**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**ІМЕНІ ІГОРЯ СІКОРСЬКОГО"**

Радіотехнічний факультет

Кафедра прикладної радіоелектроніки

# ЗВІТ

## З ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

**Виконав**:

Студент 3 курсу, групи РА-п01

Собко О.В.

(Прізвище І.П.) Підпис

**Звіт прийняв:**

Шульга А. В.

«____» _____2023 р.

Дружинін В. А .

(Прізвище І.П. Підпис керівника диплому)

«____» _____2023 р.

Київ – 2023 р.

ЗМІСТ

# ВСТУП

Широке поширення бездротових локальних мереж і застосування їх в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню властивих їм проблем інформаційної безпеки. При цьому існуючі засоби захисту, в тому числі комерційні бездротові системи виявлення атак, не забезпечують повноцінного захисту від шкідливої мережевої активності.

Технологія WiFi є однією з найперспективніших на сьогоднішній день в області комп'ютерного зв'язку та змінює весь світ. Ці зміни стосуються того, як ми працюємо, граємо і взаємодіємо один з одним. Економіка Wi-Fi швидко змінює світ за рахунок високошвидкісних бездротових служб роботи з інформацією. Вона дозволяє користувачеві завжди бути «підключеним», ущільнює час, оскільки він може бути продуктивним незалежно від того, де знаходиться. Мобільність - це ікона нового покоління.

Стандарт 802.11, або Wi-Fi, переходить з самого початку властивого йому розряду вертикальних додатків для складів, управління запасами і засоби зв'язку для касових апаратів до горизонтальних додатків, що використовуються багатьма з нас вдома і на роботі. На сьогоднішній день Wi-Fi в основному використовується як високошвидкісне бездротове розширення мереж Ethernet, єднаючи нас постійно і без будь-яких зусиль з нашого боку з Internet і нашими офісними додатками, де б ми не знаходилися.

Бездротові локальні мережі (WLANs), засновані на стандарті 802.11, забезпечують мобільність і смугу частот, які необхідні користувачам мереж.

Перші бездротові мережі, такі як Aloha, ARDIS і Ricochet, забезпечували швидкість передачі даних менше 1 Мбіт/с. Стандарт 802.11 дозволяє виробникам забезпечувати взаємодію зі швидкостями 2 Мбіт/с. В результаті ратифікації в 1999 році стандарту 802.11b планка піднялася до 11 Мбіт/с; ця швидкість конкурентоспроможна з Ethernet на 10 Мбіт/с. Стандарти 802.11a і 802.11g регламентують швидкість передачі даних близько 54 Мбіт/с, що можна

порівняти з Fast Ethernet при тих же витратах. Як і перші розробники WLAN, вертикальні (охоплюють всі стадії виробництва) галузі, такі як роздрібна торгівля, охорона здоров'я і виробництво, оцінили переваги WLAN і бездротових додатків. Багато з цих галузей розглядають WLAN як невід'ємну частину свого бізнесу. Завдяки високому попиту виробники можуть збільшити обсяги виробництва і знизити собівартість, а отже, і ціну своїх виробів, тому апаратне забезпечення WLAN стає доступним споживачам і підприємствам за помірними цінами.

Однак бездротова середовище передачі в силу своїх особливостей створює потенційні умови для прослуховування мережевого трафіку і неконтрольованого підключення до бездротової мережі зловмисників, які перебувають в її зоні дії. Крім того, дані мережі схильні до, в тому числі з причини недосконалості протоколів, множинним типам атак. Великі підприємства змушені купувати дорогі системи виявлення та запобігання атак. Системи виявлення атак можуть бути реалізовані як на основі моделі виявлення відомих ознак (сигнатур), так і на основі виявлення відхилень від нормальної поведінки (аномалій).

Таким чином, у дипломній роботі вирішується актуальне завдання, що полягає в дослідженні алгоритмічного та програмного забезпечення системи, що дозволяє підвищити ефективність виявлення атак в локальних бездротових мережах Wi-Fi.

# 1. АНАЛІЗ СТАНУ РОЗВИТКУ ТА ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БЕЗПРОВОДОВИХ ЛОКАЛЬНИХ МЕРЕЖ НА БАЗІ ТЕХНОЛОГІЇ WI-FI

## 1.1 Тенденції розвитку локальних мереж на базі технології Wi-Fi

За прогнозами фахівців, в 2020 році загальна кількість проданих мобільних пристроїв перевищить три з половиною мільярди, з них один мільярд - це «звичайні» мобільні апарати, другий – смартфони і півтори планшети та пристрої які підтримують Wi-Fi з`єднання. У минулий 2019-й рік став першим роком, коли більшість всіх мобільних телефонів стала мати можливість роботи з Wi-Fi. Таким чином, найближчим часом користування мобільними пристроями і портативною технікою стане масовим і повсюдним. Аналітична компанія Infonetics прогнозує зростання застосування в світі бездротового обладнання рис. 1.1.

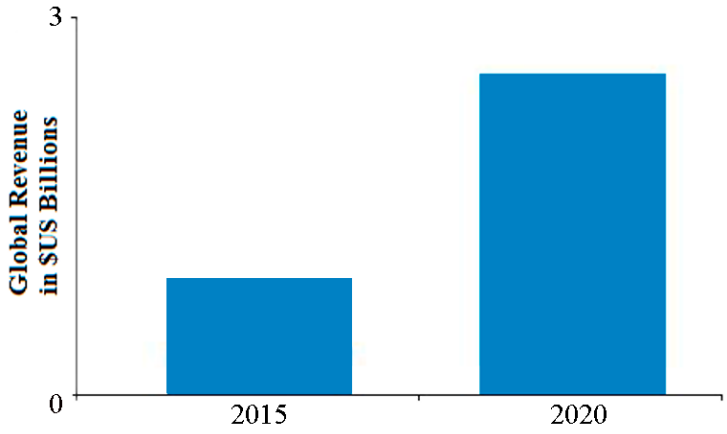


Рис. 1.1. Тенденція зростання користувачів Wi-Fi

Багато аналітиків як і раніше серйозно оцінюють наміри Wi-Fi Alliance скласти реальну конкуренцію рішенням WiMAX і LTE в секторі мобільної передачі даних для великих міст. І для такого оптимізму поки є всі підстави, враховуючи високі витрати на розгортання мобільних мереж 4-го покоління (4G), в той час як Wi-Fi залишається порівняно дешевої і високопродуктивної

технологією бездротового доступу, що має найширший асортимент термінальних пристроїв і значну доступність обслуговування .

У найближчі кілька років можна очікувати подальшого розвитку лінійки Wi-Fi рішень. При цьому очікується наступні рішення:

- освоєння частотного діапазону 60 ГГц. Wireless Gigabit Alliance (WiGig Alliance) активно працює над освоєнням технологією Wi-Fi діапазону 60 ГГц з піковими швидкостями передачі до 7 Гбіт/с для сценаріїв піко стільникового покриття. Подібне збільшення продуктивності Wi-Fi є серйозним кроком вперед навіть порівняно з високошвидкісними рішеннями IEEE 802.11n (до 300 Мбіт / с), які передбачають одночасне використання двох або трьох призначених для користувача потоків і об'єднання двох робочих радіоканалів по 20 МГц. Обмежуючим фактором даного рішення є короткий радіус дії, а також необхідність одночасної підтримки базових частотних діапазонів Wi-Fi - 2,4 ГГц і 5 ГГц. Зате перспективи розвитку «хмарних» сервісів і OTT-послуг на базі високошвидкісного бездротового доступу Wi-Fi 60 ГГц здаються цілком реалістичними;

- розвиток рішень Wi-Fi Direct, що дозволяють забезпечити зі стандартними швидкостями Wi-Fi прямі з'єднання між самими різними клієнтськими пристроями (комунікатори, смартфони, принтери, цифрові фото / відео камери і ін.), минаючи традиційні точки доступу і бездротові маршрутизатори;

- за прикладом технології Bluetooth Wi-Fi Alliance, як розробник рішень Wi-Fi Direct, підтримує ряд специфікацій, зокрема, для забезпечення інформаційного захисту - Wi-Fi Protected Access 2 (WPA2);

- підтримка поліпшених рішень VoIP з новим набором WFA-протоколів з метою подальшого розвитку конкурентоспроможних альтернативних голосових послуг;

- розвиток стільникових (сітка) Wi-Fi мереж, заснованих на відносно дешевих модулів, кожен з яких з'єднаний з радіо з усіма своїми сусідами в рамках діапазону. Важливою перевагою Wi-Fi пористих мереж також мережеві

модулі самоорганізації і можливість відновлення в разі виходу з ладу деяких вузлів. Реалізація специфікації IEEE 802.11s створить простий і недорогий мережі Wi-Fi з підтримкою альтернативних маршрутів і підвищення надійності;

- подальше удосконалення радіоінтерфейсу Wi-Fi. Передбачувані в рамках специфікації IEEE 802.11n поліпшення параметрів радіозв'язку доповнюються підвищенням надійності чіпсетів, застосуванням технології паритетного кодування для усунення помилок, поліпшенням прийому в точках доступу за рахунок оптимізації формування діаграм спрямованості приймальних антен;

- удосконалення клієнтського досвіду Wi-Fi за рахунок оптимізації взаємодії з точками доступу. Розвиток специфікації IEEE 802.11v націлене на підтримку механізмів управління параметрами радіомережі Wi-Fi в аспекті зменшення енергоспоживання. У свою чергу впровадження протоколу 802.11k для поліпшення управління радіоресурс дозволить в мережах Wi-Fi ідентифікувати слабкі сигнали або зони невпевненого прийому і, відповідно, оптимізувати бездротове обслуговування.

