

# 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.

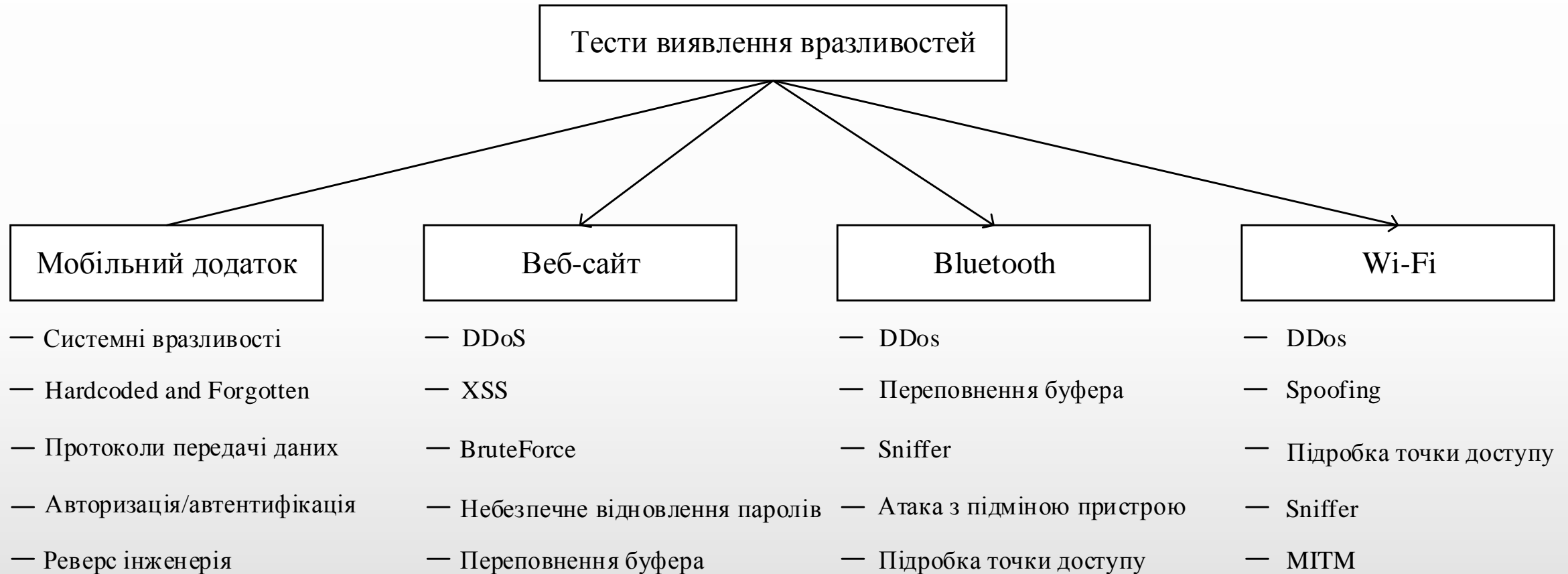
# Аналіз сучасних методик

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.

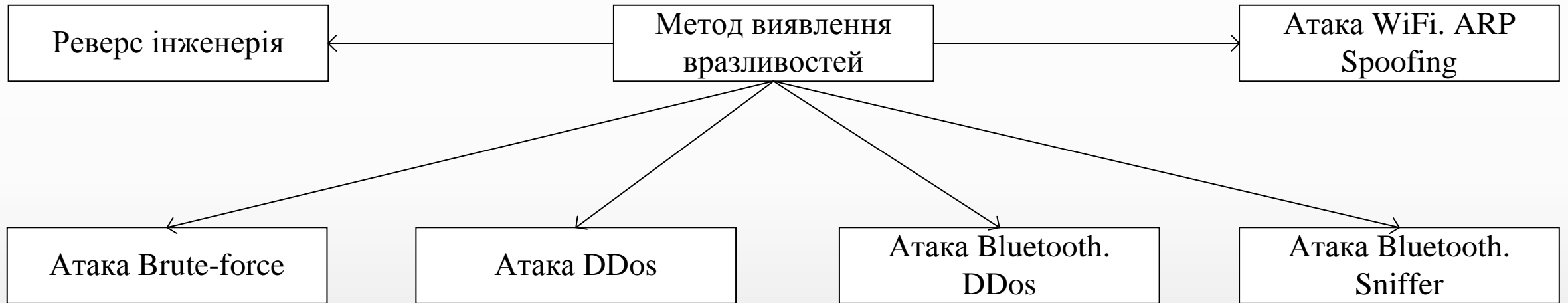
# Аналіз програмних рішень

№	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 функцій з 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.

