**COMPUTER SYSTEMS AND NETWORKS**

**Vol. 6, No. 1, 2024**

DOI: https://doi.org/10.23939/csn2024.01.133

**УДК 004.75; 004.8**

# АНАЛІЗ БЕЗПЕКИ СУЧАСНИХ ПРОТОКОЛІВ ЗАХИСТУ МЕРЕЖ WI-FI: ОЦІНКА СТІЙКОСТІ ПРОТОКОЛУ WPA3 ПІД АТАКИ НА БАЗІ УТІЛІТИ DRAGONBLOOD

**О. О. Михайлова, А. В. Стефанків, Т. І. Наконечний**

Національний університет "Львівська політехніка",
кафедра захисту інформації
*E-mail: olha.o.mykhailova@lpnu.ua, artem.stefankiv.kb.2020@lpnu.ua, yurii.m.nakonechnyi@lpnu.ua*



**В умовах постійного розвитку інформаційних технологій та щораз більшої загрози кібератак безпека бездротових мереж Wi-Fi набуває особливої актуальності. Метою статті є глибокий аналіз сучасних протоколів захисту Wi-Fi, таких як WPA2, WPA3 та OWE, з акцентом на їхні сильні та слабкі сторони у контексті забезпечення безпеки мережі перед найбільш розповсюдженими типами атак.**

**У цій роботі детально розглянуто загрози безпеці бездротових мереж, зокрема атаки "людина посередині", фішинг Wi-Fi точок доступу та експлойти, спрямовані на конкретні механізми захисту. Важливою частиною дослідження є опис методик випробувань, використання інструментів для проведення атак, таких як Aircrack-ng та Wireshark, і детальний аналіз отриманих результатів.**

**Основна суть роботи полягає у детальному аналізі безпеки протоколу WPA3, застосовуючи утиліти Dragonblood для виявлення можливих вразливостей у його реалізації. Завдяки проведенню цілеспрямованих атак та симуляціям, що імітують реальні кібератаки, ця робота має на меті виявити потенційні шляхи несанкціонованого проникнення в захищені бездротові мережі, що використовують WPA3. Це дає можливість оцінити ефективність механізмів шифрування та аутентифікації, які використовуються у межах цього стандарту, і розробити рекомендації для підвищення рівня безпеки інформаційних систем. У процесі дослідження проведено практичні експерименти з модифікації коду сервера безпровідних точок доступу, а також проаналізовано дані, отримані за допомогою програми Wireshark для оцінки впливу атак на функціональність мережі. Результати роботи підкреслюють потребу постійного вдосконалення технологій захисту Wi-Fi для забезпечення надійної безпеки в умовах щораз більших кіберзагроз.**

**Ключові слова: бездротові мережі, протоколи захисту, Wi-Fi, WPA2, WPA3, методи захисту, безпека інформаційних систем, аналіз вразливостей, мережеві компоненти, шифрування даних, VPN.**

## Вступ

У світі, де цифрові технології проникають у кожен аспект нашого життя, бездротові мережі стали невід'ємною частиною повсякденності. Від моменту зародження Wi-Fi наприкінці XX століття і до сьогодні, коли ми стоїмо на порозі масового впровадження Wi-Fi 6, бездротові мережі

пройшли довгий шлях розвитку. Вони не лише забезпечують нам зручний доступ до інтернету в кафе, на роботі чи вдома, але й становлять складну інфраструктуру з великою кількістю вразливостей, які можуть бути використані зловмисниками.

Актуальність дослідження зумовлена стрімким розвитком бездротових технологій і появою нових вразливостей, які потребують глибокого аналізу та оцінки ефективності наявних протоколів захисту. Ми прагнемо визначити, які з цих протоколів найкраще здатні протистояти сучасним загрозам, забезпечуючи користувачам безпечний доступ до мережевих ресурсів.