За останній час IEEE стандартизовані наступні специфікації:

- IEEE 802.11mb - технічне обслуговування стандарту;

- IEEE 802.11aa - Робастное потокове аудіо і відео;

- IEEE 802.11ac - забезпечення високошвидкісної передачі для діапазонів нижче 6 ГГц (2013 рік);

- IEEE 802.11ad - забезпечення високошвидкісної передачі для діапазону 60 ГГц (2012 рік);

- IEEE 802.11ae - управління якістю;

- IEEE 802.11af - Wi-Fi з використанням когнітивного радіо.

Очікується стандартизація специфікацій:

- IEEE 802.11ai - забезпечення ефективного початкового доступу;

- IEEE 802.11ah - освоєння діапазонів нижче 1 ГГц.

В якості ефективного механізму забезпечення інформаційної безпеки в сучасних рішеннях Wi-Fi використовуються рішення специфікації IEEE 802.11i

і механізми встановлення автентичності EAP; обидва рішення мають сертифікати Wi-Fi Alliance's Wi-Fi Protected Access 2 (WPA2) -Enterprise certification. Технологія WPA2 заснована на стандарті IEEE 802.11i і являє собою 128-бітове AES-шифрування з перевіркою достовірності на основі попередніх ключів (PSK) або стандарту 802.1x RADIUS, що добре підходить для реалізації функцій управління авторизацією, аутентификацией і адміністрування (AAA).

Майже всі бездротові мережі мають справу з широким розмаїттям термінальних пристроїв, як за допомогою SIM-карти (наприклад, смартфони), і без обходиться їм (наприклад, планшетні комп'ютери, ноутбуки і нетбуки). Саме з цієї причини, що Wi-Fi гарячих точок доводиться підтримувати нове покоління альтернативних і аутентифікації EAP-SIM механізмів, таких як протокол X.509. рис. 1.2 представлений прогноз проникнення термінальних пристроїв в Wi-Fi мережі.


Рис. 1.2. Прогноз проникнення термінальних пристроїв в Wi-Fi

Таким чином, за останні роки технологія Wi-Fi зазнала ряд поліпшень, що дозволило створювати досить недороге обладнання, яке за рахунок високої швидкості передачі (до 600 Мбіт/с) і доступного широкого спектра (до 500 МГц) є цілком конкурентоспроможним на тлі стільникових мереж 2G/3G/4G.

Розподілений Wi-Fi. Останнім часом спостерігається тенденція поділу широкосмугового бездротового з'єднання і цифрового контенту мереж Wi-Fi. Крім реалізації концепції систем, що самоорганізуються (ad-hoc) мереж поділ Wi-Fi дозволить операторам впровадити нові бізнес-моделі, в яких самі абоненти мають можливість розподіляти свою пропускну здатність.

### 1.2 Переваги і особливості мереж Wi-Fi

Бездротова технологія Wi-Fi володіє наступними особливостями:

- підтримка множинних діапазонів частот (2,4 ГГц, 5 ГГц і в перспективі 60 ГГц);

- скорочення експлуатаційних витрат завдяки підтримці методів підвищення пропускної здатності;

- забезпечення безшовного роумінгу для призначених терміналів користувачів;

- підтримка якості обслуговування на рівні корпоративного класу;

- підтримка множинних мережевих ідентифікаторів (SSID) для диференціювання послуг;

- реалізація функцій управління авторизацією, аутентифікації та обліком (AAA);

- скорочення витрат завдяки підтримці структури пористих мереж;

- оптимізація управління параметрами радіоінтерфейсу.

Бездротова технологія Wi-Fi має наступні переваги:

- підтримка множинних діапазонів частот дозволить операторам більш ефективно і гнучко застосувати радіочастотний ресурс і тим самим зменшити собівартість послуг;

- застосування специфікації IEEE 802.11n дозволяє збільшити швидкість передачі даних до 300 Мбіт/с і поліпшити радіопокриття за рахунок функції агрегування кадрів, об'єднання каналів і просторового мультиплексування;

- користувачі Wi-Fi після авторизації та аутентифікації в найближчій точці доступу зберігають такі ж права і в інших точках доступу, що дозволяє

уникнути переривання обслуговування при повторній перевірці автентичності під час процедури переходу між точками доступу;

- забезпечення високої якості сервісів за рахунок підтримки функцій пріоритетності мультимедійного трафіку (VoIP, потокове відео);

- одночасна підтримка кожною точкою доступу Wi-Fi від 4-8 дискретних SSID дає можливість операторам надавати різні рівні безпеки і якості обслуговування для кожного хот-стопуі мережі і на цій основі диференціювати послуги для різних категорій абонентів;

- підтримка стандарту аутентифікації 802.11x через RADIUS-сервер дозволяє операторам реалізувати функції авторизації, аутентифікації та обліку для управління доступом користувача;

- підтримка протоколів автоматичного формування мікростільникової структури Wi-Fi мережі і уникнути необхідності використання кабельної Ethernet-мережі в складних сценаріях розгортання;

- підтримка додаткових функцій (автоматичний вибір каналу, інтелектуальний автоматичний вибір частоти DFS, управління потужністю передавача TPC), які дозволяють домогтися оптимального покриття мережі з мінімальним рівнем перешкод.

### 1.3 Аналіз проблем інформаційної безпеки бездротових мереж зв'язку

Бездротова локальна мережа (Wireless Local Area Network, WLAN) являє собою групу бездротових мережевих вузлів, розташованих на невеликій відстані один від одного, яка здійснює обмін даними через радіоефір. Бездротові локальні мережі мають досить обмежений діапазон дії і застосовуються, наприклад, в офісних будівлях, аеропортах, кафе і т.д., де вони реалізовані у вигляді розширень для існуючої дротової локальної мережі з метою забезпечення мобільності користувачів. Надалі при згадці терміна «бездротова мережа» мова йтиме про локальних бездротових мережах, побудованих за технологією Wi-Fi.

В даний час бездротові мережі завоювали величезну популярність. Повсюдне поширення даних мереж обумовлено незаперечними перевагами перед традиційними кабельними мережами:

- доступність і простота розгортання мережі;
- мобільність користувачів в зоні дії мережі;
- просте підключення до мережі нових користувачів;
- широке поширення мобільних пристроїв.

Згідно з прогнозом компанії Cisco Systems, до 2020 р. половина всього трафіку, що генерується в корпоративних інформаційних мережах буде доводитися на бездротові пристрої. Це обумовлено, в тому числі і ростом пропускної здатності бездротових мереж, представлених на рис. 1.3. У червні 2013 був ратифікований стандарт 802.11ac [79], що забезпечує в перспективі швидкість передачі до 6,9 Гбіт/с з завдяки використанню нових принципів модуляції, підтримки до восьми просторових потоків передачі даних і смуги шириною до 160 МГц [1].

Провідні виробники мережевого обладнання вже почали випуск пристроїв, що підтримують цей стандарт.

