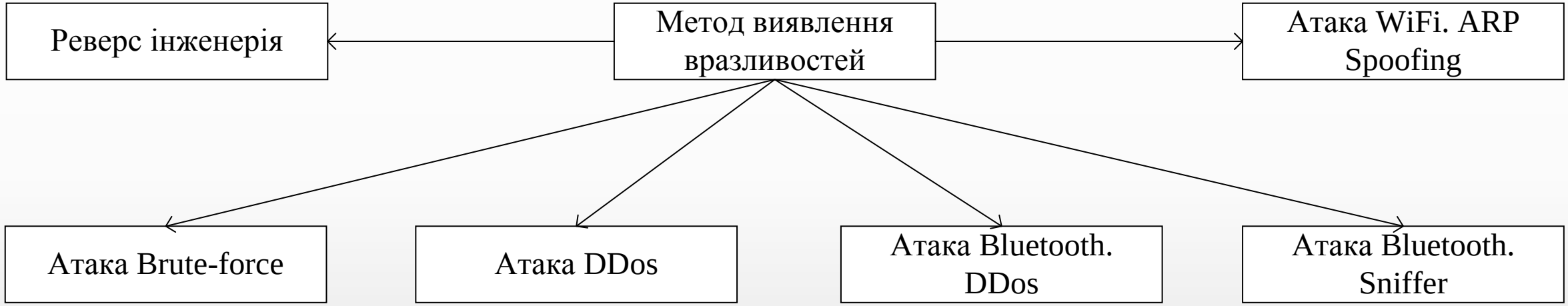
Аналіз програмних рішень

№	Рішення	Переваги	Недоліки
1	websploit	Підтримка великої кількості методів з пентестингу для технології інтернет речей.	Мала кількість документації по виконанню атак.
2	BruteSSH	Використання готових функційз Metasploit.	Не передбачено модуля для сканування пристроїв.
3	nmap	Велика кількість документації по використанню.	Відсутність рекомендацій по виправленню знайдених вразливостей.
5	spooftooph	Зручність використання та зрозумілий інтерфейс.	Обмежена кількість на формування потоків при виконанні атаки.
6	btcrack	Підтримка версій Bluetooth для інтернет речей.	Використання стандартного словника без можливості підключення власного.
7	btscanner	Детальний опис знайдених пристроїв Bluetooth.	Непередбачено підтримку сканування Bluetooth Low Energy.

