МІНІСТЕРСТВО ОСВІТИ І НАУКИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

АТЕСТАЦІЙНА ВИПУСКНА РОБОТА БАКАЛАВРА

на тему:

Розробка інформаційної системи побудови кабельних та бездротових мереж

Керівник АВР: д.т.н., проф. Терентьєв О.О.

Розробив: студент спеціальності
122 «Комп`ютерні науки» ОС «бакалавр»
Горкуценко В.

Мета роботи – створити та налаштувати захищену бездротову локальну мережу.

Метод дослідження – теоретичний аналіз протоколів бездротових локальних мереж, вивчення механізмів передачі даних в Wi-Fi мережах, можливості її захисту та аналіз програмних продуктів для реалізації даного типу мереж.

Результат – реалізована захищена бездротова мережа на базі стандарту IEEE 802.11n.

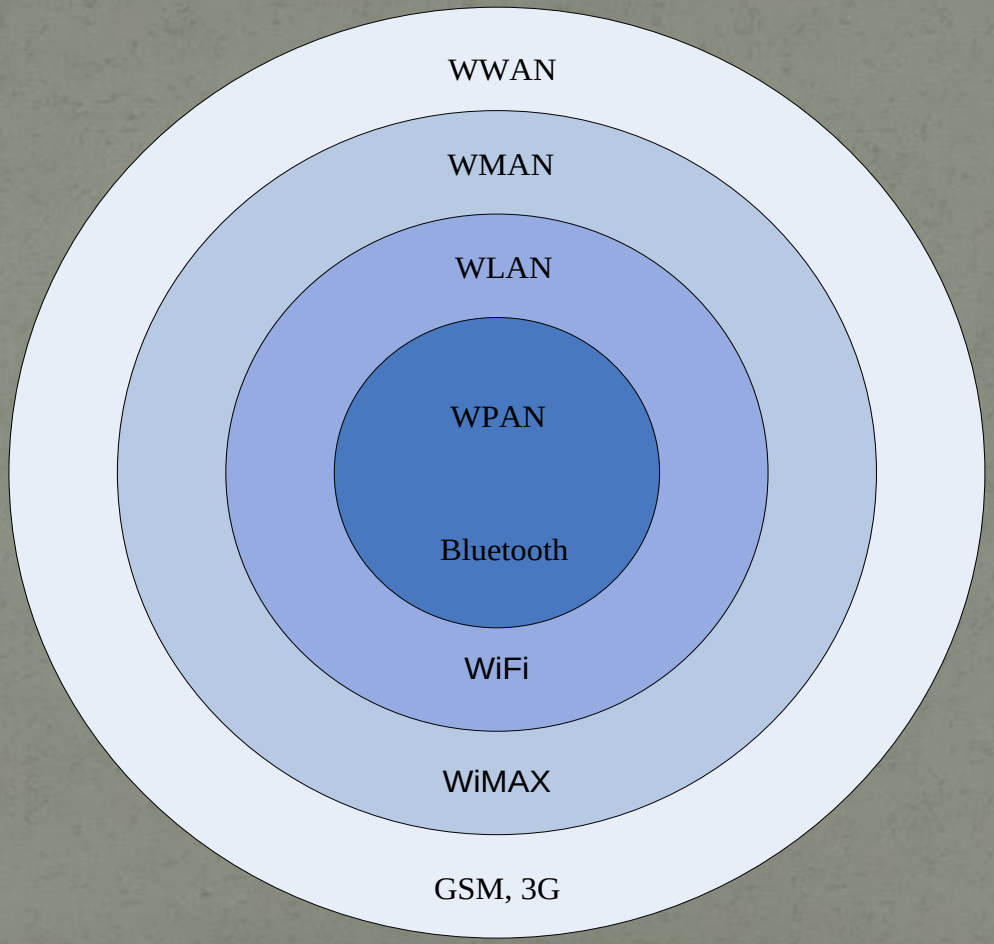
Актуальність робити

Способи мережного доступу з кожним роком стають все популярніше, їх кількість невпинно зростає. І постає звичайно питання про безпеку. Адже саме безпека доступу користувачів та механізм захисту – є одними з нагальних проблем сьогодення.