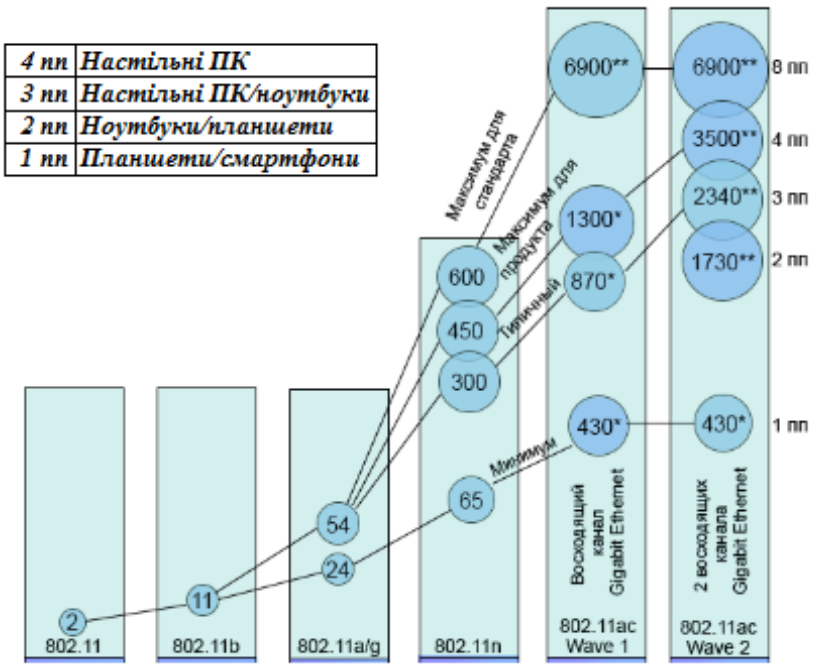


Рис.1.3. Зростання швидкості передачі даних з розвитком стандартів 802.11 (швидкості вказані в Мбіт с; пп - просторовий потік)

З іншого боку, невисокий рівень безпеки таких мереж часто обмежує їх застосування. Мережеві кабелі входять до складу структурованої кабельної системи організації і зазвичай прокладені в спеціальних кабель-каналах, в стінах будівлі або під стелею, що ускладнює фізичне підключення зловмисника до мережі. У разі бездротових мереж сигнал поширюється всеспрямовано, тому зловмисник може бути розташований в будь-якій точці зони дії мережі. Крім того, за рівнем потужності та напрямку поширення сигналу можна вирахувати місцезнаходження його джерела.

У стандарті 802.11 [2], що є основоположним для бездротових локальних мереж, визначені два способи організації бездротової мережі: інфраструктурний та спеціальний робочий (Ad-Hoc). В тимчасової мережі всі клієнти є рівноправними членами мережі. В інфраструктурному режимі функції координації передачі даних виконує точка доступу (Access Point, AP). Всі підключені бездротові клієнти взаємодіють через неї [3], при цьому для кожної бездротової мережі призначається свій ідентифікатор набору послуг (Service Set Identifier, SSID).

Широке поширення Wi-Fi мереж призвело до спроби зробити налаштування бездротової мережі простіше для людей, що не володіють навичками комп'ютерної грамотності. Результатом стала технологія Wi-Fi Protected Setup (WPS). WPS автоматично призначає ім'я мережі і включає шифрування для захисту бездротової мережі від несанкціонованого доступу, при цьому немає необхідності вручну налаштувати кожен параметр. WPS реалізується на більшості вироблених в даний час бездротових точках доступу, включаючи Cisco, Linksys, Zyxel, D-Link і Netgear. Крім того, на багатьох пристроях дана функція включена за замовчуванням.

Однак реалізація ідеї використання WPS має недолік, який дозволяє зловмисникові виконати атаку шолом підбору PIN-коду, за яким відбувається аутентифікація користувача. Хоча довжина PIN-коду становить S цифр, він розділений на дві половини, причому остання цифра є контрольною сумою

коду. Це зменшує максимально можливу кількість спроб аутентифікації, необхідних для вгадування PIN-коду, з $10^8$ (100 000 000) до $10^4 + 10^5$ (11000). Відновлення PIN-коду дає атакуючому повний доступ до мережі, причому якщо точка доступу віщає в двох діапазонах частот одночасно (2,4 ГГц і 5 ГГц), то так як радіомодулі використовують один і той же WPS PIN-код, знання його дозволяє відновити всі ключі WPA.

З вищесказаного можна зробити висновок, що налаштування параметрів бездротового підключення повинна проводитися вручну грамотним фахівцем і відповідно до інструкцій і рекомендацій виробників обладнання.

Таким чином, питання захищеності бездротових локальних мереж на даний момент залишаються відкритими.

Основні проблеми захисту інформації в бездротових мережах полягають при в наступному:

- поширення сигналу за межі контрольованої зони;

- легкий доступ зловмисника до бездротового каналу передачі в порівнянні з кабельними мережами;

- використання вразливих протоколів і методів аутентифікації;

- відсутність повноцінного захисту від атак при випуску доповнень до стандартів;

- можливі помилки в налаштуванні різних компонентів бездротової мережі.

### 1.4 Огляд підходів до вирішення проблем інформаційної безпеки

Для організації безпечного функціонування безпроводової корпоративної мережі необхідно побудувати систему багаторівневої захисту. Дана система включає в себе наступні рубежі (заходи):

- захист параметра бездротової мережі: точок доступу і пристрою користувача;

- забезпечення безпеки сеансів зв'язку: застосування надійних методів аутентифікації, стійких алгоритмів шифрування т.д.

- постійний моніторинг радіоефіру, включаючи фізичний рівень, виявлення і аналіз підозрілої активності.

Для вирішення зазначених вище проблем забезпечення безпеки інформації в бездротових мережах використовуються як технічні засоби захисту, так і організаційні заходи. Технічні засоби захисту по об'єкту застосування можна розділити на три основні групи табл.1.1:

- засоби захисту бездротової мережі в цілому;
- засоби захисту точці бездротового доступу;
- кошти захисту стороні користувача (клієнта).

Тонка і грамотне налаштування пристроїв, застосування останніх найбільш захищених протоколів дозволяє знизити ймовірність реалізації загроз. Однак і вони  мають свої недоліки, наприклад, відсутність в технології WPA2аутентіфікації запитів на дисоціацію і деаутентіфікацію, в результаті чого з'являється можливість реалізації атаки роз'єднання абонентів та подальшого впровадження помилкового об'єкта мережі. Контрольні та керуючі кадри передаються у відкритому вигляді, що дозволяє прослухати їх заголовки і виконати підміну MAC-адреси.

Протокол 802.11w, покликаний захиститу керуючі кадри, забезпечує їх шифрування тільки після обміну ключами і не поширюється на контрольну інформацію. Застосування віртуальних приватних мереж (VPN) з набором протоколів IPsec забезпечує необхідний рівень безпеки, однак вимагає трудомісткою настройки апаратних засобів і програмних клієнтів. В зв'язку з вищесказаним, багато дослідників ведуть пошук можливих удосконалень поточних протоколів сімейства 802.11.

Таблиця 1.1

Методи і засоби захисту інформації в бездротових мережах

| Засоби захисту мережі | Засоби захисту точки доступу | Засоби захисту користувача |
|---|---|---|
| Міжмережеві екрани | Зміна на пристрої установок за замовчуванням | Персональні міжмережеві екрани |
| Проксі сервери | закриття невикори-стовуванихпортів | Засоби антивірусного контролю |
| бездротові системи виявлення атак | заборона настройки параметрів через бездротове з'єднання | Перевірка сертифіката сервера 802.1x |
| Списки контролю доступу по MAC-адресами | Захищені протоколи віддаленого управління | Підтримка стандарту 802.11w |
| Контроль доступу до мережі (port security) і аутенти-фікація 802.1X | Підтримка стандарту 802.11w або протоколу MFP | Останні оновлення безпеки, драйверів бездротового модуля |
| | Функція переходу в режим Multi - BSSID (Virtual AP) і PSPF | |
| Організація демілітаризованої зони | Відключення розсилки імені бездротової мережі Service Set Identifier (SSID) | |
| Сканери мережевих вразливостей | Відключення технології спрощеної налаштування бездротової мережі Wi -Fi Protected Setup (WPS) | |

В роботі розглянуто недоліки протоколів 802.11 і методів побудови захисту бездротової мережі. В якості вирішення проблеми вразливості стандартних протоколів пропонується шифрувати весь блок даних протоколу MAC (MPDU), включаючи MAC-заголовки, крім послідовності перевірки кадру FCS. Однак це стане причиною значних затримок в передачі даних і низької пропускної здатності каналу.

В автори пропонують другий спосіб захисту від атак. При встановленні з'єднання між клієнтом і точкою доступу в запит асоціації поміщається

розрахований за алгоритмом SHA-512 хеш нікого випадкового набору символів, відомого тільки даного клієнта, який зберігається на точці доступу. У разі появи запиту на закриття з'єднання одержувач звіряє хеш вкладеного в запит значення з раніше збереженим і, в разі збігу, обробляє запит, інакше запит ігнорується. Варто зазначити, що даний спосіб дозволяє захиститися тільки від DoS-атак, які виконуються через підроблені запити на дисоціацію і деаутентіфікацію.