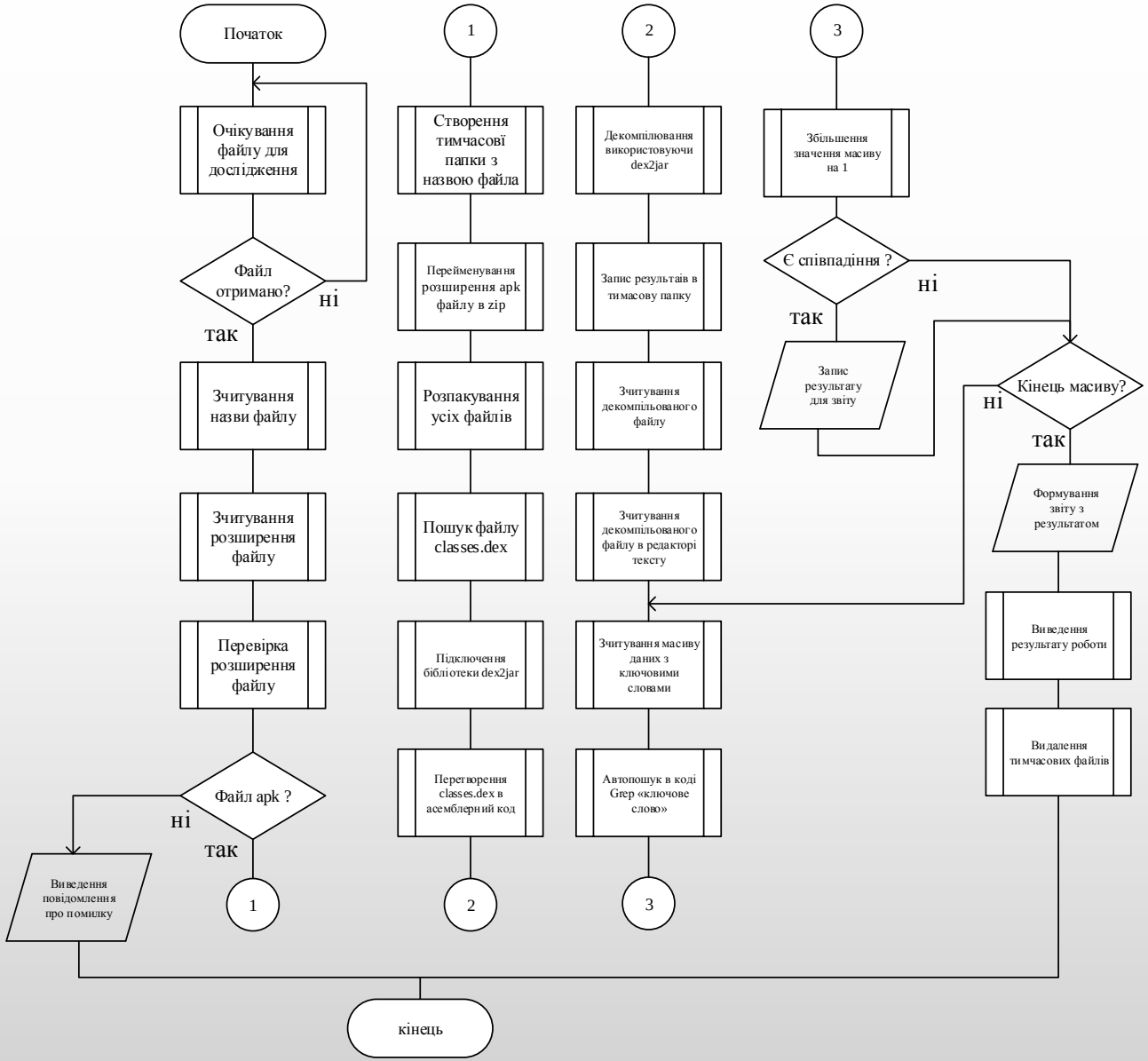
Тести для виявлення вразливостей



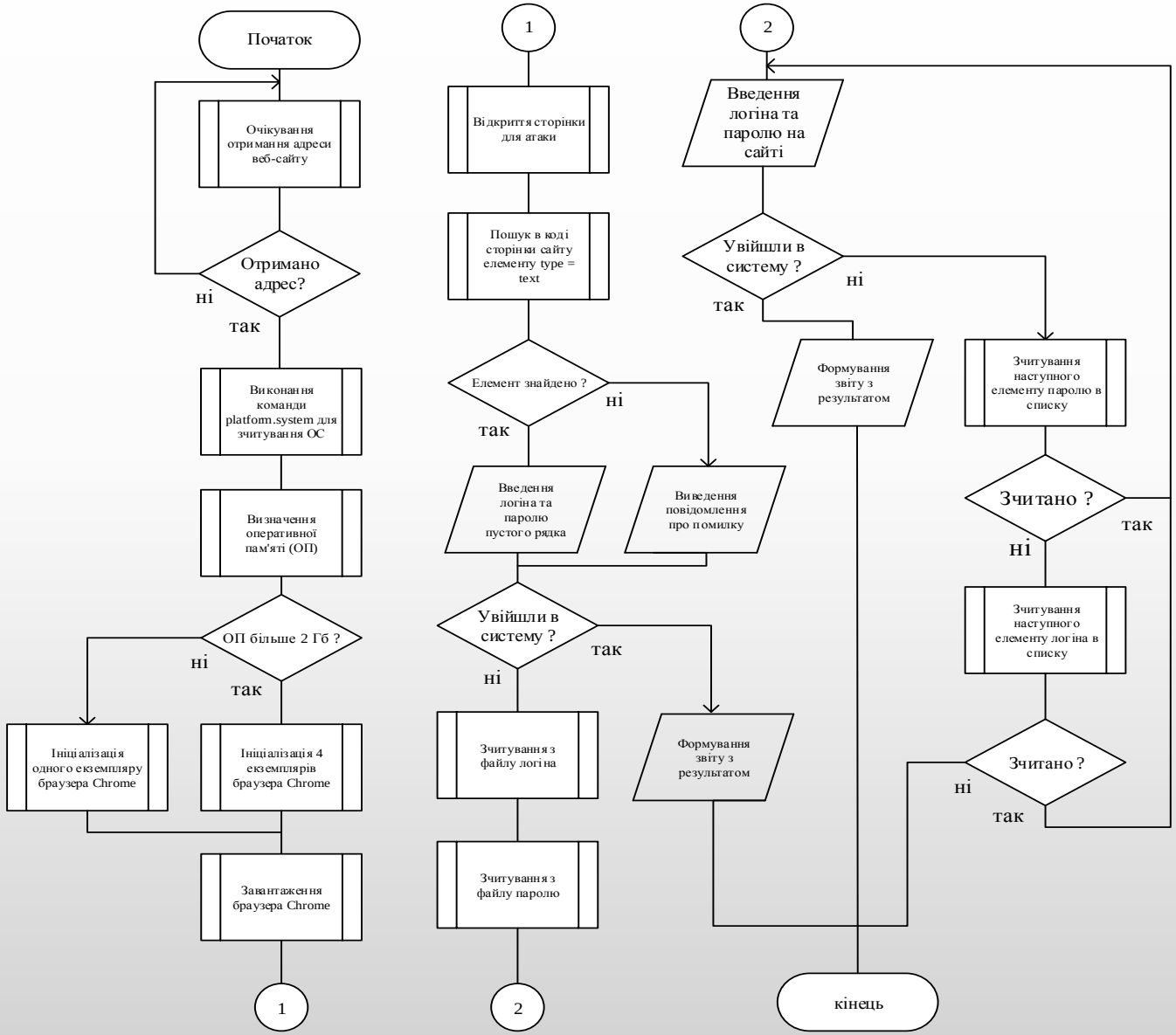
Запропоновані методи виявлення вразливостей