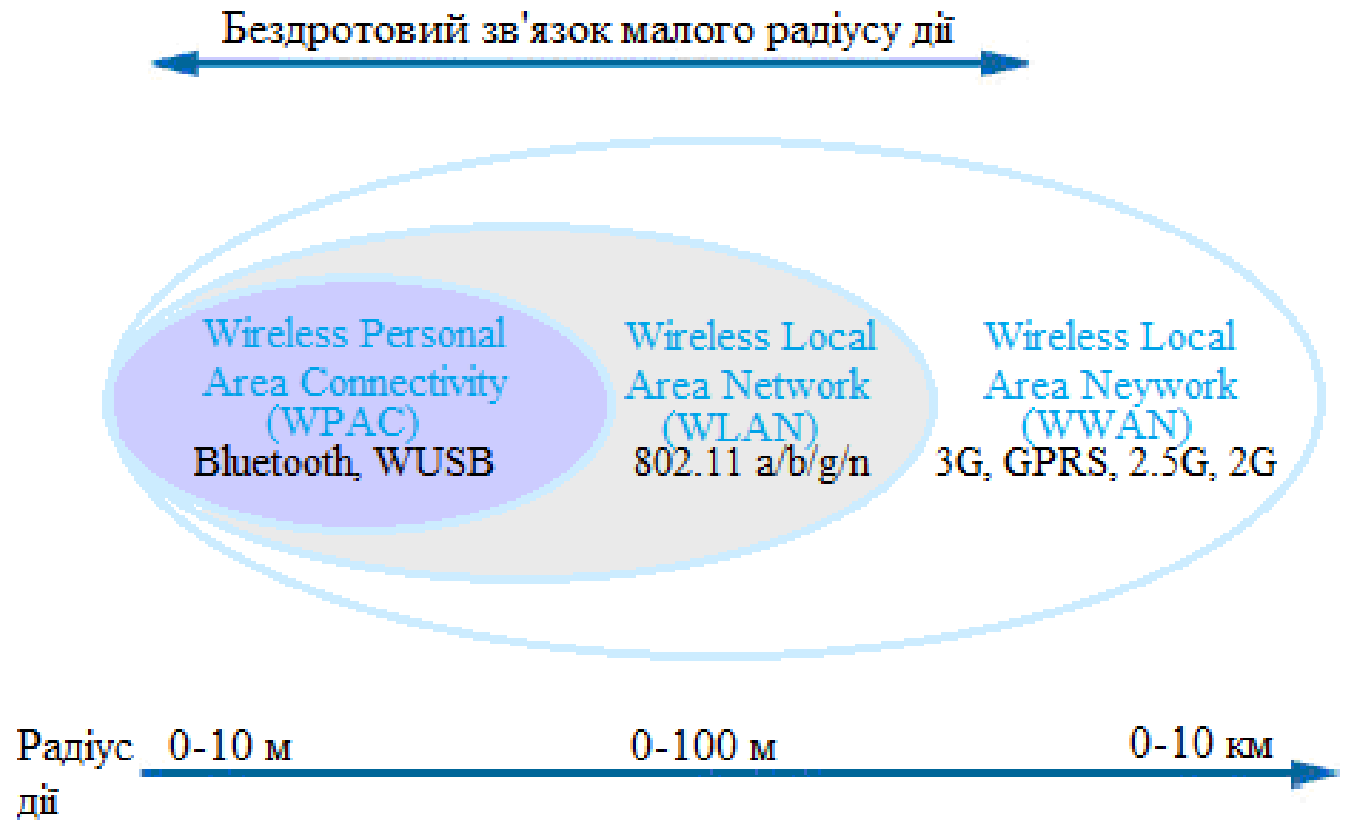
Постановка задачі

- вивчити роботу бездротових мереж на фізичному рівні;
- проаналізовати можливості протоколів автентифікації та їх характеристики;
- розглянути сучасні можливості бездротових технологій;
- протестувати можливість серверів автентифікації на забезпечення захищеності Wi-Fi мереж;
- провести аналіз бездротових з’єднань та використати одне із типів з'єднань з точкою доступу ;
- вивчити ринок серверів та налаштовати один з серверів для точки доступу.