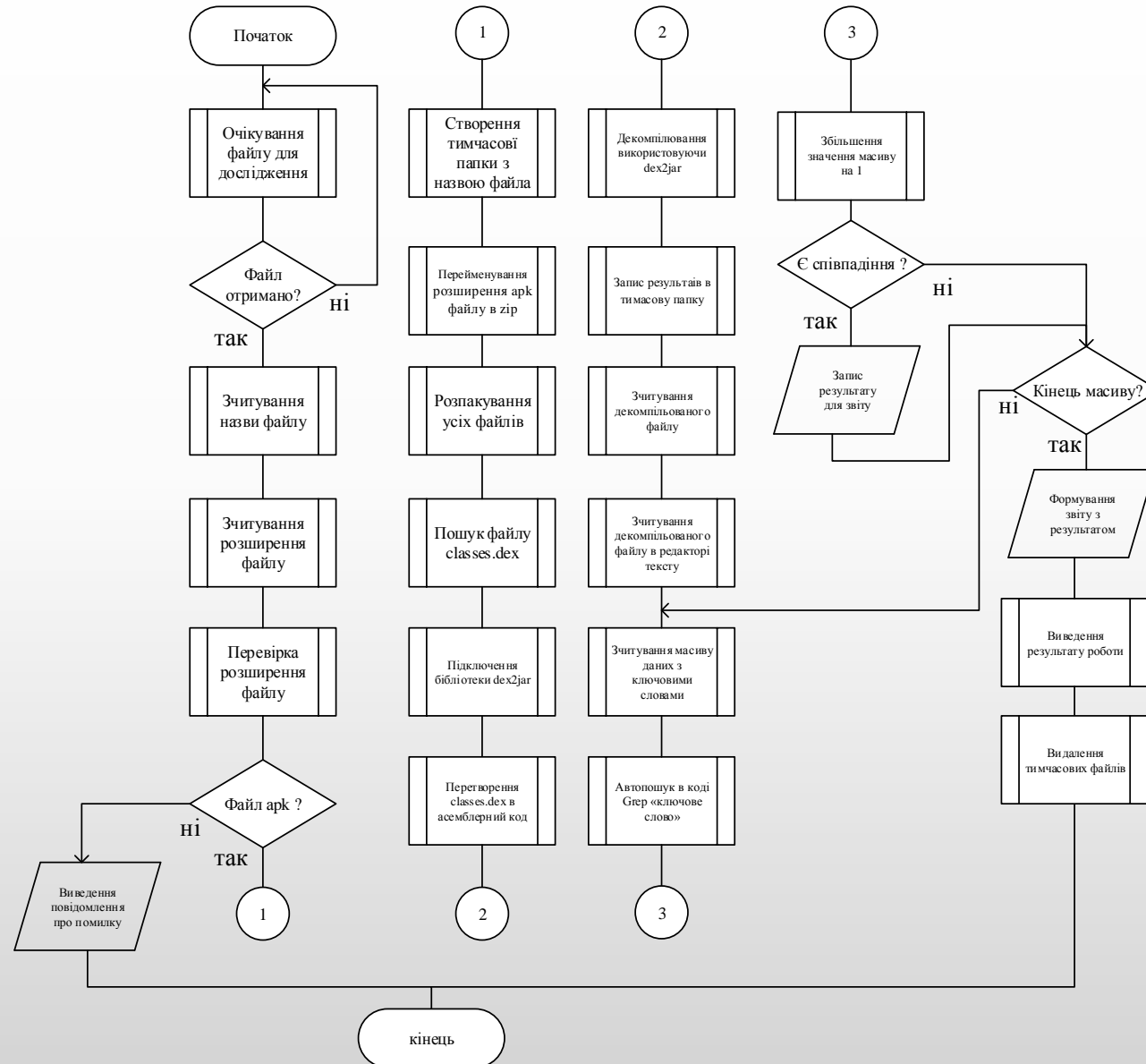
# Тести для виявлення вразливостей



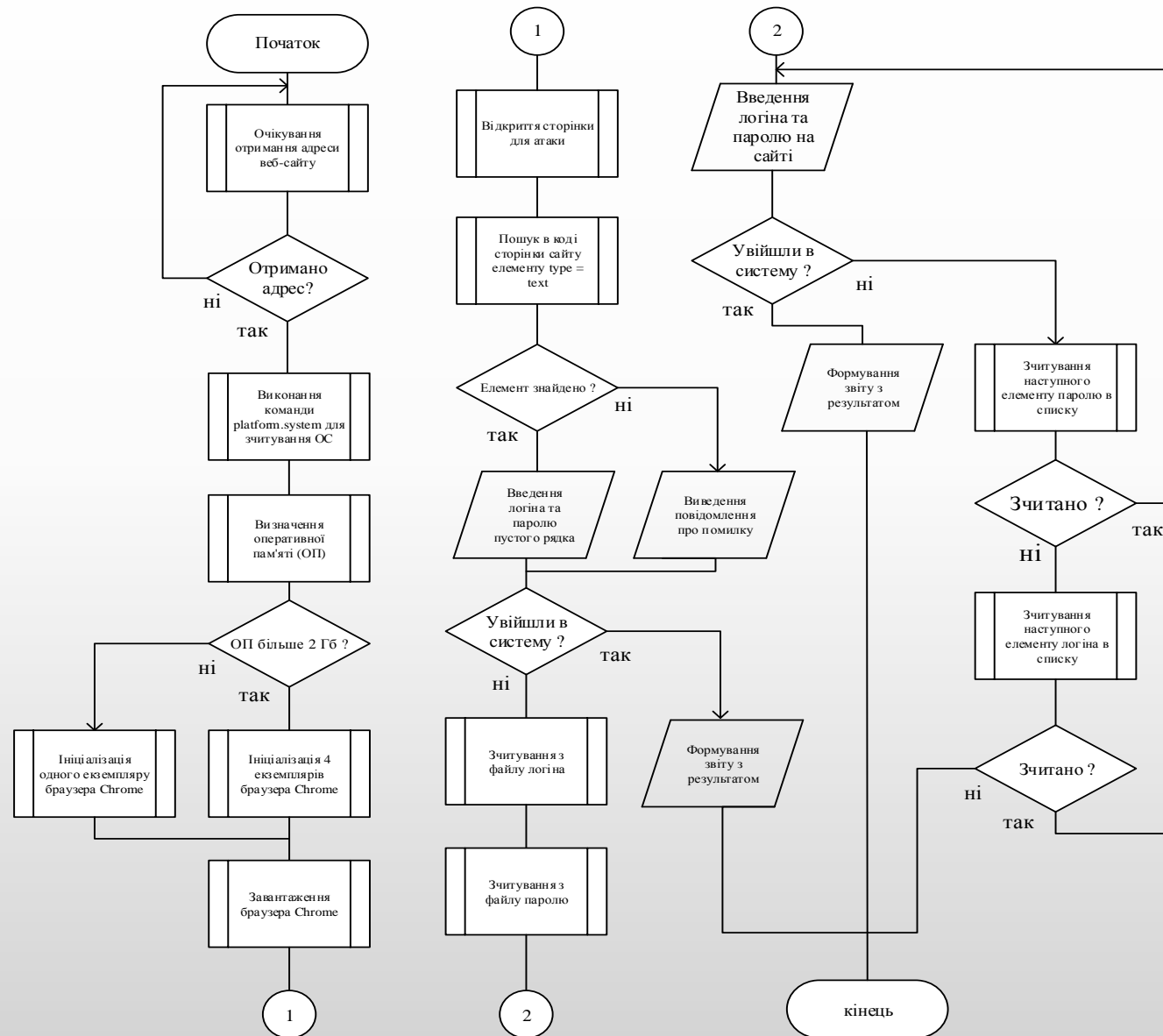
# Запропоновані методи виявлення вразливостей