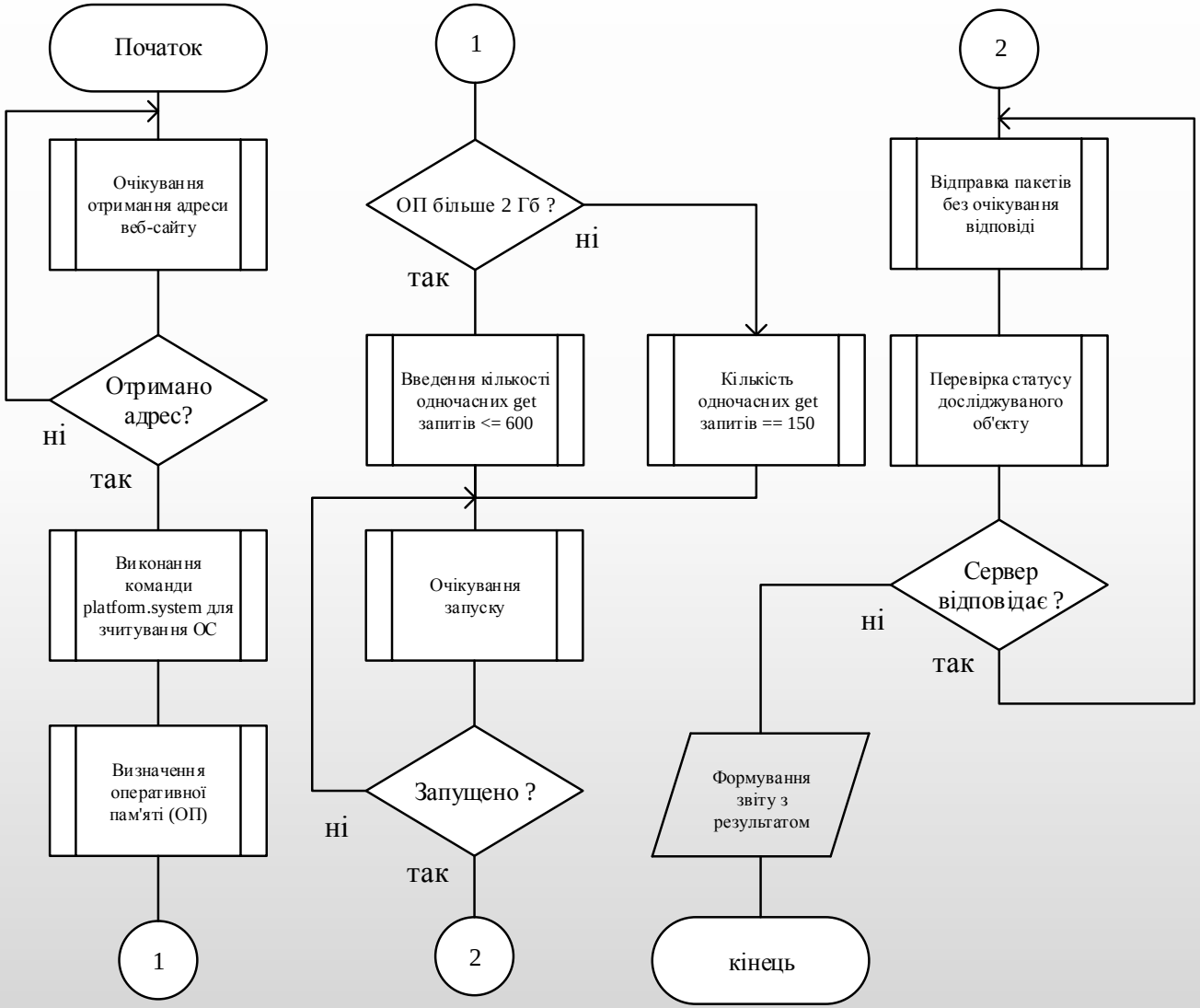
Алгоритм роботи методу реверсної інженерії