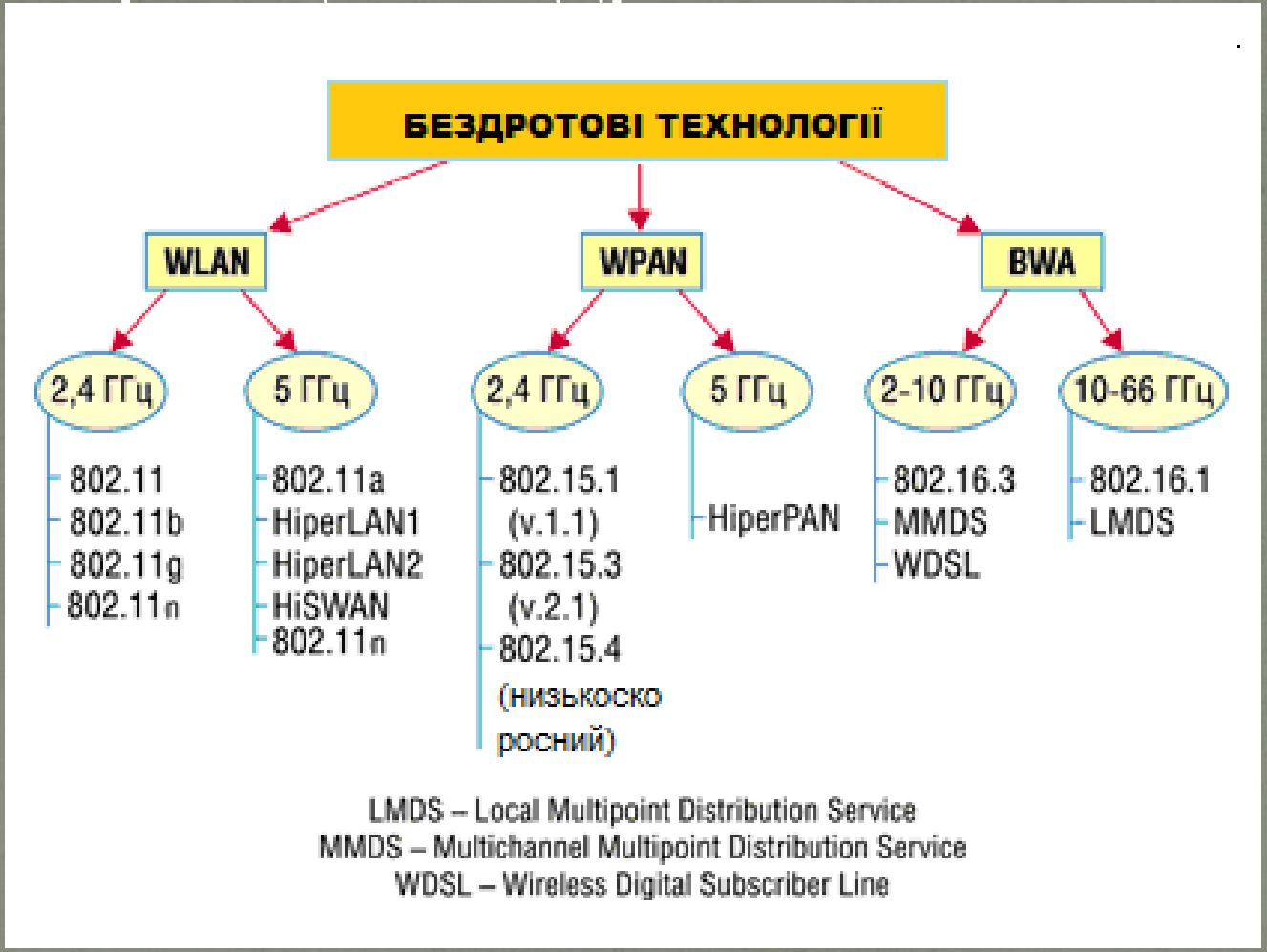
Класифікація бездротових мереж