У контексті безперервного розвитку цифрових технологій та зростаючого ризику кібератак, безпека бездротових мереж Wi-Fi набуває критичного значення. Захист даних у бездротових мережах забезпечується за допомогою протоколів захисту, таких як WPA2 і WPA3, кожен з яких має свої сильні та слабкі сторони у боротьбі з потенційними загрозами.

Значення протоколів захисту, таких як WPA2 і WPA3, та новітнього механізму OWE (Opportunistic Wireless Encryption), не може бути переоцінено в контексті забезпечення безпеки даних. Кожен з цих стандартів пропонує унікальні методи захисту, покликані протистояти специфічним загрозам. Поряд із розвитком технологій бездротового зв'язку еволюціонували і методи кібератак, що змушує наукову спільноту постійно шукати нові шляхи захисту. Розуміння основних принципів Wi-Fi допоможе краще оцінити виклики, які стоять перед протоколами захисту, такими як WPA2 і WPA3.

Метою дослідження є вивчення стійкості протоколу WPA3 до кібератак, аналіз потенційних вразливостей і розробка рекомендацій щодо зміцнення захисту бездротових мереж. Особлива увага присвячена аналізу вразливостей, виявлених за допомогою утиліти Dragonblood, яка дає змогу оцінити стійкість протоколу до специфічних типів атак.

## 1. Огляд літературних джерел

В умовах постійного розвитку технологій бездротових мереж і зростання кіберзагроз значний прогрес було досягнуто у захисті даних за допомогою сучасних криптографічних методів. Цей огляд критично розглядає різні протоколи, зосереджуючись на їхніх сильних та слабких сторонах у контексті забезпечення безпеки мережі. Безпека Wi-Fi зазнала багато змін, починаючи від WEP, введеного як частина оригінальних стандартів 802.11 у 1997 році, до надійнішого WPA3 і опортуністичного шифрування бездротових мереж (OWE), введених останніми роками. WPA2 і WPA3 були в центрі цих досягнень, пропонуючи поліпшений захист через такі функції, як покращені стандарти шифрування та захищені керівні кадри [9, 5]. Введення WPA3 вирішило кілька обмежень попередників, зокрема сильніші криптографічні практики. WPA3 надає індивідуальне шифрування даних, що значно зменшує поширені атаки, такі як ті, що виконувалися на слабших реалізаціях WPA2 [8]. Зокрема, WPA3 вводить передовий секрет, забезпечуючи, що попередні комунікації не можуть бути скомпрометовані, навіть якщо поточний сесійний ключ буде викрито [1, 2, 5].

Незважаючи на ці досягнення, вразливості все ще існують, як підкреслено у недавніх аналізах, таких як дослідження Dragonblood, яке виявило недоліки у механізмі рукостискання Dragonfly WPA3 [5]. Ці вразливості підкреслюють важливість постійного вдосконалення в протоколах безпеки для ефективної боротьби з новими загрозами.

Порівняльні дослідження WPA2, WPA3 і OWE демонструють значний прогрес у забезпеченні захисту бездротових з'єднань. Кожен протокол вносить специфічні переваги та виклики, що потребують збалансованого підходу до безпеки, особливо в середовищах з високим ризиком передання даних [3, 4, 6, 7, 10, 11, 12, 13].

## 2. Постановка завдання

Враховуючи той факт, що використання бездротових мереж стає щораз більшим, безпека цих з'єднань стає надзвичайно актуальним завданням у контексті захисту особистих даних користувачів та інформації організацій. Протоколи захисту Wi-Fi, такі як WPA2 і WPA3, відіграють основну роль

у забезпеченні цієї безпеки, однак вони також мають певні потенційні вразливості. Виявлення та аналіз цих вразливостей, особливо у новітньому протоколі WPA3, є критично важливими для підтримання високого рівня безпеки бездротових мереж.

Завдання дослідження містять:

1. Аналіз сучасних протоколів захисту мереж Wi-Fi з акцентом на вивчення протоколу WPA3.
2. Ідентифікація і оцінка потенційних вразливостей протоколу WPA3 за допомогою утиліти Dragonblood.
3. Розробка рекомендацій щодо підвищення безпеки бездротових мереж на основі результатів аналізу.