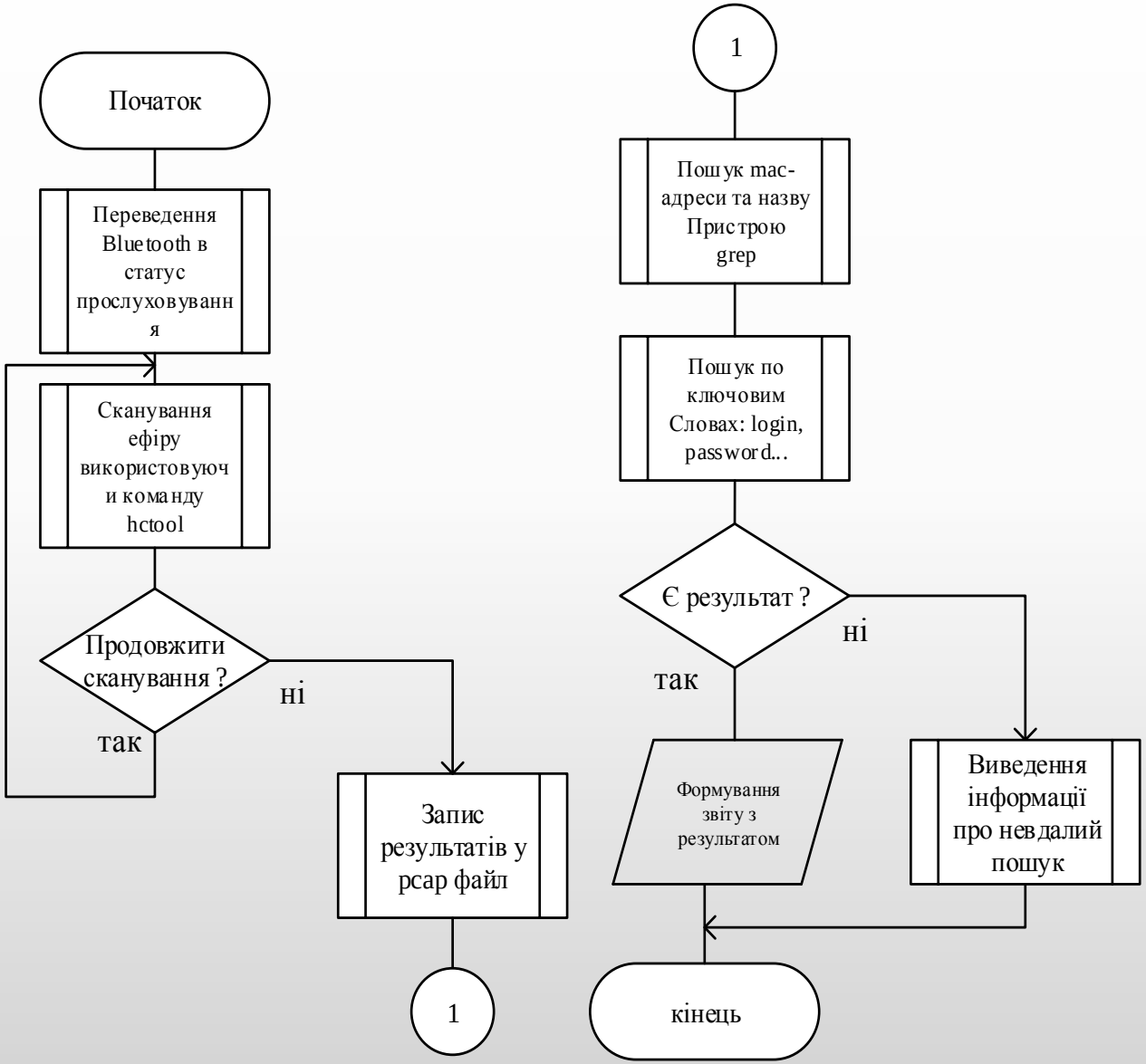
Алгоритм роботи методу грубої сили



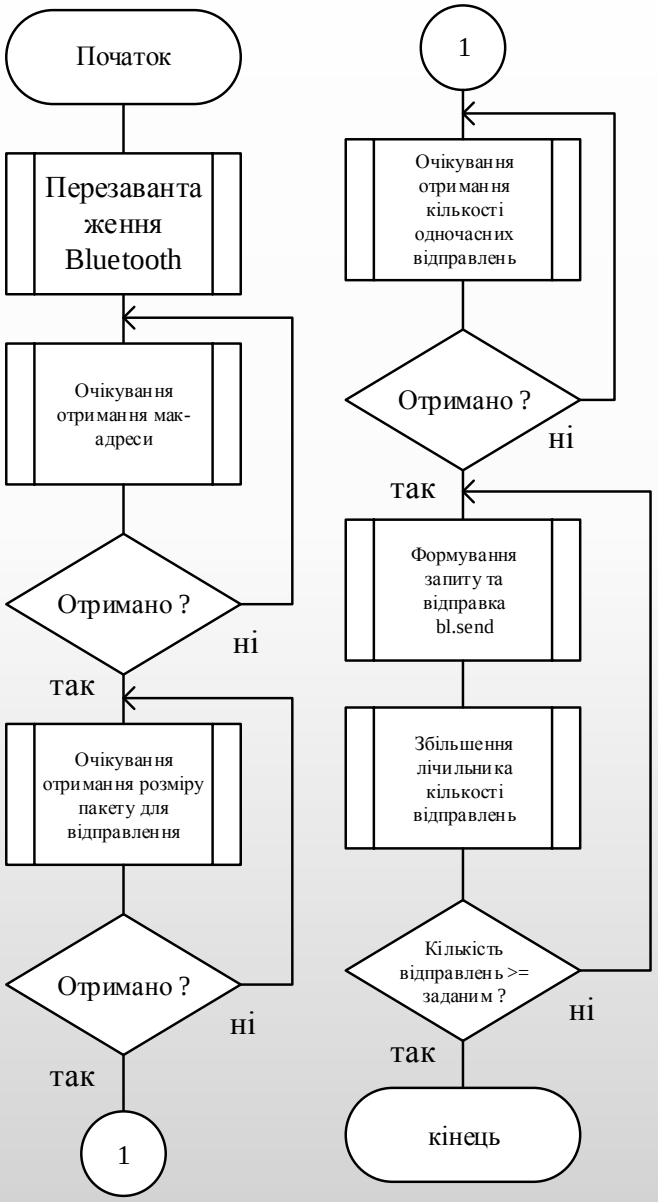
Алгоритм роботи методу DDos-атаки