# Алгоритм роботи методу реверсної інженерії

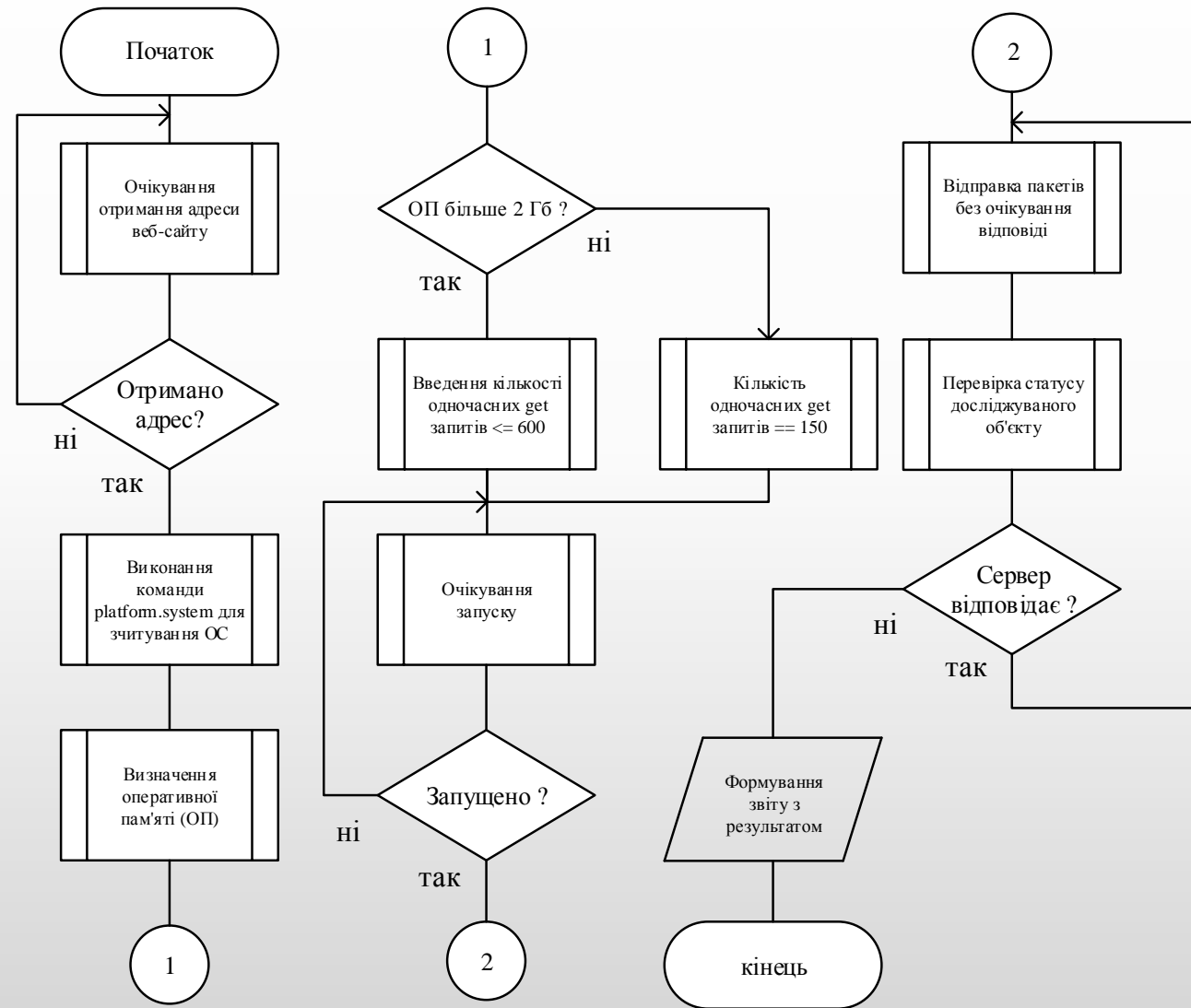


# Алгоритм роботи методу