Дослідження має на меті не тільки виявити слабкі місця в захисті, який пропонує WPA3, але й сприяти розробленню ефективних стратегій забезпечення безпеки в умовах, коли кібератаки стають все більш витонченими і руйнівними.

В статті розглянуто комплексний порівняльний аналіз протоколів захисту Wi-Fi мереж, зокрема WPA2, WPA3 та OWE, з акцентом на їхні сильні та слабкі сторони у контексті найбільш розповсюджених типів атак. Вивчення цих протоколів дасть можливість не лише оцінити їх ефективність, але й сформулювати рекомендації щодо підвищення рівня безпеки інформаційних систем загалом, а також наголосити на важливості освіти користувачів у питаннях кібербезпеки.

## 3. Бездротові мережі Wi-Fi: загальний огляд

Wi-Fi – це бездротова технологія передання даних, що використовує радіохвилі для швидкого передання інформації на короткі відстані. Історія Wi-Fi починається у 1985 році, коли Федеральна комісія зв'язку США (FCC) ухвалила рішення про відкриття діапазонів радіочастотного спектра на частотах 900 МГц, 2,4 ГГц та 5,8 ГГц для неліцензійного використання. Цей крок дав можливість використовувати ці частоти для розробки та комерціалізації бездротових технологій, ставши фундаментом для майбутнього розвитку Wi-Fi. Вперше основні параметри для бездротового зв'язку були визначені у 1997 році інститутом інженерів з електротехніки та електроніки (IEEE) та були затверджені стандартом 802.11. Це стало можливим завдяки зусиллям комітету видатних компаній, які прагнули створити уніфікований стандарт, щоб усунути проблему несумісності між пристроями різних виробників.

У відповідь на потребу в маркетингу та подальшому розвитку стандарту група компаній створила неприбуткову організацію Wireless Ethernet Compatibility Alliance (WECA), яка пізніше була перейменована на Wi-Fi Alliance. Організація мала на меті сприяння уніфікації та сумісності бездротових пристроїв, а також популяризацію стандарту Wi-Fi.

Назве "Wi-Fi", що стала синонімом бездротового доступу до інтернету, розробила маркетингова фірма, найнята WECA. Попри поширену інформацію, що Wi-Fi є скороченням від "Wireless Fidelity", насправді це просто назва, яка не має конкретного значення.

З моменту свого створення стандарт 802.11 пройшов через кілька значних удосконалень, включаючи випуск 802.11b, 802.11a, 802.11g, 802.11n – версія Wi-Fi 4, 802.11ac – наступне покоління Wi-Fi 5, і останнього покращення 802.11ax – Wi-Fi 6, всі ці ітерації пропонували збільшення пропускної здатності та покращення ефективності. Ці розвитки спрямовані на задоволення щораз більших потреб у швидкості передання даних та одночасного під'єднання багатьох пристроїв.

IEEE 802.11, перший стандарт бездротового зв'язку, встановлений у 1997 році, заклав основу для того, що ми сьогодні знаємо як Wi-Fi. Початкова версія мала обмежену пропускну здатність до 2 Мбіт/с, що було адекватно для потреб того часу, але швидко стало недостатньо із зростанням обсягів передання даних. У 1999 році IEEE представило два значні вдосконалення: 802.11a та 802.11b. Стандарт 802.11b працював на частоті 2,4 ГГц і забезпечував швидкість передання даних до 11 Мбіт/с, тоді як 802.11a використовував частотний діапазон 5 ГГц для досягнення швидкості