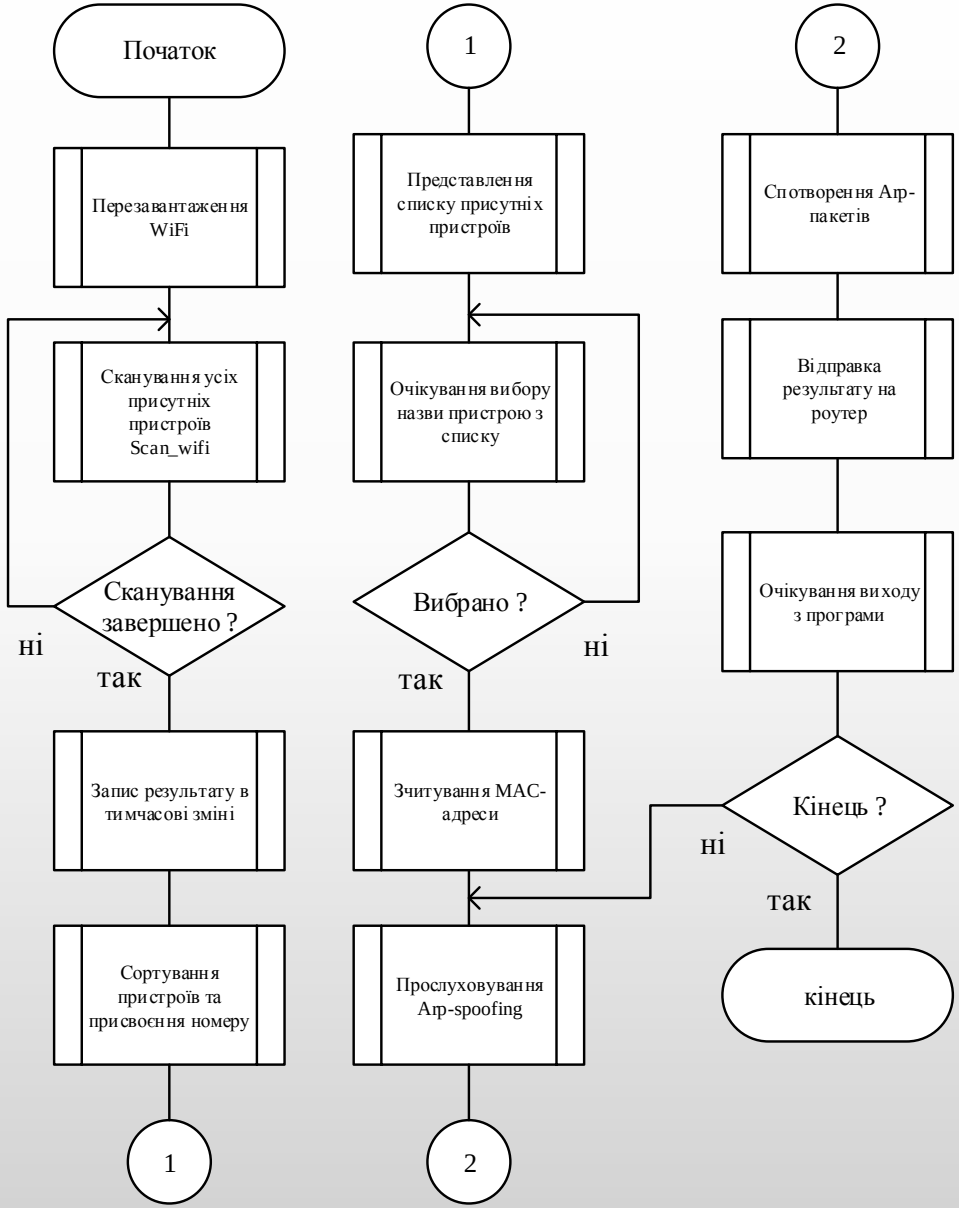
Алгоритм роботи методу Bluetoth sniffer



Алгоритм роботи методу DDos-атаки на Bluetoth



Алгоритм роботи методу атаки spoofing