В роботі автор пропонує методику захисту інформації в бездротових мережах на основі динамічної маршрутизації трафіку. Однак розроблений автором алгоритм визначення довіреної маршруту передачі даних в більшій мірі спрямований на вирішення завдання забезпечення доступності середовища передачі і не дозволяє гарантувати конфіденційність і цілісність трансльованих даних. Д. Райт в статтях зазначає особливості мережевого трафіку, що генерується утилітами для активного пошуку бездротових мереж, ін'єкції кадрів в ефір і створення помилкових точок доступа. Автор виявляє шкідливий трафік в ході аналізу значень поля «номер послідовності» (Sequence Number) в заголовку кадру, тега «унікальний ідентифікатор організації» (Organizationally Unique Identifier, OUI) і тега SSID. Дані ознаки також використані в дипломній роботі. Порада по стандартам безпеки індустрії платіжних карт (Payment CardIndustry Security Standards Council, PCISSC), заснований провідними міжнародними платіжними системами, розробив стандарт безпеки даних індустрії платіжних карт (Payment CardIndustry Data Security Standard, PCIDSS), який містить требованіяк забезпечення безпеки даних про власників карток, відповідно до яких повинна будуватися і функціонувати інфраструктура корпоративних інформаційних мереж. Базова мережева безпека PCI DSS 3.0 вимагає установки брандмауера між дротової і бездротової мережами і наявності на ньому правил для обмеження доступу між бездротовими мережами і заданими серверами (службами), а також регулярне сканування корпоративної мережі з метою ідентифікації бездротових пристроїв, пошуку неавторизованих або небажаних точок доступу.

Додатковими вимогами є:

1. Забезпечення фізичного захисту бездротових пристроїв.

2. Розгортання бездротової системи запобігання вторженій.

3.Ізмененіе паролів і налаштувань за замовчуванням на всіх пристроях бездротової мережі і захищена налаштування безпроводових пристроїв.

4. Протоколи надання бездротового доступа.

5. Застосування методів суворої аутентифікації, стійких до злому алгоритмів шифрування і захищених протоколів безпеки: для переданих через мережу компанії даних повинен застосовуватися протокол WPA2 з використанням AES-алгоритму з 128-бітовим ключом.6. Розробка і застосування політики безпеки бездротових мереж, що визначає правила використання мережі співробітниками, гостями та контрагентами.

### 1.5 Методи і алгоритми виявлення мережевих атак

Основу функціонування бездротової системи виявлення атак становить класифікує модель, на базі якої приймається рішення про віднесення фрагмента мережевого трафіку до нормальної мережевої активності або до будь-якого типу атаки. Формально завдання класифікації мережевого трафіка можливо представити таким чином. Нехай *X*-безліч вхідних образів (записів мережевої активності) xi, Y-безліч виходів (міток класів) $y_i$. Передбачається, що існує відображення F: X → Y, значення якої відомі на записах кінцевої навчальної вибірки $X^m = \{(x_1, y_1), ..., (x_m, y_m)\}$. Потрібно побудувати алгоритм A: X → Y, здатний класифікувати довільну запис мережевої активності $x_i \in X$ рис.1.6,*а*.

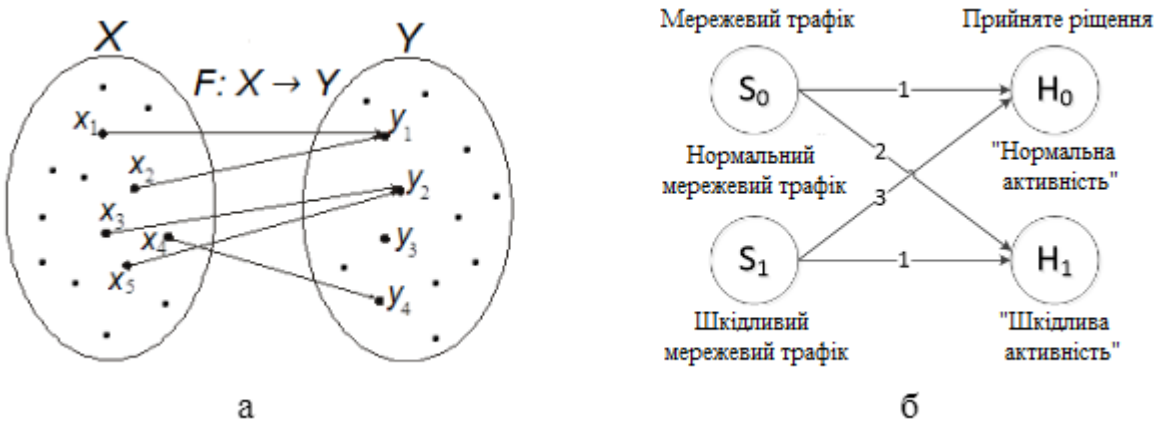


Рис. 1.6. Графічне представлення задачі класифікації і мережевого трафіку (а) і можливих результатів процесу класифікації (б)

У загальному випадку можливі три результати процесу класифікації записів мережевої активності рис.1.6,*б*:

1.Правільное рішення: S0 → H0 або S1 → H1.Соответственно, ймовірність правильної класифікації записів визначається як:

$$P_{прав} = P\{H_0 \mid S_0 \vee H_1 \mid S_1\} = P\{H_0 \mid S_0 + H_1 \mid S_1\} \quad (1.1)$$

2. Помилка першого роду: $S_0 \rightarrow H_1$. Імовірність помилок першого роду:

$$P_1 = P\{H_1 \mid S_0\} \quad (1.2)$$

3. Помилка другого роду: $S_1 \rightarrow H_0$. Імовірність помилок другого роду

$$P_2 = P\{H_0 \mid S_1\} \quad (1.3)$$

Потрібно побудувати таку класифікуючу модель, яка дозволила б мінімізувати сумарну ймовірність виникнення помилок $P_{ош} = P_1 + P_2$ (на практиці потрібно забезпечити значення $P_{ош} = 3 \div 5\%$). Для виявлення найбільш ефективного методу побудови класифікованої моделі стосовно до бездротової системі виявлення атак в даній роботі проведено порівняння наступних методів ІАД: методу опорних векторів, метода k-найближчих сусідів, дерев прийняття рішень, а також нейронних мереж.

*Метод опорних векторів* (Support Vector Machine, SVM) є відносно новим алгоритмом в співтоваристві машинного навчання. За час свого існування він показав як переваги по відношенню до раніше запропонованих методів, так і

деякі недоліки, які ти не менше, можуть бути подолані за рахунок більшої обчислювальної потужності комп'ютерного обладнання. Основу методу опорних векторів становить алгоритм класифікації, запропонований Вапніка на підставі теорії Вапніка-Червоненкіса. Головна ідея методу опорних векторів полягає в перекладі вихідних векторів в простір більш високої розмірності і пошук розділяє гіперплощини з максимальним зазором між кластерами в цьому просторі. По обидва боки гіперплощини, що розділяє різні класи, будуються дві паралельні гіперплощини рис.1.7. Розділяти гіперплощиною буде така гіперплощина, відстань від якої до двох паралельних гіперплощин максимальні. Даний алгоритм працює на припущенні, згідно з яким збільшення відстані між цими паралельними гіперплощинами призводить до зменшення середньої помилки класифікації.

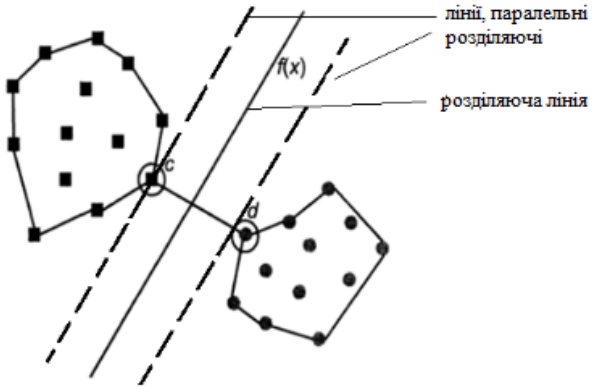


Рис.1.7. Графічна інтерпретація методу опорних векторів для двомірного простору ознак

У разі методу опорних векторів кожен об'єкт даних представлений у вигляді вектора (точки) в n-вимірному просторі (послідовність n чисел). Кожна така точка належить тільки одному з двох класів. Питання полягає в тому, чи можна розділити ці точки гіперплощиною з розмірністю (n-1). Це називається лінійним класифікатором. Таких гіперплощин, які класифікують дані, може бути безліч. Так як максимізація зазору між класами сприяє більш впевненою класифікації, вибирається така гіперплощина, відстань від якої до найближчої точки з навчального набору з кожного боку гіперплощини максимально. Якщо

дана гіперплощина існує, то вона є оптимальною розділяє гіперплощиною, а відповідний їй лінійний класифікатор оптимальний розділяє класифікатором. Найближче розташовані вектори різних класів називаються опорними векторами c і d на рис. 1.7. В якості переваг SVM можна відзначити здатність до узагальнення, високу точність і низьку обчислювальну складність прийняття рішення. Недоліком даного методу є відносно велика обчислювальна складність побудови класифікуючої моделі. Ідея застосування SVM при розробці мереж виявлення вторгнень (IDS) є відносно молодою. У роботах досліджується спосіб виявлення атак за допомогою особливого варіанту SVM - LMRL (Large Margin Rectangle Learning - навчання на основі прямокутних кластерів з максимальним зазором), в якому також використовується принцип максимізації зазору і, крім того, кожен клас представляється у вигляді набору прямокутних кластерів. Метод застосовувався для побудови класифікуючої моделі системи виявлення атак, що функціонує на основі технології сигнатурного аналізу, з даних навчальної вибірки. Модель випробувана на атаках типу переповнення буфера, руткіт і SYN-FLOOD і показала актуальність застосування методу опорних векторів в якості основи системи виявлення атак.