до 54 Мбіт/с. Це розширення пропускної спроможності дало можливість Wi-Fi знайти ширше застосування у домашніх та офісних мережах. У 2003 році було введено стандарт 802.11g, який об'єднав переваги 802.11b та 802.11a, працюючи на частоті 2,4 ГГц із максимальною швидкістю 54 Мбіт/с. Це забезпечило кращу сумісність з наявним обладнанням та поліпшену пропускну спроможність. Стандарт 802.11n, введений у 2009 році, став переломним моментом завдяки використанню технології MIMO (Multiple Input, Multiple Output), що дало можливість збільшити швидкість передання даних до 600 Мбіт/с. Використання кількох антен для передання та прийому сигналів значно поліпшило якість зв'язку та дальність дії. Стандарт 802.11ac, запущений у 2013 році, відомий як Wi-Fi 5, приніс ще більше збільшення швидкості –до 3,46 Гбіт/с в теорії, використовуючи ширший канал зв'язку (до 160 МГц), більшу кількість MIMO потоків та модуляцію вищої щільності. Найновіший стандарт, 802.11ax або Wi-Fi 6, представлений у 2019 році, має на меті підвищити ефективність мережі в переповнених умовах, досягаючи максимальної теоретичної швидкості до 9,6 Гбіт/с. Використання таких технологій, як MU-MIMO (Multi-User MIMO) та OFDMA (Orthogonal Frequency Division Multiple Access), покращує роботу в середовищах із високою щільністю мереж і забезпечує більшу пропускну спроможність та надійність. Wi-Fi використовує метод розподілення спектра для ефективного передання даних, зменшуючи інтерференцію та підвищуючи ефективність використання радіочастотного спектра. Розвиток технології Wi-Fi тісно пов'язаний з інноваціями у сфері модуляції, керування спектром та оптимізації передання даних, що забезпечує неперервне покращення швидкості, дальності дії та надійності бездротових з'єднань.

Wi-Fi відіграє основну роль у розвитку цифрової економіки, забезпечуючи основу для бездротового доступу до інтернету вдома, на роботі та у публічних місцях. За його допомогою стало можливим легке під'єднання до інтернету без обмежень, що сприяло поширенню інформаційних технологій і цифровізації суспільства. Попереду Wi-Fi чекає продовження еволюції з особливим акцентом на підвищення швидкості, зменшення затримок та покращення безпеки. Розвиток технологій, таких як Інтернет речей (IoT), потребує від Wi-Fi адаптації до нових викликів, що спонукає до постійних інновацій у цій сфері. Wi-Fi залишається однією з найважливіших технологій сучасного світу, сприяючи розвитку бездротового зв'язку та інтернету, і продовжує адаптуватися до змінних потреб суспільства та технологій.

Еволюція безпеки в Wi-Fi мережах є основним аспектом у розвитку цифрової інфраструктури, яка відіграє важливу роль у сучасному суспільстві. Від ранніх днів бездротових технологій, коли був введений протокол WEP (Wired Equivalent Privacy) у 1997 році як частина оригінального стандарту IEEE 802.11, була потреба у забезпеченні безпеки переданих даних. Незважаючи на те, що WEP мав на меті створити рівень безпеки, порівняний з проводовими мережами, він швидко став недостатньо ефективним через серйозні недоліки в алгоритмі шифрування.

З появою WPA (Wi-Fi Protected Access) у 2003 році, Wi-Fi Alliance зробила крок вперед у покращенні безпеки бездротових мереж. WPA використовувала поліпшене шифрування TKIP (Temporal Key Integrity Protocol), яке забезпечувало динамічну зміну ключів і покращену перевірку цілісності даних. Однак навіть з цими покращеннями TKIP мала потенційні вразливості, що потребувало подальших удосконалень. Відповіддю на ці виклики стало введення WPA2 у 2004 році, яке стало новим стандартом безпеки для Wi-Fi мереж. WPA2 використовує AES (Advanced Encryption Standard) для шифрування, що забезпечує значно вищий рівень безпеки порівняно з TKIP. Впровадження WPA2 стало обов'язковим для всіх пристроїв, що підтримують Wi-Fi, забезпечуючи істотне покращення захисту мережевих з'єднань.