грубої сили

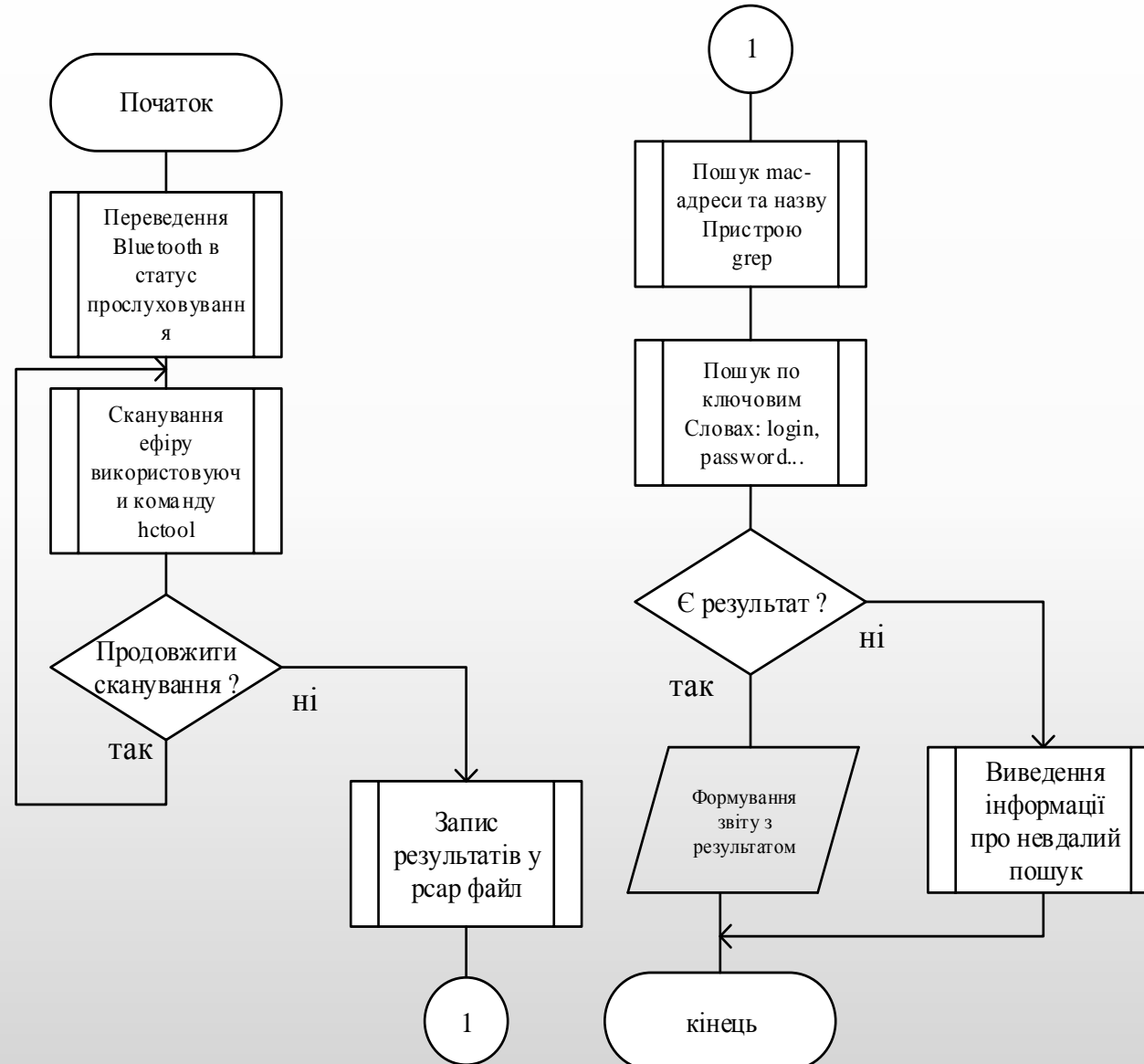




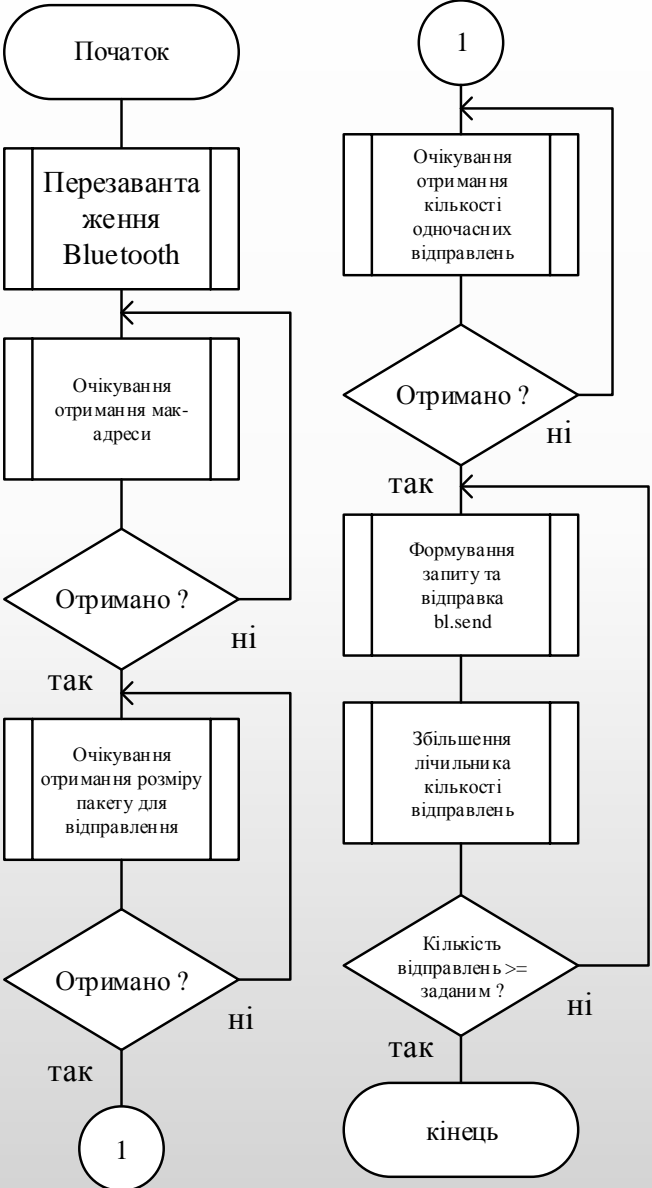