Алгоритм модуля прийняття рішень

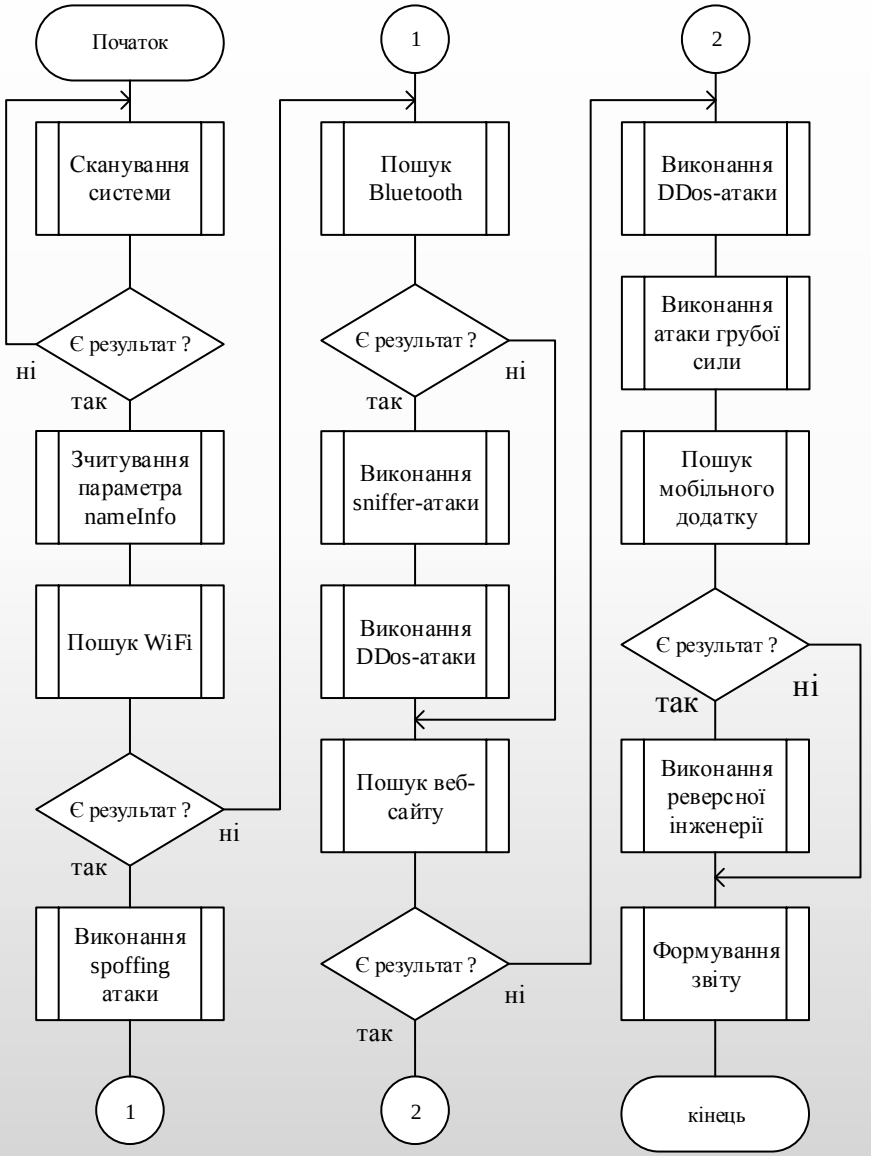
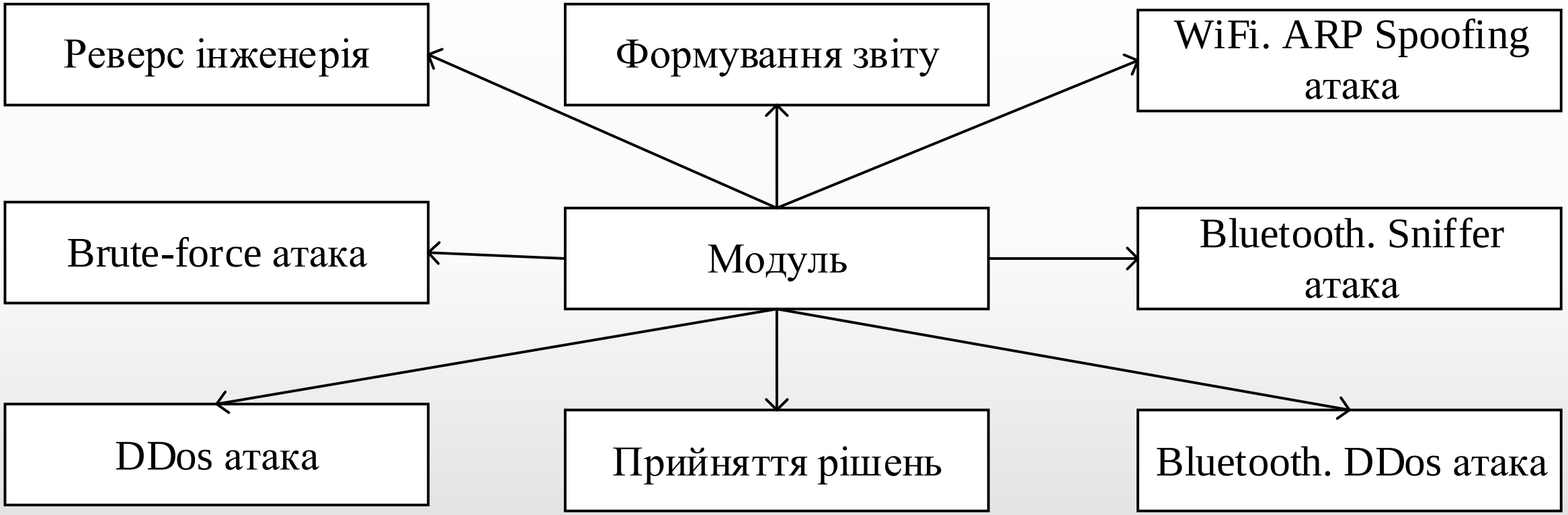
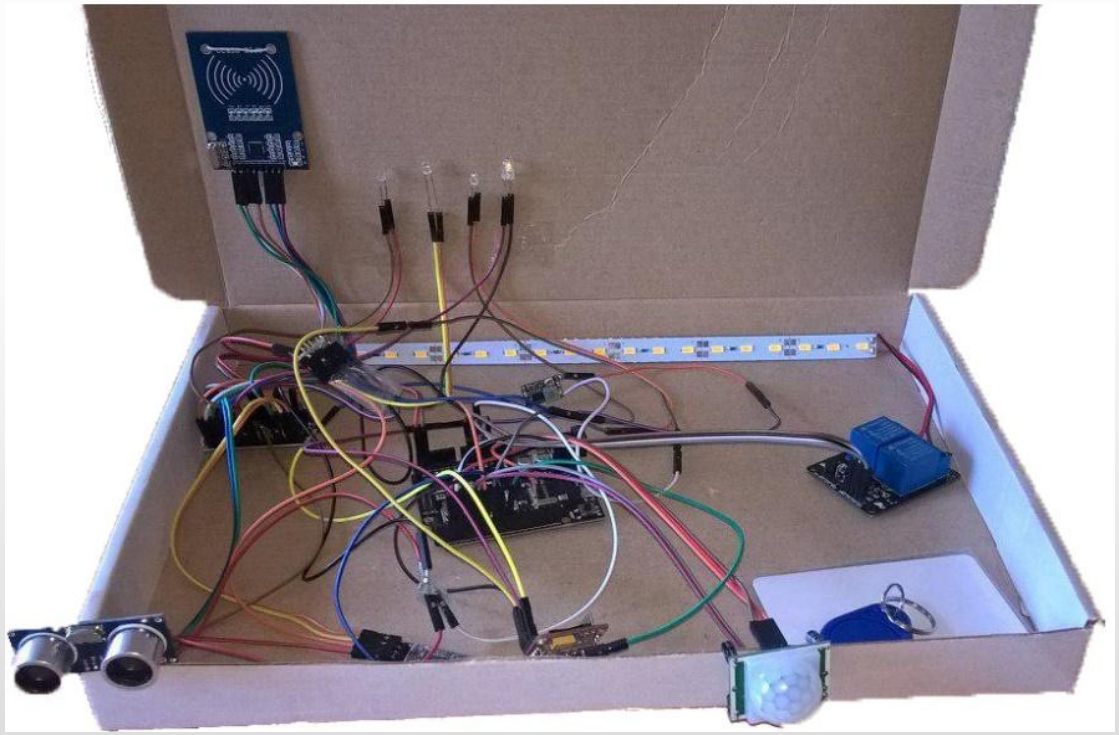