Анонсований у 2018 році, WPA3 став останньою великою інновацією у сфері безпеки Wi-Fi, відкривши нову еру захищеності бездротових мереж. Цей стандарт був розроблений як відповідь на щораз більші вимоги до безпеки та приватності в цифровому світі, де кібератаки стають все більш витонченими та руйнівними. WPA3 містить низку основних інноваційних характеристик, що значно поліпшують захист користувачів і мережевої інфраструктури. Однією з основних переваг

WPA3 є покращений захист персональних даних. Завдяки використанню передових методів шифрування та аутентифікації, WPA3 забезпечує конфіденційність інформації, яка передається між пристроями та точками доступу, навіть на відкритих або публічних мережах. Це зменшує ризики перехоплення даних зловмисниками та гарантує, що особиста інформація залишається захищеною. Запобігання атакам брутфорсом на паролі є ще однією важливою особливістю WPA3. Використання механізму SAE (Simultaneous Authentication of Equals) забезпечує додатковий рівень захисту у процесі автентифікації, ускладнюючи зловмисникам підбір паролів через послідовні або автоматизовані спроби. SAE використовує складніші алгоритми обміну ключами, що робить процес аутентифікації стійким до зовнішніх втручань. Захист від спроб деавтентифікації також покращено в межах WPA3. Такі атаки, що вимикають користувачів із мережі за допомогою навмисного переповнення деавтентифікаційними пакетами, стали поширеним засобом кібератак. WPA3 вводить механізми, які ускладнюють проведення цього типу атак, забезпечуючи стабільніше та безперервне під'єднання для користувачів.

Загалом впровадження WPA3 значно підвищує рівень безпеки Wi-Fi мереж, вносячи істотні вдосконалення в захист даних, аутентифікацію користувачів та стійкість до атак. Ці інновації відіграють основну роль у забезпеченні безпечного доступу до інтернету в епоху, коли цифрова безпека є важливішою ніж будь-коли.

Opportunistic Wireless Encryption (OWE) є значним проривом у забезпеченні безпеки відкритих Wi-Fi мереж, який був представлений разом із введенням стандарту WPA3 у 2018 році. Цей механізм безпеки забезпечує автоматичне шифрування даних між користувачами та точками доступу без потреби в паролях, значно підвищуючи безпеку з'єднань, які раніше вважалися незахищеними. Реалізація OWE використовує передові методи шифрування, зокрема Diffie-Hellman key exchange, для створення унікального зашифрованого каналу для кожного з'єднання, що значно ускладнює несанкціонований доступ до переданих даних. Незважаючи на його переваги в покращенні безпеки відкритих мереж і простоті у використанні, OWE має певні обмеження, зокрема вимогу до сумісності обладнання та потенційну вразливість до деяких типів атак, якщо не використовуються додаткові заходи безпеки. Незважаючи на це, впровадження OWE становить важливий крок у напрямку більш безпечного та приватного використання відкритих Wi-Fi мереж, спонукаючи до подальших інновацій у цій сфері.

## 4. Безпека протоколу WPA2

Широке прийняття та довіра до протоколу WPA2 серед виробників та користувачів зумовлені кількома основними аспектами, які визначають його як надійний стандарт захисту бездротових мереж. Ці фактори містять взаємну автентифікацію, високий рівень шифрування, широку взаємодію між обладнанням, що підтримує WPA2, та простоту використання.

Взаємна автентифікація дає можливість не тільки користувачеві перевіряти мережу, але й мережі перевіряти користувача, що значно знижує ризик під'єднання до несанкціонованих точок доступу. Шифрування з використанням AES (Advanced Encryption Standard) забезпечує надзвичайно високий рівень захисту даних. AES є стандартом, прийнятим урядом США для захисту конфіденційної інформації, і визнаний одним з найбезпечніших методів шифрування. Взаємодія забезпечує, що всі пристрої, які пройшли сертифікацію Wi-Fi CERTIFIED з 2006 року, можуть взаємодіяти між собою, використовуючи WPA2. Це гарантує, що користувачі можуть безпечно під'єднуватися до мереж, незалежно від бренду обладнання. Простота використання з впровадженням програми Wi-Fi Protected Setup у 2007 році значно спрощує процес налаштування захисту мережі, роблячи WPA2 доступним і зрозумілим для широкого кола користувачів.