# Алгоритм роботи методу DDos-атаки



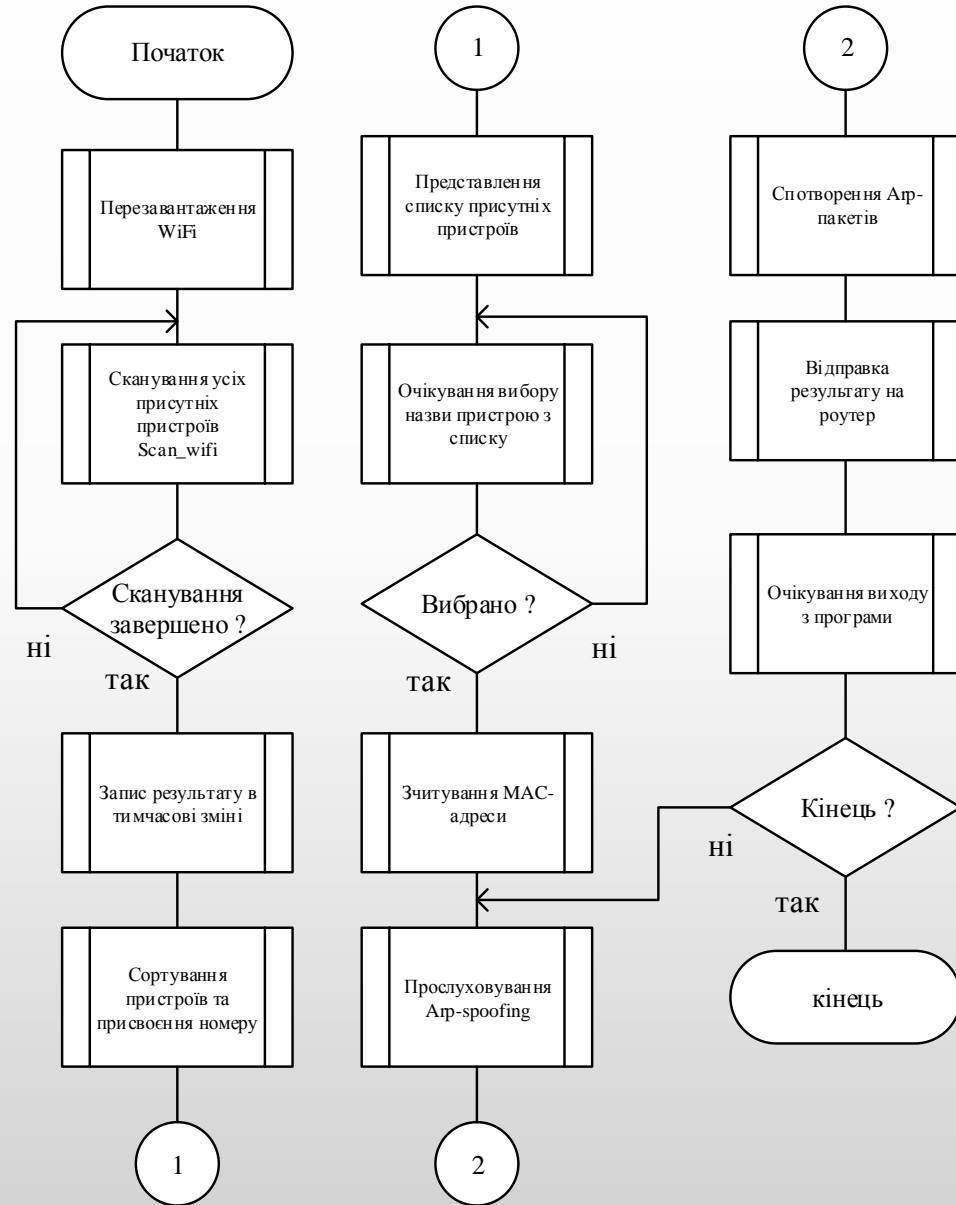
# Алгоритм роботи методу Bluetooth sniffer