Схема модулів програмного засобу

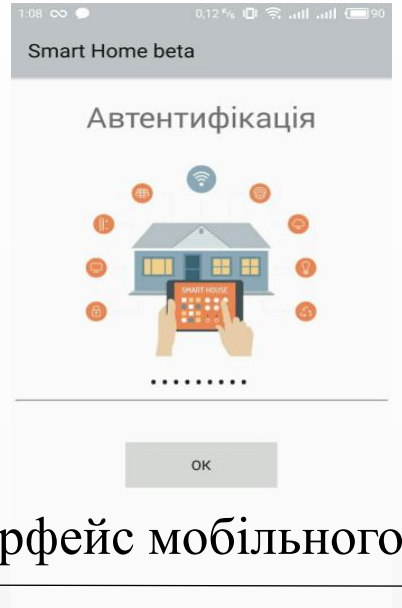


Експериментальне дослідження

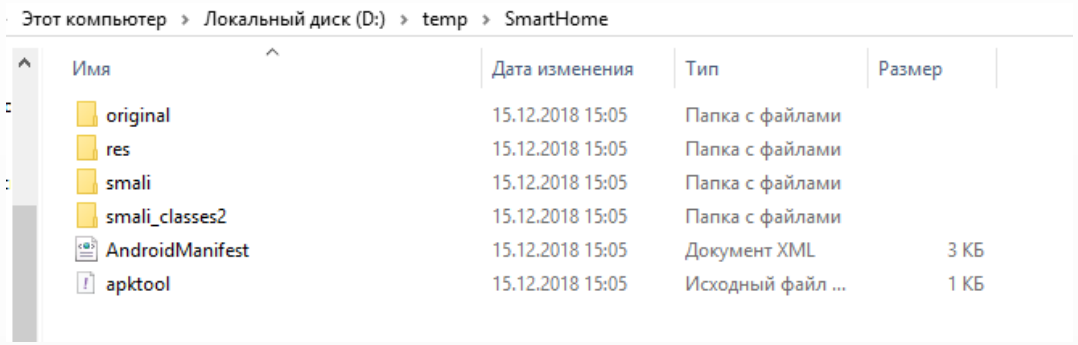


Назва	Марка
Arduino Uno	Robotdyn uno ch340/atmega328pa
Arduino Nano	V3.0 AVR ATmega328 P – 20AU
GSM модуль	SIM800L
RFID мітка	Rfid – rc522
Bluetooth модуль	HC – 06
Датчик руху	HC – SR501
WiFi	ESP 8266
Датчик відстані	hC – SR04

Вигляд результатів дослідження



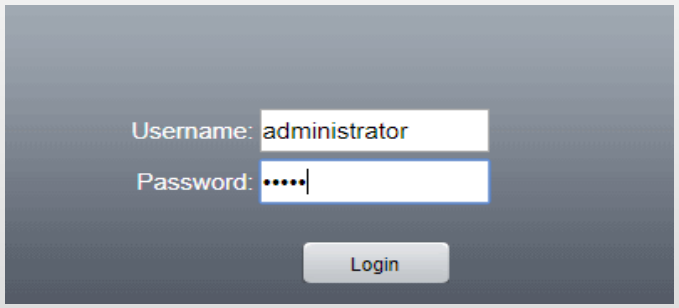
Інтерфейс мобільного додатку



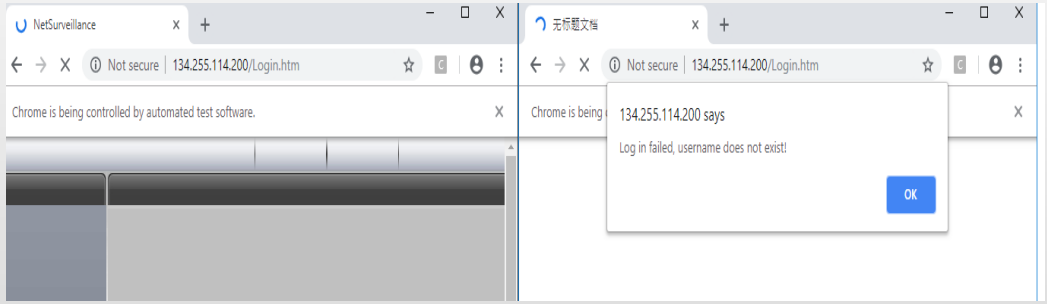
Декомпільований apk-файл

```
.annotation system Ldalvik/annotation/InnerClass;
    accessFlags = 0x609
    pass = "admin"
.end annotation
```

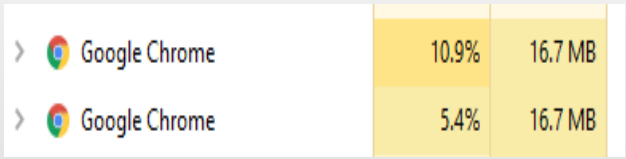
Фрагмент коду автентифікації



Форма авторизації



Результати виконання грубої сили



Запуск багатопоточності

Вигляд результатів дослідження

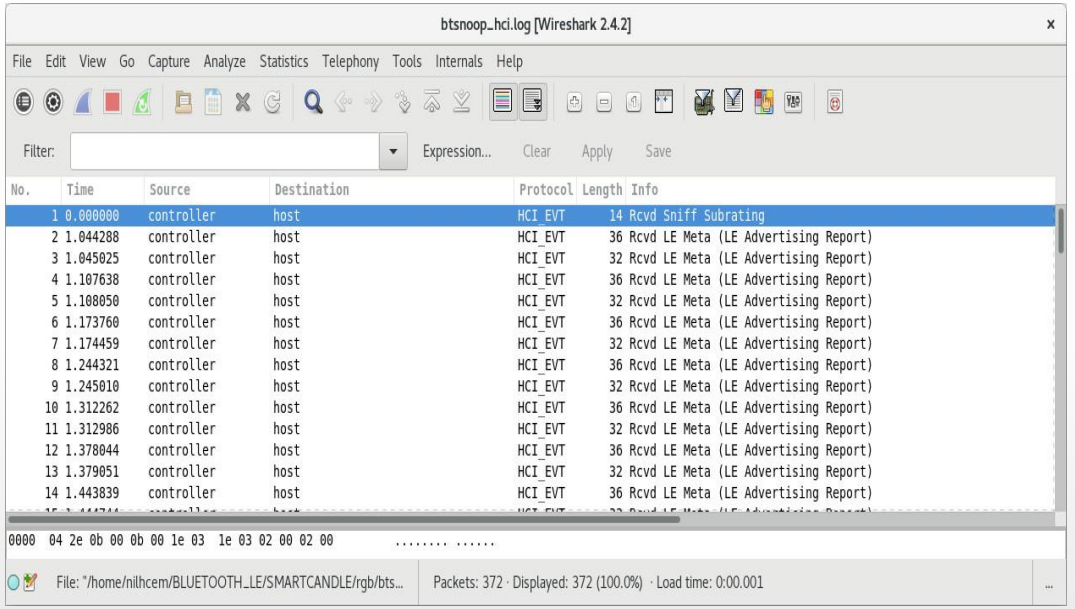
```
134.255.114.200  port:  80  turbo:  150
Please wait...
Sat Dec 15 23:08:49 2018  <--packet sent!
Sat Dec 15 23:08:49 2018  <--packet sent!
Sat Dec 15 23:08:49 2018  <--packet sent!
Sat Dec 15 23:08:49 2018  <--packet sent!
Sat Dec 15 23:08:49 2018  <--packet sent!
Sat Dec 15 23:08:49 2018  <--packet sent!
Sat Dec 15 23:08:49 2018  <--packet sent!
```