*Метод k-найближчих сусідів* (k-nearest neighbors, k-NN) -метод класифікації, принцип роботи якого полягає в присвоєння об'єкту класу, найбільш поширеного серед сусідів даного об'єкта. Формування сусідів відбувається з безлічі об'єктів з вже відомими класами, і, виходячи з заданого значення k ($k \geq 1$), визначається, який з класів найбільш численний серед них. У разі якщо k = 1, то об'єкт просто відноситься до класу єдиного найближчого сусіда. Метод k-NN є одним з найбільш простих методів ІАД. Результати застосування методу легко піддаються інтерпритації. Недоліком методу є його чутливість до локальної структури даних.

Дерева прийняття рішення являють собою деревоподібну структуру з «листя» і «гілок». На ребрах («гілках») дерева прийняття рішень записані атрибути, від яких залежить цільова функція, в «листі» записані значення цільової функції, а в інших вузлах - атрибути, за якими розрізняються об'єкти.

Для класифікації нового об'єкта необхідно спуститися по дереву від кореня до листа і отримати відповідний клас. Таким чином, шлях від кореня до листа виступає правилами класифікації на основі значень атрибутів об'єкта. Перевагами дерев прийняття рішень є простий принцип їх побудови і хороша інтерпретація результатів, недоліком-невисока точність класифікації. Перераховані вище методи інтелектуального аналізу даних часто використовуються дослідниками як класифікаторів записів про мережеву активність (сигнатур). Наприклад, в роботі ця задача вирішується за допомогою застосування методу опорних векторів і нейронних мереж. Як зразки атак використовується база сігнатур KDD-99 агентства DARPA.

У статті представлений варіант комбінації методу опорних векторів і дерев прийняття рішень для забезпечення мультикласового розпізнавання атак. З цією метою будується бінарне дерево рішень, що складається з SVM, які на першому етапі поділяють дані на два класи: «атака» і «не атака». На наступних етапах процедура повторюється для чотирьох категорій атак, представлених в базі KDD-99: відмова в обслуговуванні (DoS), несанкціоноване отримання прав користувача (R2L), несанкціоноване підвищення прав користувача до супер користувача (U2R), зондування (Probe). Для вирішення практичних завдань, зв`язаних с розпізнаванням і класифікацією атак, активно застосовуються і нейронні мережі. Нейронна мережа складається з взаємозв'язаних нейронів, що утворюють вхідний, проміжні (Приховані) і вихідний шари. Навчання мережі відбувається шляхом коригування значень ваг нейронів для мінімізації помилки класифікації. Переваги нейронних мереж виражаються в їх здатності автоматично здобувати знання в ході навчання, а також здатності до узагальнення, основний недолік полягає в чутливості до шуму у вхідних даних.

Розглянуто підхід к організації нейромережевої системи виявлення атак на базі двошарового персептрона та мережі Кохонена. Для підвищення швидкості обробки мережевого трафіку застосовується стиснення простору ознак за допомогою методу головних компонент і рециркуляціонної нейронної мережі. Запропоноване рішення реалізовано у вигляді модуля для IDS Snort. В

даний час в області нейронних мереж бурхливо розвивається напрямок DeepLearning ( «глибоке навчання»), що представляє собою третє покоління нейронних мереж .В цю категорію входять багатошарові нейронні мережі, навчання яких проводиться не на цілих об'єктах, а на їх складові частини з поступовим збільшенням їх розміру. Прикладом є глибокі мережі довіри (Deep Belief Networks, DBN). В основі їх лежить RBM-мережу (Restricted Boltzmann Machine) – стохастична нейронна мережа, що складається з одного баченого і одного прихованого шарів, представлена на рис. 1.8.

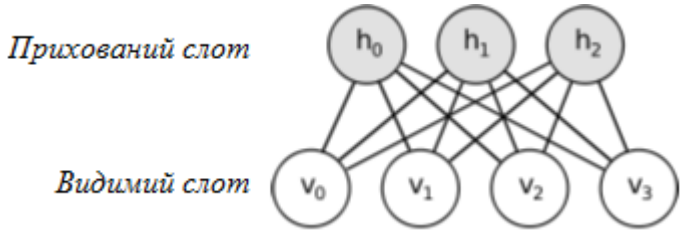


Рис. 1.8. Структура RBM-мережі

Головною особливістю мереж глибокого навчання є процес навчання мережі, що проводиться пошарово без вчителя. Прихований шар кожної RBM-підмережі виступає як видимий для наступної підмережі рис.1.9. Після закінчення навчання можлива точна доналаштування DBN-мережі з учителем для функціонування в якості класифікатора.

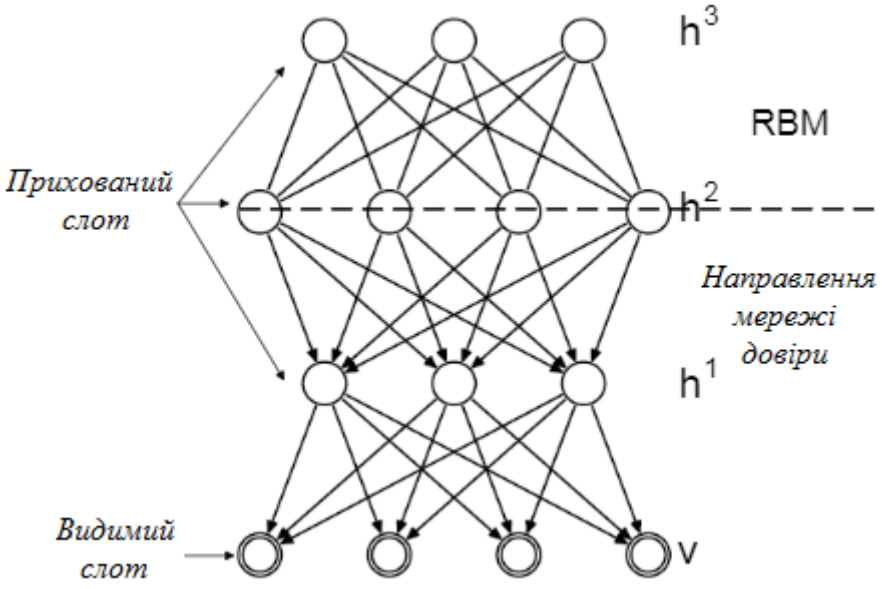


Рис. 1.9. Структура DBN-мережі

Переваги мереж глибокого навчання: скорочення розмірності вектора даних (кількості ознак), що збільшує продуктивність при класифікації, і високий точність в задачах розпізнавання складних об'єктів (зображень, мови) .В розглянутих роботах пропонується гібридна схема, яка об'єднує гідності глибоких мереж довіри і методу опорних векторів. Як зразки атак обрана база сигнатур NSLKDD-2009, що представляє собою вдосконалений варіант бази даних KDD-99. На першому етапі використовується DBN-мережу для зменшення розмірності набору вхідних ознак, далі за допомогою SVM проводиться класифікація за чотирма категоріями мережевих атак і нормальної мережевої активності. Варто зазначити, що наведені вище дослідження українських і зарубіжних авторів відносяться до виявлення вторгнень в традиційні дротяні мережі. Однак роботи, присвячені безпосередньо застосуванню методів інтелектуального аналізу даних для рішення задачі виявлення атак, властивих локальним бездротових мереж, відсутні в доступній літературі. Розглянуті основні типи атак, характерні для локальних бездротових мереж, деякі способи захисту від них, включно із застосуванням методів інтелектуального аналізу даних в якості основи для виявлення даних атак. В якості методів ІАД розглянуті метод опорних векторів, метод k-найближчих сусідів, нейронні мережі і дерева прийняття рішень.

### 1.6 Комерційні засоби захисту від мережевих атак

Існуючі системи виявлення вторгнень в бездротових мережах орієнтовані на аналіз протоколів бездротового зв'язку сімейства IEEE 802.11, ідентифікацію та аналіз підозрілої активності. Крім того, деякі виробники забезпечують можливість запобігання вторгнень в корпоративну мережу. В цьому випадку бездротові системи здатні здійснювати дії двох типів при виявленні атаки: бездротове вплив -З'єднання між користувачем і точкою доступу обривається за допомогою відправки повідомлення про дисоціації (роз'єднання), після чого точка доступу відмовляє у відновленні з'єднання; мережеве вплив-система

передає комутатора команду блокувати з'єднання з даним користувачем мережі по порту або MAC-адресу. Крім того, деякі системи можуть визначити фізичне розташування джерела виявленої загрози за допомогою методу тріангуляції.