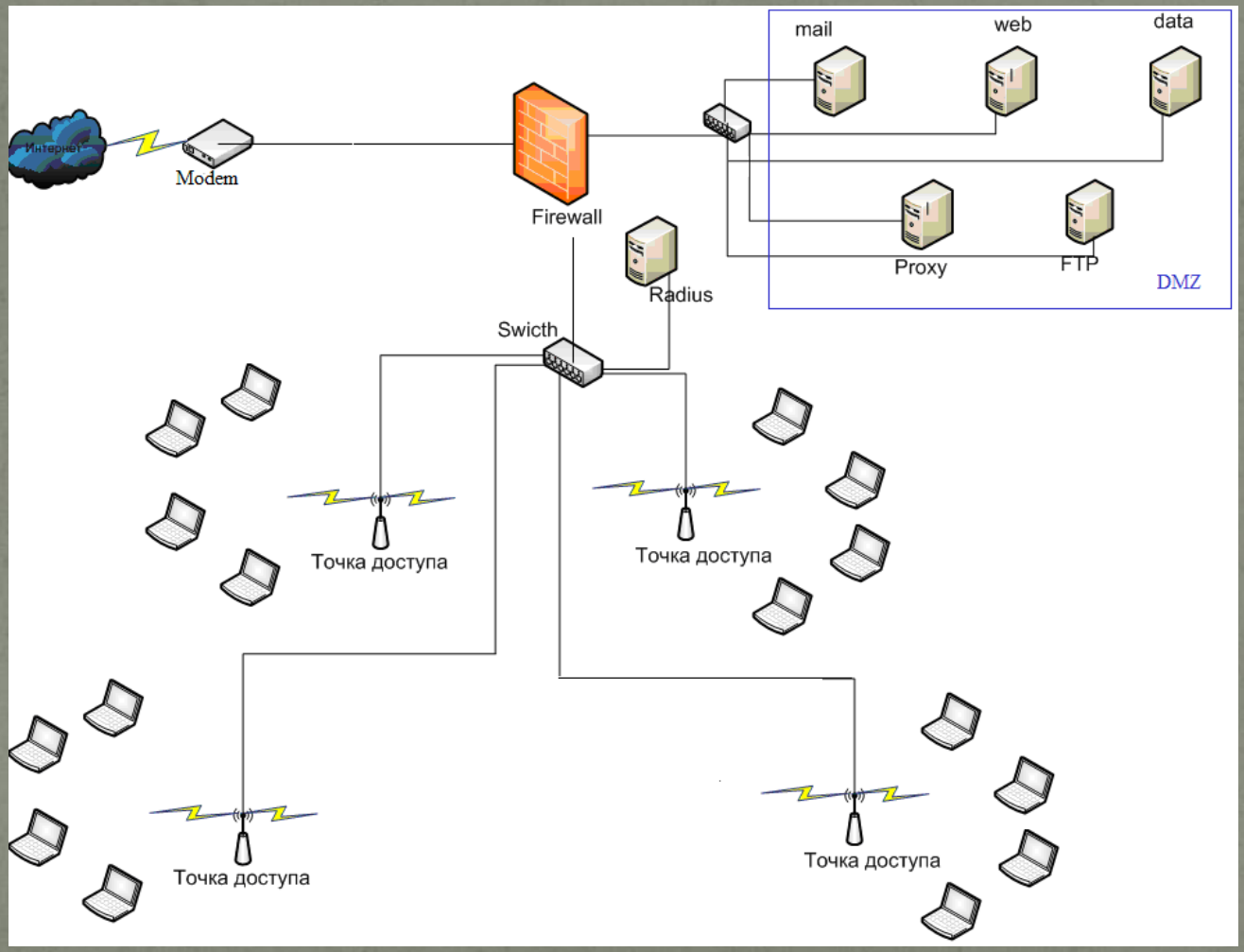
Радіус дії персональних, локальних та глобальних бездротових мереж