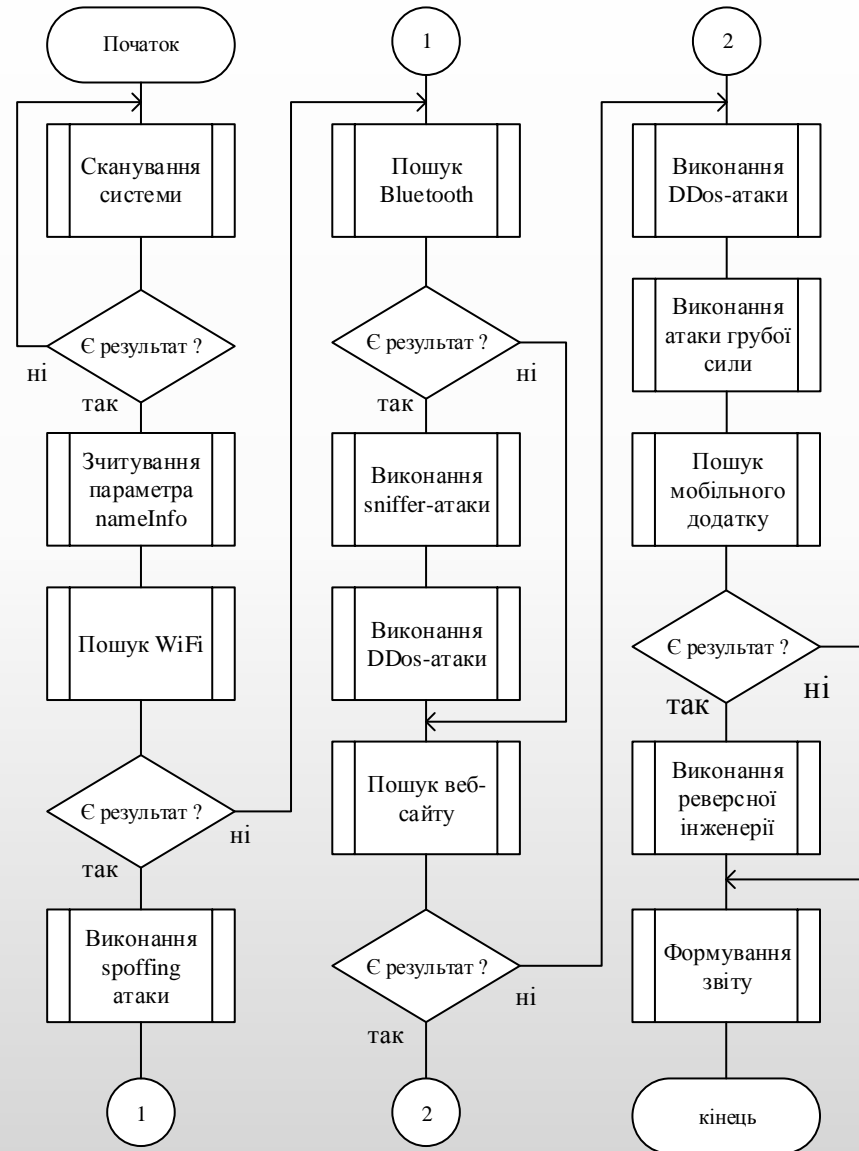
# Алгоритм роботи методу DDos-атаки на Bluetooth