У цьому підрозділі наведено опис і порівняння чотирьох комерційних систем виявлення вторгнень в бездротові мережі.

Основною перевагою системи WIPS компанії Air Tight Networks є можливість її розгортання над існуючою мережевою інфраструктурою організації, тобто відсутня залежність від того, наскільки однорідна мережа організації. Рішення інтегрується з продукцією різних виробників мережевого устаткування. Також до переваг рішення варто віднести низьку вартість володіння і простоту настройки. Основні характеристики системи:

- автоматичне виявлення і блокування різних видів бездротових загроз, в тому числі несанкціонованих точок доступу і пасток, DoS-атак, Ad-Hoc мереж і ін.;

- цілодобовий моніторинг продуктивності мережі;

- можливість функціонування сенсорів в режимі офлайн;

- виявлення радіочастотного зашумлення і перешкод;

- розслідування бездротових інцидентів по журналам реєстрації;

- обчислення розташування бездротового пристрою або джерела перешкод;

- розслідування бездротових інцидентів по журналам реєстрації;

- обчислення розташування бездротового пристрою або джерела перешкод; захист мобільних пристроїв;

- інтеграція з платформами ArcSight, CheckPoint, McAfee ePO і Qualys, підтримка SNMP і Syslog;

- звіти про відповідність стандартам PCI DSS, SOX, HIPAA, GLBA, DoD Directive 8100.2;

- управління через фізичне підключення, віртуальний сервер або хмара.

В якості сенсорів використовуються власні пристрої AirTightC-75, C-60, C-55, C-50 з підтримкою одного або двох радіоканалів і режимами роботи в

ролі точки доступу або виділеного активного сенсора. Найбільш функціональні моделі мають підтримку стандарту 802.11ac і можливість підключення зовнішніх антен. Ще однією популярною реалізацією WIDS для платформи Windows є AirMagnet Enterprise компанії Fluke Networks. Система дозволяє вирішувати наступні завдання:

- визначення несанкціонованих точок доступу і клієнтів;

- контроль політики безпеки використання бездротових мереж;

- виявлення атак в бездротової мережі і протидію їм;

- локалізація зловмисника методом тріангуляції. Основні характеристики Air Magnet Enterprise:

- підтримка стандарту 802.11ac;

- сигнатурний метод виявлення вторгнень для захисту більш ніж від 230 загроз;

-наявність аналізатора радіочастот, що дозволяє виявляти перекриття каналів 802.11 і виявляти радіоперешкоди;

-звіті про відповідність стандартам HIPAA, PCI DSS, GLBA, DoD, ISO 27001, BASEL 2 і CAD3;

- запобігання виявлених атаккак за допомогою бездротового впливу, так і в кабельній мережі. Система складається з сенсорів, сервера і консолі управління, взаємодія яких зображено на рис. 1.10.

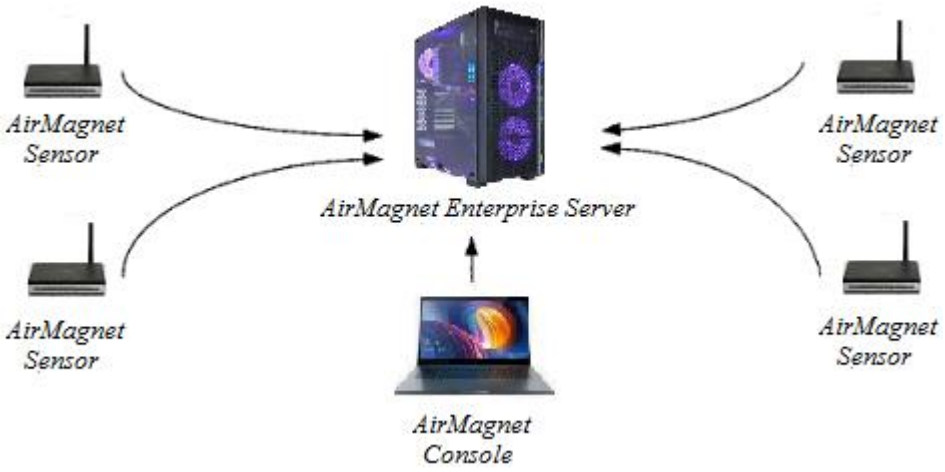


Рис.1.10. Компоненти системи Air Magnet Enterprise

Функція тріангуляції дозволяє визначити місцезнаходження бездротового пристрою порушника. Для цього необхідно імпортувати в систему план поверху і вказати розміщення сенсорів і точок доступу на плані. Приблизне розташування пристрою забезпечується в разі виявлення його як мінімум трьома сенсорами, при цьому великий обсяг генерованої ним трафіку сприяє підвищенню точності визначення місця розташування. Крім того, функція тріангуляції дозволяє заборонити з'єднання з корпоративною мережею, ініційовані з-за меж кордонів захищається периметра організації. Система дозволяє виявити такі бездротові загрози:

- застосування утиліт злому NetStumbler, ASLEAP, Wellenreiter;

- ARP Request Replay-атаки з повтором перехопленого зашифрованого пакета для прискорення розкриття шифрування;

- атаки по словнику на протокол EAP (велика кількість невдалих спроб встановити сесію);

- помилкові точки доступу, створені за допомогою утиліт Airsnarf, FakeAP, Hotspotter, SoftAP, HostAP і маскуються під корпоративні;

- підміна MAC-адреси з метою обходу фільтрів на основі MAC-адрес;

- спотворені кадри стандарту 802.11;

- пряма передача пакетів між клієнтами, що є порушенням політики Publicly Secure Packet Forwarding (PSPF);

- атака «людина посередині»;

- помилковий Dynamic Host Configuration Protocol (DHCP) сервер;

- зондування - спроба встановлення з'єднання з будь-якою точкою доступу (Probing). Перевагою системи є широкий набір ідентифікованих атак на канальний рівень бездротової мережі з їх докладним описом, гнучка система побудови звітів відповідність регулюючим стандартам.

Як істотного недоліку системи можна виділити складність конфігурації, так як настройки за замовчуванням дозволяють використовувати тільки функціонал запобігання вторгнень. Для виявлення підроблених мереж і нелегальних точок доступу дана система вимагає значних налаштувань. Третє

розглянутої WIDS є рішення Air Defense Enterprise компанії Motorola. Дана система дозволяє вирішувати наступні завдання:

- безперервний моніторинг бездротового трафіку 802.11 a / b / g / n і виявлення неавторизованих пристроїв;

- автоматизований захист мережі від несанкціонованого доступу по бездротових каналах;

- моніторинг у відповідності заданої політиці безпеки (конфігурації), моніторинг/діагностика бездротової інфраструктури;

- надання інструментарію для розслідування інцидентів безпеки і віддаленого аналізу мережевих проблем;

- координати обчислюються випромінювального пристрою;

- візуалізація покриття мережі в реальному часі;

- аналіз частотного спектра та ін.

Система складається з наступних компонент рис.1.11:

- центральний сервер у вигляді програмно-апаратного комплексу;

- розподілені сенсори, які збирають інформацію і передають її на сервер;

- консоль адміністратора з веб-інтерфейсом на мові Java;

- програмні модулі розширення.

У ролі сенсорів виступають бездротові точки і порти доступу Motorola AP300, AP-5131, AP-7131. При цьому точки, оснащені двома радіомодулями, здатні паралельно виконувати функції цілодобового моніторингу та надавати бездротовий доступ.

# 2. Дослідження побудови моделей процесу функціонування систем виявлення атак в без проводових мережах WI-FI

## 2.1 Дослідження побудови моделі загроз безпеки в безпровідній мереже зв’язку

На підставі розглянутих у першому розділі проблем захисту інформації в бездротових мережах можна визначити перелік можливих загроз інформаційній системі організації.

Загроза (безпеки інформації) - сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації. За видами можливих джерел загроз виділяють два класи загроз:

- загрози, пов'язані з навмисними або ненавмисними діями осіб, що мають доступ до інформаційної системи (внутрішній порушник);

- загрози, пов'язані з навмисними або ненавмисними діями осіб, які не мають доступу до інформаційної системи, що реалізують загрози з зовнішніх мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну (зовнішній порушник).

Види порушників, характерних для ІС з заданими характеристиками і особливостями функціонування, виділяються на основі припущень про можливі цілі (мотивації) при реалізації загроз безпеці інформації цими порушниками. Цілями реалізації порушниками загроз безпеки інформації в ІС можуть виступати:

а) нанесення збитків державі, окремим його сферам діяльності або секторам економіки;

б) ідеологічні або політичні мотиви;

в) організація терористичного акту;

г) заподіяння майнової шкоди шляхом обману, зловживання довірою, шахрайства або іншим злочинним шляхом;

д) дискредитація або дестабілізація діяльності органів державної влади, організацій;

е) отримання конкурентних переваг;

ж) впровадження додаткових функціональних можливостей в ПО або програмно-технічні засоби на етапі розробки;

з) цікавість або бажання самореалізації;

і) виявлення вразливостей з метою їх подальшого продажу і отримання фінансової вигоди;

к) реалізація загроз безпеці інформації з помсти;

л) реалізація загроз безпеці інформації ненавмисно через необережність або некваліфікованих дій.