Класифікація бездротових технологій



Структура захищеної локальної бездротової мережі



КНУБА

Емблема WI FI

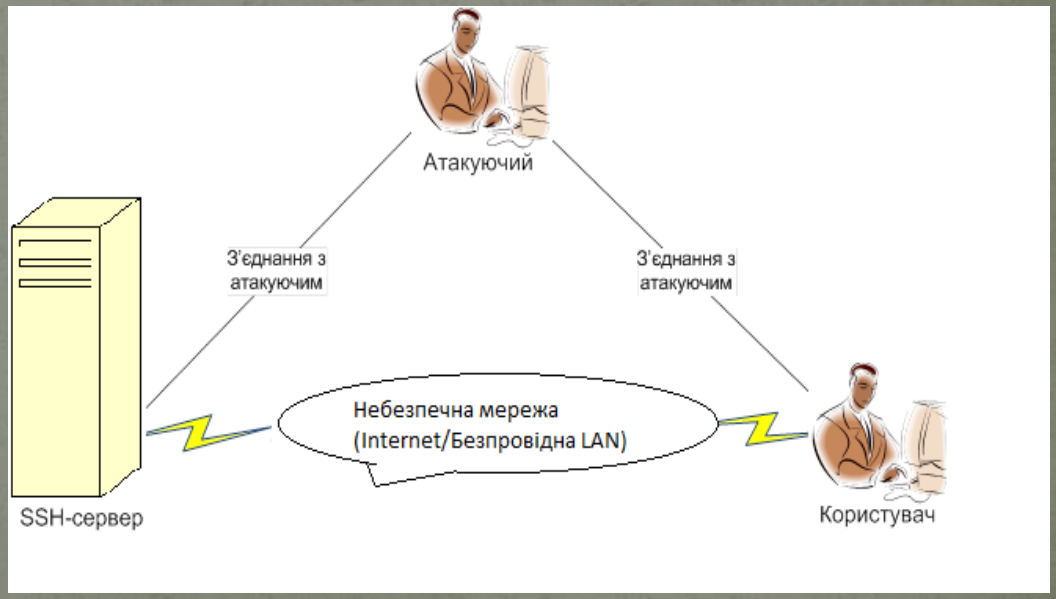
Емблема Wi-Fi У останні два роки, сотні нових компаній почали встановлювати Wi-Fi точки доступу (звані «хот споти») в кафе, готелях, аеропортах і вокзалах і інших місцях масового дозвілля і перебування. Ці «Оператори хот-спотів» або «HSOs» встановлюють Wi-Fi AP's і надають високошвидкісний Інтернет доступ в цьому місці на комерційній основі.

АТАКА ПІДСЛУХОВУВАННЯ

- **Підслуховування – найпоширеніша проблема. Анонімні шкідники можуть перехопити радіосигнал і розшифрувати передаваємі дані, як показано.**
- **Обладнання для прослуховування в мережі може бути не складніше, ніж те, що використовується для звичайного доступу до цієї мережі. Щоб перехопити передачу, зловмисник повинен знаходитись поблизу передавача.**

Атака «людина всередині»

- розподілена відмова в обслуговуванні (DDoS);
- збір конфіденційної інформації;
- спамінг;
- кібер шантаж;
- анонімний доступ в мережу.