Виконання DDos-атаки

504 Gateway Time-out

nginx

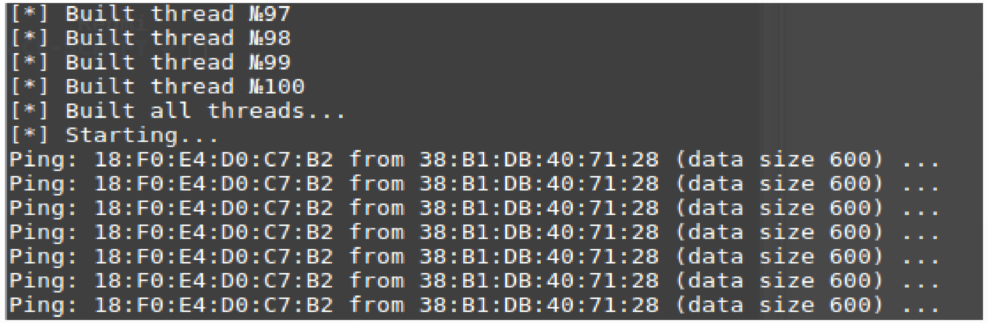
Результат виконання DDos-атаки



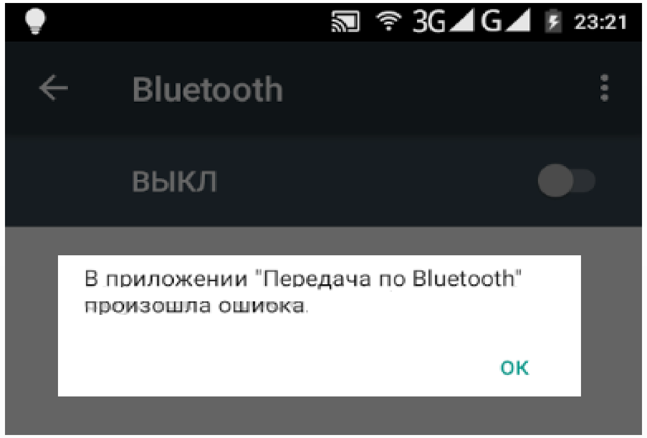
Результат виконання sniffer-атаки

Вигляд результатів дослідження

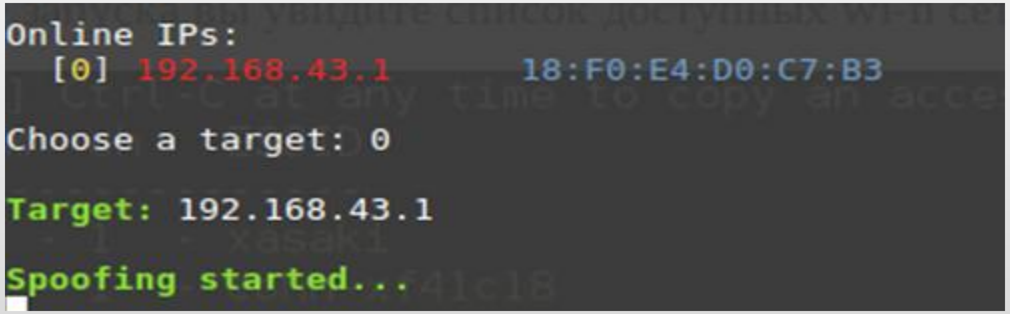
Задання параметрів для DDos-атаки на Bluetoth



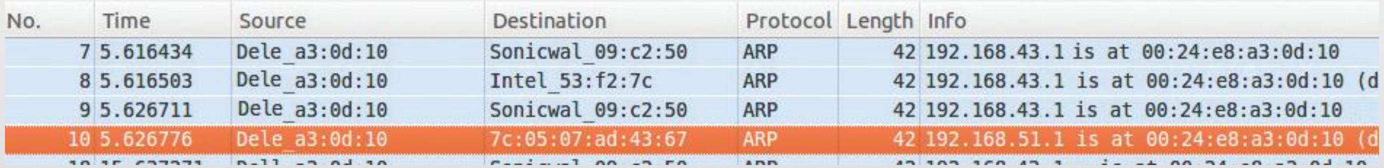
Виконання DDos-атаки на Bluetoth



Результат виконання DDos-атаки на Bluetoth



Виконання атаки arp-spoofing



Результат виконання атаки arp-spoofing

Обґрунтування економічної доцільності:

- ✓ Проведено оцінку комерційного потенціалу розробки;
- ✓ Спрогнозовано витрати на виконання наукової роботи – 79680,63 грн.;
- ✓ Спрогнозовано чистий прибуток від впровадження результатів розробки – за 3 роки 219479,56 грн.;
- ✓ Термін окупності – 1,1 року.

Представлення результатів комплексної магістерської кваліфікаційної роботи:

Конференції:

- XLVI науково-технічна конференція факультету інформаційних технологій та комп’ютерної інженерії Вінницького національного технічного університету. Доповідь визнана найкращою.
- 54 студентська наукова конференція Науково-Технологічного Університету AGH в Кракові (Польща).
- Шоста Міжнародна науково-практична конференція «Методи та засоби кодування, захисту й ущільнення інформації»
- XLVII Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії.

А також опубліковані тези доповідей.

Дякую за увагу!