Атаки за своїм походженням можуть бути пасивними і активними. Пасивна атака полягає в перехопленні трафіку за допомогою мережевих аналізаторів і його подальшому аналізі зловмисником. Як правило, дана атака здійснюється для збору необхідної інформації про бездротової мережі перед проведенням активних дій. В ході активної атаки зловмисник здійснює передачу даних в бездротову середу.

Атаки можуть бути реалізовані на різних рівнях моделі OSI: прикладному, транспортному, мережевому, канальному і фізичному [8]. Специфічними для бездротових мереж є фізичний і канальний рівні, на використанні яких заснований стандарт IEEE 802.11. Саме використання вразливостей протоколів і технологій цих рівнів є основою проведення атак на бездротову мережу і початкової стадією атак на ІС через несанкціоноване отримання доступу до бездротової мережі.

На рис. 2.1 наведено класифікацію атак на локальні бездротові мережі за кількома ознаками.

Таким чином, в даному підрозділі розглянуті основні загрози, до яких схильні бездротові локальні мережі, і їх джерела, наведені класифікація поширених типів атак і сценарії їх здійснення, представлені у вигляді дерев атак.

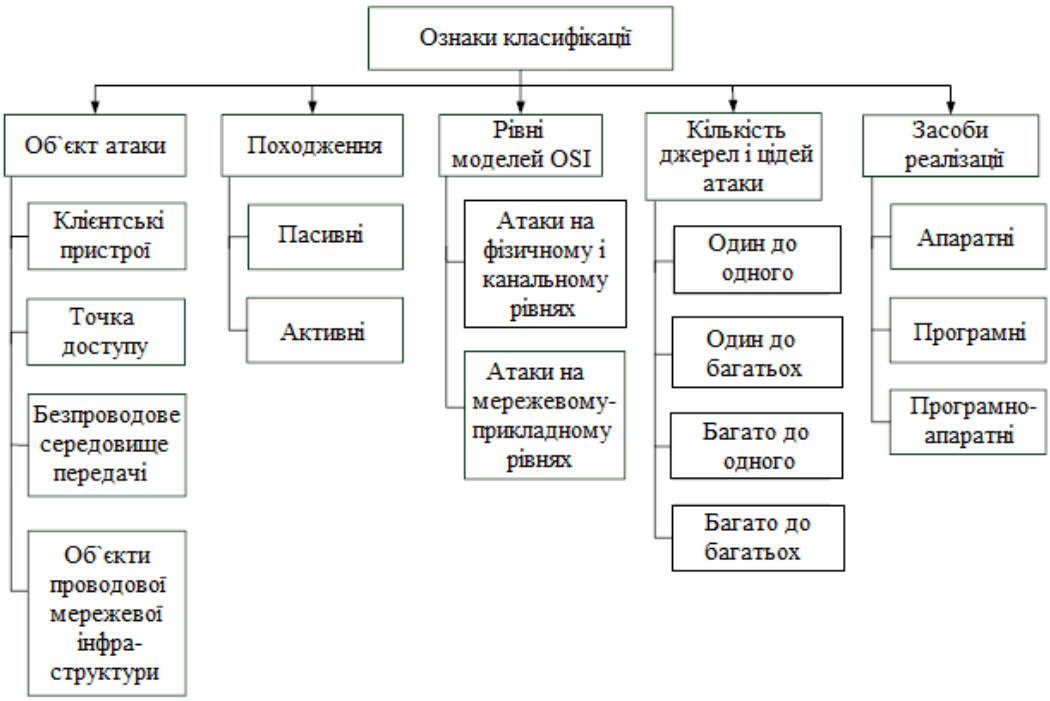


Рис.2.1. Класифікація атак на локальні бездротові мережі

Атаки фізичного і канального рівня, специфічні для бездротових мереж, представлені на рис. 2.2.

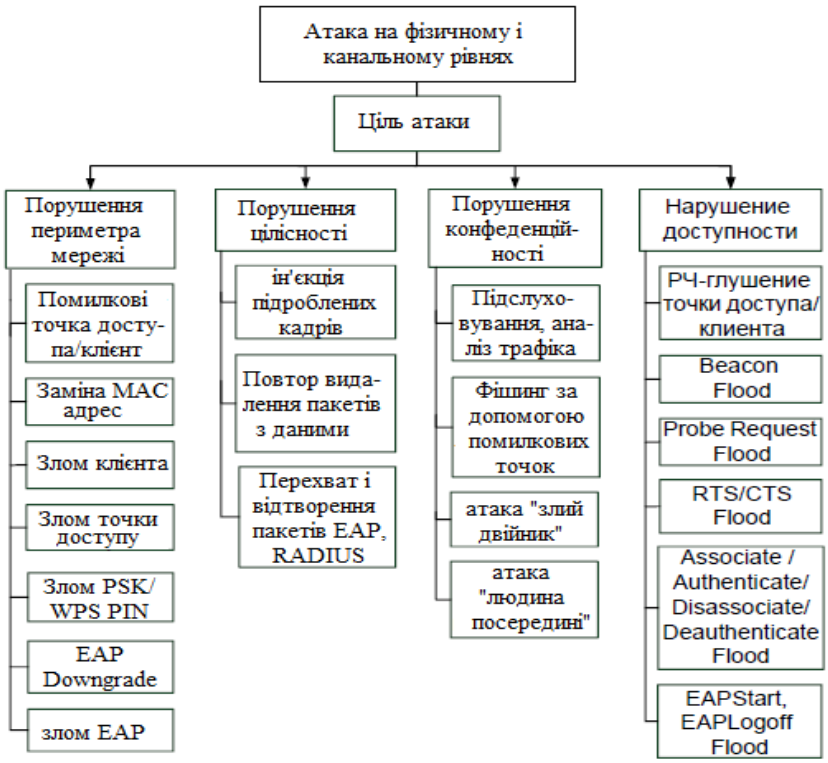


Рис.2.2. Класифікація атак фізичного і канального рівня в залежності від мети

## 2.2 Схема проведення експерементів

Імітаційне моделювання здійснювалося з метою перевірки працездатності розглянутих моделей і алгоритмів виявлення атак в реальному бездротової локальної мережі. Процес моделювання зводився до генерації атак на мережу, представлених в попередньому розділі, і дослідженню здатності прототипу СВА їх виявити і виробити відповідні захисні заходи. Як об'єкт випробування при проведенні моделювання використовувався сегмент локальної бездротової мережі з технологією захисту доступу WPA 2-Enterprise, структура якого представлена на рис. 2.10. моделювання проводилося за допомогою розробленого дослідного прототипу СВА, детально описаного в третьому розділі.

Тестування СВА проводилося в дві стадії. В ході першої стадії здійснювався набір різних категорій атак на бездротову мережу одночасно з передачею даних легальними користувачами. Бездротовий трафік прослуховувався сенсорами СВА, які збирали кадри даних, створювали по ним моделі з'єднань між абонентами, формували опис подій з набором характерних ознак і передавали їх в модуль виявлення атак для аналізу.