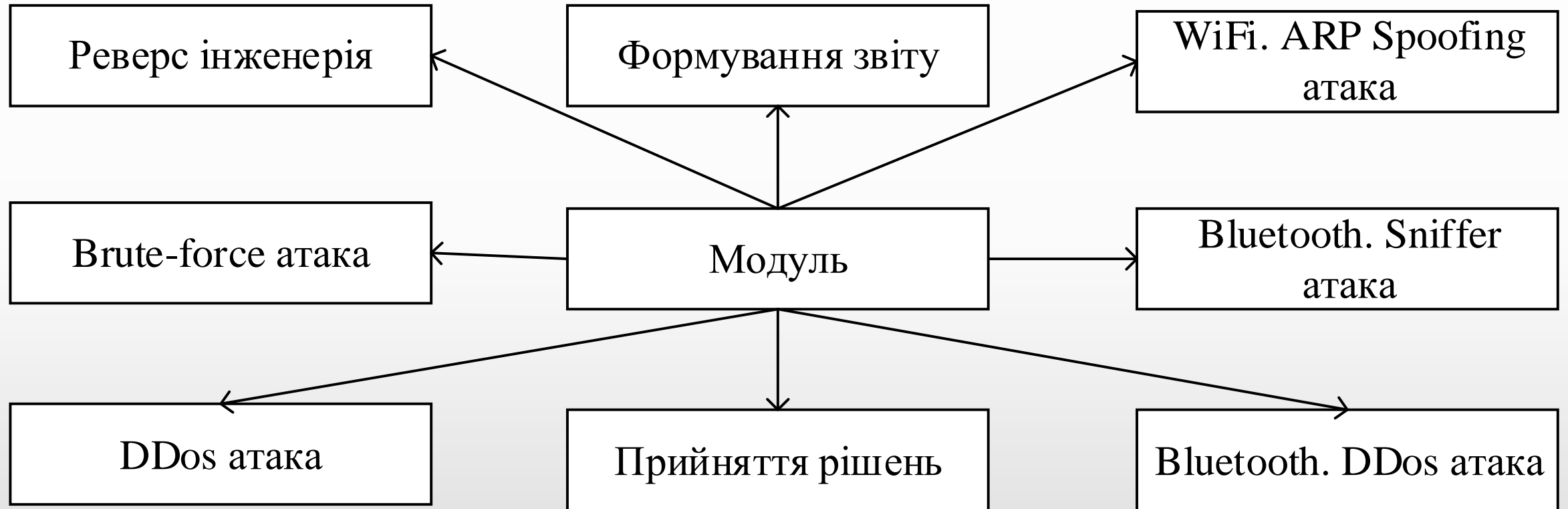
# Алгоритм роботи методу атаки spoofing



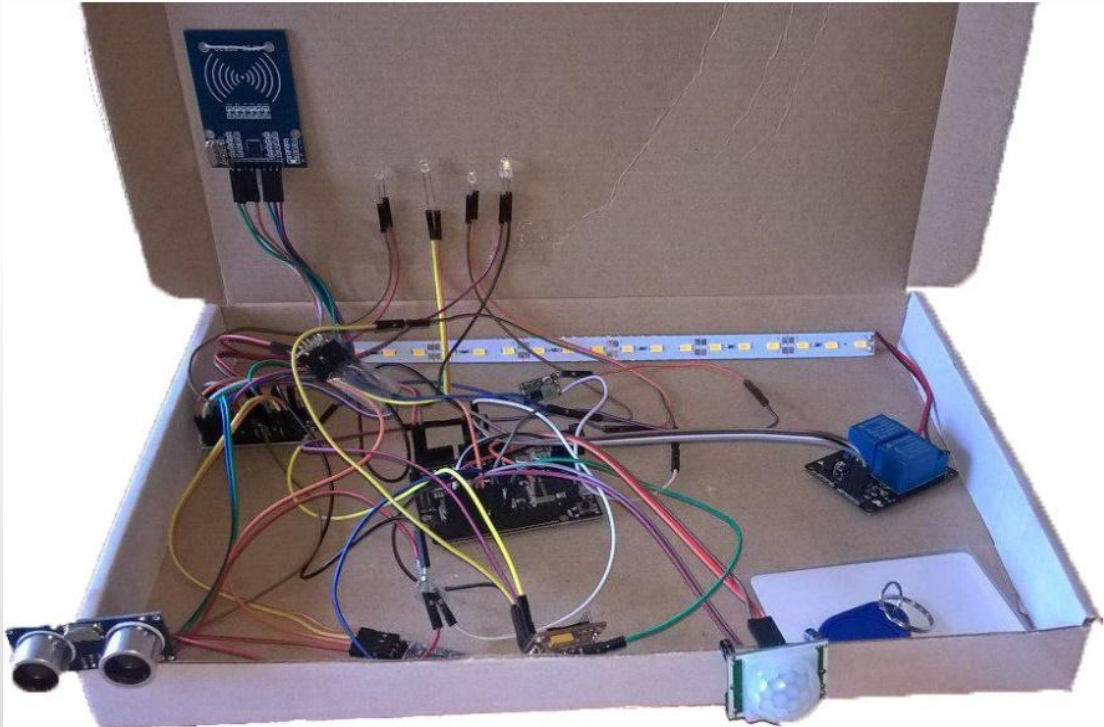
# Алгоритм модуля прийняття рішень



# Схема модулів програмного засобу



# Експериментальне дослідження

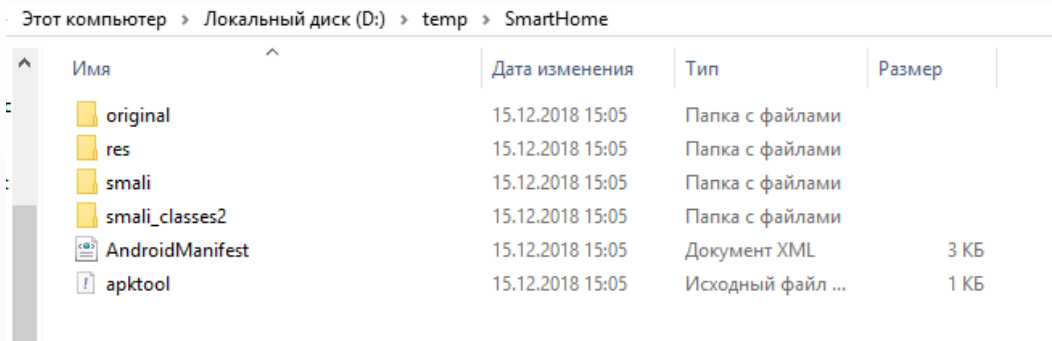


Назва	Марка
Arduino Uno	Robotdyn uno ch340/atmega328pa
Arduino Nano	V3.0 AVR ATmega328 P – 20AU
GSM модуль	SIM800L
RFID мітка	Rfid – rc522
Bluetooth модуль	HC – 06
Датчик руху	HC – SR501
WiFi	ESP 8266
Датчик відстані	hC – SR04