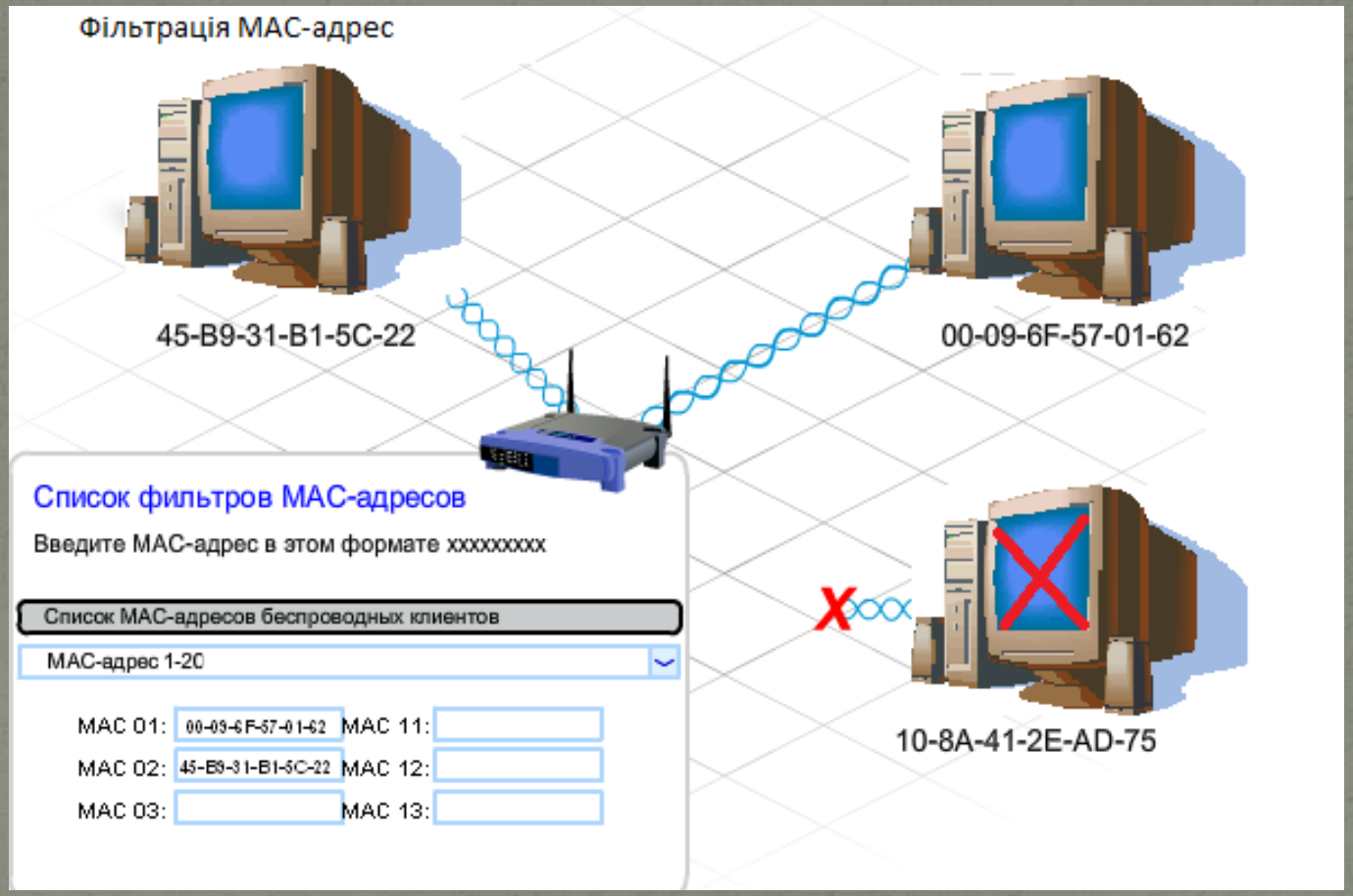


Атака „відмова в обслуговуванні”

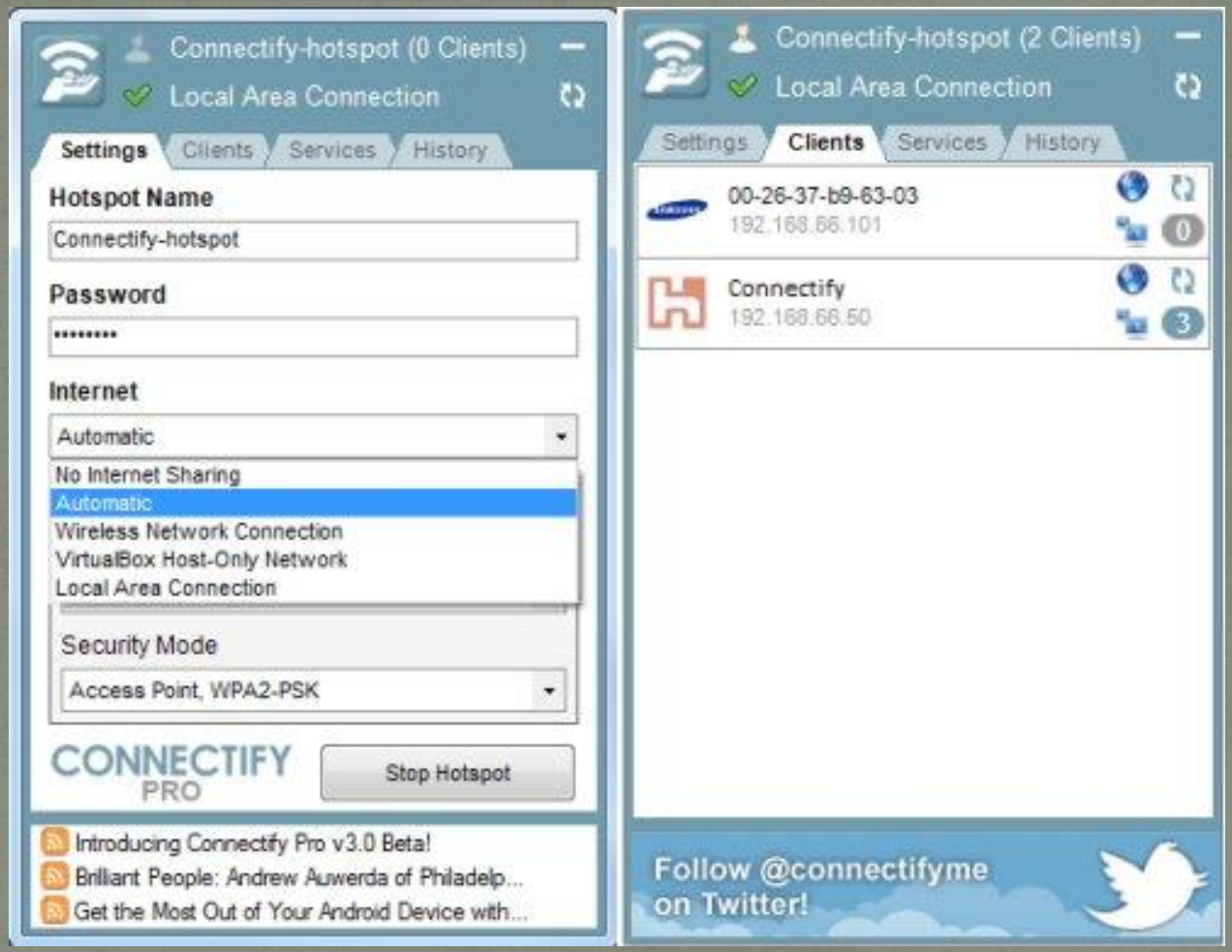
Методи захисту комп'ютерних мереж від проникнення