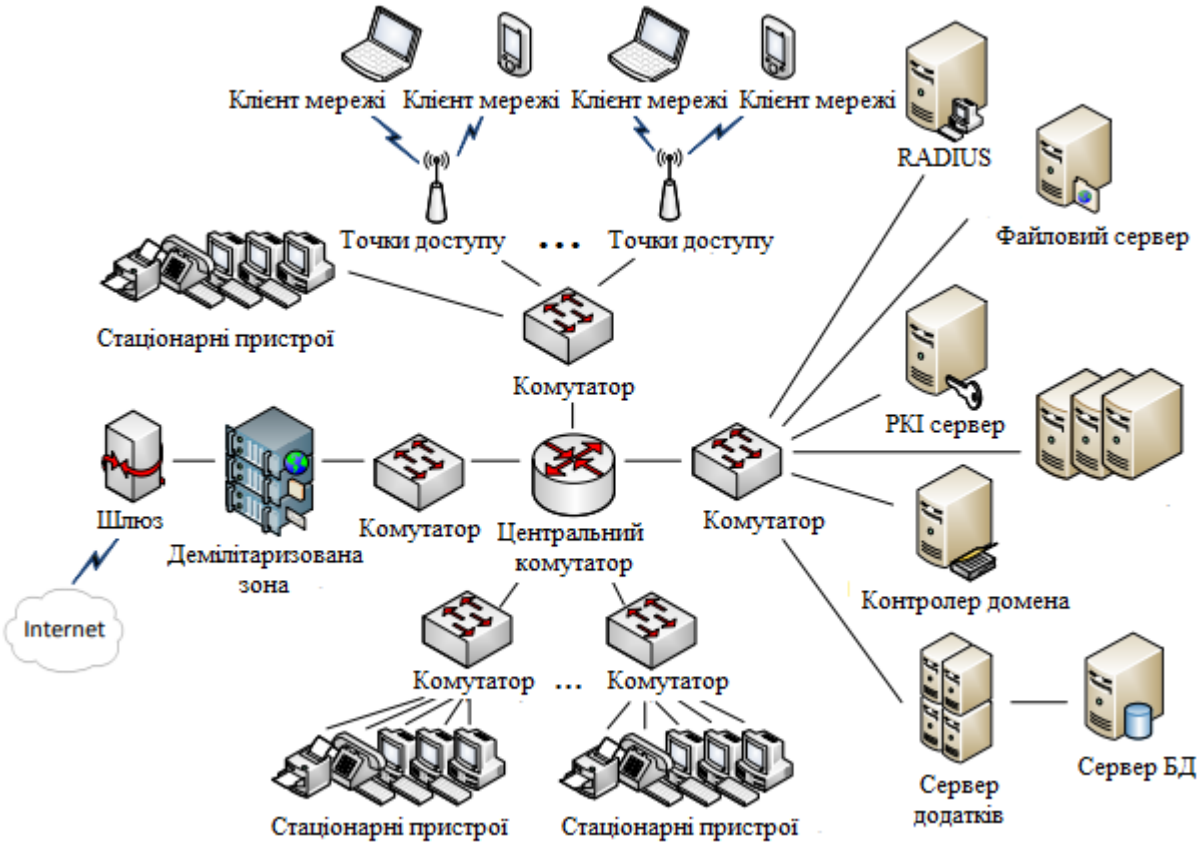


Рис. 2.10. Структура сегмента мережі

Друга стадія тестування полягала власне в перевірці здатності системи до виявлення атак. В ході неї на першому етапі проводилося навчання системи на навчальній вибірці з метою побудови класифікуючої моделі, що становить основу бази знань, різними методами ИАД. Потім на вхід модуля виявлення атак подавалися тестові дані, перехоплені сенсорами. Даний модуль проводив класифікацію подій безпеки на підставі класифікуючої моделі за критеріями, містяться в базі знань, і привласнював мітку класу мережевої активності.

На підставі збігу очікуваними і фактичними міток класів розраховувалася точність і повнота виявлення атак і обчислювалися величини помилок першого і другого роду.

Як і для будь-якого процесу класифікації, при вирішенні даного завдання можна виділити чотири категорії, на які поділяються класифіковані записи:

- істинно-позитивні (true positives, TP) - ті записи, класи яких ми очікували побачити і отримали на виході;

- помилково-позитивні (false positives, FP) - записи, класів яких бути на виході не повинно, але модуль їх помилково видав на виході;

- помилково-негативні (false negatives, FN) - записи, класи яких ми очікували побачити, але модуль їх не визначив;

- істинно-негативні (true negatives, TN) - записи, класів яких бути на виході не повинно і на виході модуля вони вірно відсутні.

Загальний відсоток коректно класифікованих атак A (accuracy) обчислюється як:

$$A = \frac{TP + TN}{N}, \tag{2.12}$$

де *TP* і *TN* - кількість справжніх записів;

*N* - загальна кількість класифікованих записів.

При цьому точність класифікації P (precision) розраховується за такою формулою:

$$P = \frac{TP}{TP + FP}, \tag{2.13}$$

де *TP* і *FP* - кількість відповідним чином класифікованих записів.

Метрика точності характеризує, скільки отриманих від модуля позитивних відповідей є правильними. Однак вона не дає уявлення про те, чи всі правильні відповіді повернув класифікатор. Для цього використовується метрика повноти R (recall), що розраховується за формулою:

$$R = \frac{TP}{TP + FN}, \tag{2.14}$$

де *TP* і *FN* - кількість відповідним чином класифікованих записів.

Для комбінування значень показників *P* і *R* використовують метрику $F_1$, що є середнім гармонійним значенням величин *P* і *R*:

$$F_1 = 2 \cdot \frac{P \cdot R}{P + R} \qquad (2.15)$$

Схема проведення експериментів по оцінці ефективності розроблених алгоритмів виявлення атак в бездротової мережі на основі технологій інтелектуального аналізу даних представлена на рис 2.11.

Експерименти проводилися в середовищі RapidMiner версії 5.3.015. На першому кроці навчання відбувалася обробка перехоплених даних, оскільки для коректної роботи алгоритмів кожен атрибут повинен бути представлений у вигляді чисельного значення в діапазоні від нуля до одиниці. Для цього виконувалося конвертувати текстові атрибутів в бінарні, а також нормалізація численних атрибутів щодо мінімального і максимального значень. Значення в відносних одиницях розраховується формулою:

$$K_i = \frac{a_i - a_{\min}}{a_{\max} - a_{\min}}, \qquad (2.16)$$

де $K_i$ - значення $i$-го атрибута в відносних одиницях;

$a_i$ - початкове значення;

$a_{min}$, $a_{max}$ - мінімальне і максимальне значення відповідно

Після цього дані навчальної вибірки надходили на вхід блоку побудови відповідної моделі. За допомогою розроблених у другому розділі алгоритмів формувалася класифікує модель і записувалася в базу знань СВА. Далі на її основі в модулі виявлення атак відбувалася класифікація записів тестової вибірки.

Обчислення проводилися на комп'ютерах з процесорами Intel Core i3 з частотою (1,9 - 2,4) ГГц і ОЗУ об'ємом 8 ГБ. Експерименти повторювалися з метою визначення найкращого набору параметрів функціонування кожного алгоритму виявлення атак, що забезпечують найвищу можливу для нього точність класифікації. Результати експериментів представлені в підрозділі 2.4.


Рис. 2.11. Схема проведення експерименту

# ВИСНОВКИ

Широке поширення бездротових локальних мереж і застосування їх в корпоративних інформаційних системах призводить до необхідності приділяти активну увагу вирішенню властивих їм проблем інформаційної безпеки. При цьому існуючі засоби захисту, в тому числі комерційні бездротові системи виявлення атак, не забезпечують повноцінного захисту від шкідливої мережевої активності. Тому у бакалаврській роботі було поставлено мету проаналізувати можливі рішення підвищення ефективності виявлення атак в локальних бездротових мережах Wi-Fi.

Проведено дослідження тенденцій розвитку локальних мереж на базі технології Wi-Fi, та оглянуто переваги і їх особливості.

Проведено аналіз існуючих методів і засобів захисту локальних бездротових мереж Wi-Fi, в тому числі комерційних систем виявлення атак, який виявив відсутність надання повноцінного захисту від шкідливої мережевої активності в таких типах мереж.

Проаналізовано алгоритми виявлення атак в бездротової мережі на основі застосування класифікуючої моделі з використанням методів інтелектуального аналізу даних, які на відміну від існуючих алгоритмів виявлення атак дозволяють підвищити точність виявлення атак.

Представлено архітектуру інтелектуальної системи виявлення бездротових атак, що функціонує на основі розглянутих алгоритмів виявлення атак, застосування яких дозволяє з більш високою точністю та дозволяє виявляти і блокувати атаки на бездротової компонент інформаційної системи.

У практичній частині дипломної роботи на базі програмного забезпечення виконано дослідження ефективність досліджуваної системи виявлення атак підтверджена методом імітаційного моделювання атак на сегмент локальної бездротової мережі організації з використанням реального мережевого трафіку, та розроблено рекомендації щодо її застосування.

## Перелік джерел посилання


1. https://itc.ua/articles/802-11ac-chto-neobhodimo-znat-o-novom-standarte-wi-fi/

2. https://ntools.com.ua/information/faq/standart-802-11-ac-chto-eto

3. Kent S., Seo K. Security Architecture for the Internet Protocol. BBN Technologies, December 2005. IETF Network Working Group, RFC 4301, Standards Track, Obsoletes RFC 2401.

4. IEEE 802.11-2012. IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards Association, 2012.

5. Memon A.Q., Raza A.H., Iqbal S. WLAN Security // Master's Thesis in Computer Network Engineering. School of Information Science, Computer and Electrical Engineering, Halmstad University, Sweden, 2010. – 66 p.

6. Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4 // Selected Areas in Cryptography, Lecture Notes in Computer Science, 2001. – Vol. 2259. – Pp. 1–24.

7. Chaabouni R. Break WEP faster with statistical analysis. Technical report, EPFL, LASEC, June 2006. – 55 p.

9. https://www.sciencedirect.com/science/article/abs/pii/S092054890500098X

10.https://www.speedguide.net/articles/how-to-stop-denial-of-service-dos-attacks-3316