# Вигляд результатів дослідження



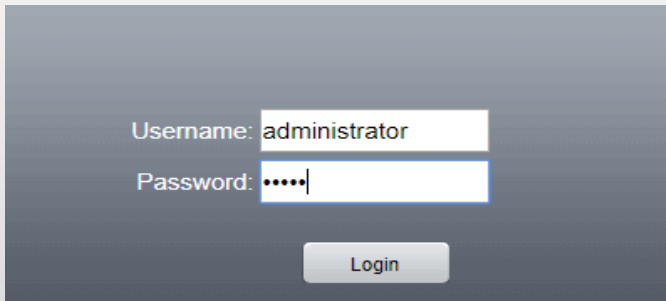
Інтерфейс мобільного додатку



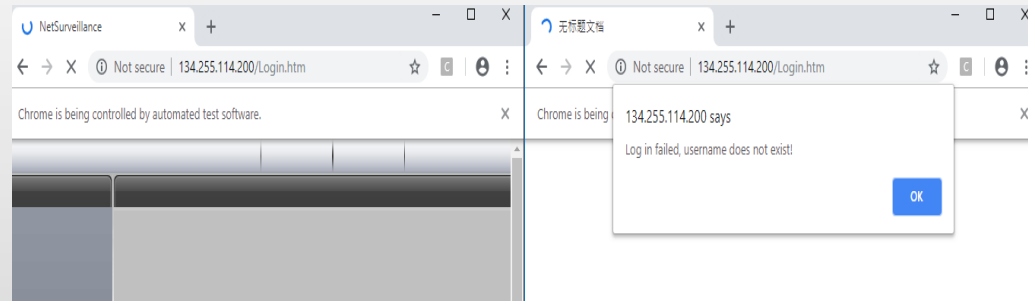
Декомпільований арк-файл

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

Фрагмент коду автентифікації



Форма авторизації



Результати виконання грубої сили

Google Chrome	10.9%	16.7 MB
Google Chrome	5.4%	16.7 MB

багатопотоковості

Запуск



# 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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	controller	host	HCI EVT	14	Rcvd Sniff Subrating
2	1.044288	controller	host	HCI EVT	36	Rcvd LE Meta (LE Advertising Report)
3	1.045025	controller	host	HCI EVT	32	Rcvd LE Meta (LE Advertising Report)
4	1.107638	controller	host	HCI EVT	36	Rcvd LE Meta (LE Advertising Report)
5	1.108050	controller	host	HCI EVT	32	Rcvd LE Meta (LE Advertising Report)
6	1.173760	controller	host	HCI EVT	36	Rcvd LE Meta (LE Advertising Report)
7	1.174459	controller	host	HCI EVT	32	Rcvd LE Meta (LE Advertising Report)
8	1.244321	controller	host	HCI EVT	36	Rcvd LE Meta (LE Advertising Report)
9	1.245010	controller	host	HCI EVT	32	Rcvd LE Meta (LE Advertising Report)
10	1.312262	controller	host	HCI EVT	36	Rcvd LE Meta (LE Advertising Report)
11	1.312986	controller	host	HCI EVT	32	Rcvd LE Meta (LE Advertising Report)
12	1.378044	controller	host	HCI EVT	36	Rcvd LE Meta (LE Advertising Report)
13	1.379051	controller	host	HCI EVT	32	Rcvd LE Meta (LE Advertising Report)
14	1.443839	controller	host	HCI EVT	36	Rcvd LE Meta (LE Advertising Report)

Результат виконання sniffer-атаки

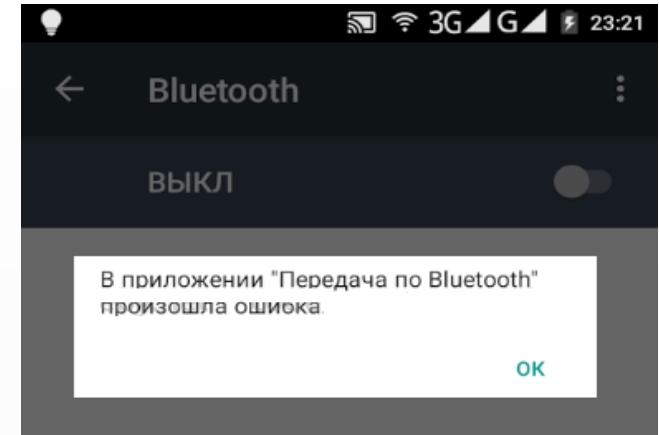
# Вигляд результатів дослідження

```
Target addr > 18:F0:E4:D0:C7:B2  
Packages size > 600  
Threads count > 100
```

Задання параметрів для DDoS-атаки на Bluetooth

```
[*] Built thread №97  
[*] Built thread №98  
[*] Built thread №99  
[*] Built thread №100  
[*] Built all threads...  
[*] Starting...  
Ping: 18:F0:E4:D0:C7:B2 from 38:B1:DB:40:71:28 (data size 600) ...  
Ping: 18:F0:E4:D0:C7:B2 from 38:B1:DB:40:71:28 (data size 600) ...  
Ping: 18:F0:E4:D0:C7:B2 from 38:B1:DB:40:71:28 (data size 600) ...  
Ping: 18:F0:E4:D0:C7:B2 from 38:B1:DB:40:71:28 (data size 600) ...  
Ping: 18:F0:E4:D0:C7:B2 from 38:B1:DB:40:71:28 (data size 600) ...  
Ping: 18:F0:E4:D0:C7:B2 from 38:B1:DB:40:71:28 (data size 600) ...  
Ping: 18:F0:E4:D0:C7:B2 from 38:B1:DB:40:71:28 (data size 600) ...
```

Виконання DDoS-атаки на Bluetooth



Результат виконання DDoS-атаки на Bluetooth

```
Online IPs:  
[0] 192.168.43.1      18:F0:E4:D0:C7:B3  
Choose a target: 0  
Target: 192.168.43.1  
Spoofing started...
```

Виконання атаки arp-spoofing

No.	Time	Source	Destination	Protocol	Length	Info
7	5.616434	Dele_a3:0d:10	Sonicwal_09:c2:50	ARP	42	192.168.43.1 is at 00:24:e8:a3:0d:10
8	5.616503	Dele_a3:0d:10	Intel_53:f2:7c	ARP	42	192.168.43.1 is at 00:24:e8:a3:0d:10 (d
9	5.626711	Dele_a3:0d:10	Sonicwal_09:c2:50	ARP	42	192.168.43.1 is at 00:24:e8:a3:0d:10
10	5.626776	Dele_a3:0d:10	7c:05:07:ad:43:67	ARP	42	192.168.51.1 is at 00:24:e8:a3:0d:10 (d

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!