- аналіз телеметрії;
- система виявлення аномалій;
- аналіз журналу DNS (бот-мережі часто використовують безкоштовні служби DNS, де розміщують адреси піддоменів серверів IRC та спеціальні програми із шкідливим кодом, який містить жорстко задані посилання на DNS-сервер);
- система-приманка («приманка» - замкнута, захищена і контрольована область, імітує вразливу мережу, ресурс або службу, основна мета - приманити і виявити шкідливі атаки та спроби вторгнення);
- Антивірусні системи.

Фільтрація MAC-адрес



Connectify


Connectify-hotspot (0 Clients)
Local Area Connection
Settings
Clients
Services
History
Hotspot Name
Connectify-hotspot
Password
Internet
Automatic
No Internet Sharing
Automatic
Wireless Network Connection
VirtualBox Host-Only Network
Local Area Connection
Security Mode
Access Point, WPA2-PSK
CONNECTIFY PRO
Stop Hotspot
Introducing Connectify Pro v3.0 Beta!
Brilliant People: Andrew Auwerda of Philadelp...
Get the Most Out of Your Android Device with...
Connectify-hotspot (2 Clients)
Local Area Connection
Settings
Clients
Services
History
00-26-37-b9-63-03
192.168.66.101
0
Connectify
192.168.66.50
3
Follow @connectifyme on Twitter!

Сучасні рішення для побудови захисту безпровідної мережі від шкідливих вторгнень

- **Palo Alto -** міжмережний екран, який працює на рівні додатків;
- **Solera DeepSee** – автоматизований аналізатор інформаційних потоків, функціонал якого дозволяє перехоплювати мультимедійні дані, не нести навантаження на продуктивність мережі, крім того має здатність перенаправляти потоки даних в окремі її сегменти;
- **Snort** – сучасна система виявлення вторгнень, яка працює на основі сенсорів, що розгортаються на робочих станціях користувачів мережі (контролюються з єдиного центру: «керуючого серверу»;
- Різні автоматичні способи влаштовані в програми;
- Антивіруси.

Для реалізації поставленої задачі було виконано наступне:

- ✓ вивчено роботу бездротових мереж на фізичному рівні;
- ✓ проаналізовано можливості протоколів автентифікації та їх характеристики;
- ✓ розглянуто сучасні можливості технологій;
- ✓ було протестовано можливість серверів автентифікації на забезпечення захищеності Wi-Fi мереж;
- ✓ проведено аналіз та використано одне із типів з'єднань з точкою доступу ;
- ✓ вивчино ринок серверів та налаштовано один з серверів для точки доступу.

Дякую за увагу