Ці фактори разом створюють міцну основу для захисту бездротових мереж і забезпечують користувачів впевненістю в тому, що їхні дані захищені відповідно до найвищих стандартів безпеки.

Незважаючи на всі перелічені переваги цього протоколу безпеки, він все ж містить певні недоліки, наявність яких зумовила появу протоколу WPA3. Дослідження цього новітнього протоколу дало змогу вивести поняття безпеки безпровідних мереж на новий рівень.

## 5. Безпека протоколу WPA3

У серпні 2019 року Wi-Fi Alliance започаткував процес тестування точок доступу та клієнтських пристроїв для сертифікації Wi-Fi Certified WPA3. WPA3, або Wi-Fi Protected Access 3, є оновленням стандарту безпеки Wi-Fi, який вносить важливі поліпшення до наявних можливостей захисту, які були визначені в WPA2. WPA3 підтримує нові методи безпеки, виключає застарілі протоколи та потребує використання захисту кадрів керування (MFP) для підвищення стійкості критично важливих мережевих середовищ. WPA3-Personal використовує технологію одночасної автентифікації рівних (SAE), яка захищає користувачів від атак з використанням перебору паролів. WPA3-Enterprise надає додатковий рівень надійності шифрування з еквівалентом 192-біт.

WPA3-Personal вводить заміну автентифікації PSK (попередньо розділений ключ) традиційною аутентифікацією SAE, що є стійкою до атак з використанням офлайн-словників. Це покращення безпеки є особливо важливим для домашніх користувачів і середовищ, де використання 802.1X є недоступним. З погляду користувача, процес під'єднання залишається незмінним, але обмін даними за допомогою протоколу SAE захищає парольну фразу від атак грубою силою.

На відміну від WPA3-Personal, WPA3-Enterprise продовжує використовувати автентифікацію на основі 802.1X/EAP для забезпечення корпоративного рівня безпеки, залишаючи процес автентифікації корпоративного рівня незмінним. Основні вдосконалення полягають у підтримці багатофункціонального пристрою та додатковому розширеному криптографічному режимі.

Dragonblood містить набір вразливостей у реалізації WPA3 та протоколу обміну ключами Dragonfly. Ці вразливості можуть дати змогу зловмисникам знизити рівень захисту з'єднання або використовувати бічні канали для вилучення чутливої інформації, такої як пароль або частини ключа.

Для захисту від атак, пов'язаних з вразливостями WPA3 та Dragonblood, важливо дотримуватися таких рекомендацій. Виробники обладнання та програмного забезпечення часто випускають оновлення, які усувають виявлені вразливості. Важливо регулярно оновлювати всі компоненти мережевої інфраструктури та клієнтські пристрої. Навіть з використанням WPA3 сила парольної фрази залишається критичною. Використання довгих, складних та унікальних паролів може значно ускладнити атаки грубою силою. Фізичний доступ до мережевого обладнання може дозволити зловмисникам обійти електронні заходи безпеки. Важливо забезпечити належний фізичний захист мережевих пристроїв. Регулярний моніторинг мережевого трафіку та поведінки користувачів може допомогти виявити спроби атак або несанкціонований доступ. Застосування додаткових рівнів безпеки, таких як VPN (віртуальна приватна мережа) або шифрування кінцевої точки може надати додатковий захист для даних, які передаються через мережу. Навчання користувачів основам безпеки мережі та інформування їх про потенційні загрози може значно знизити ризик компрометації мережі.

Важливо відзначити, що безпека мережі є багатоаспектним завданням, яке потребує комплексного підходу та регулярного перегляду. Завжди корисно бути в курсі останніх досліджень у сфері кібербезпеки та впроваджувати рекомендовані практики безпеки.

Після розгляду покращень, які пропонує WPA3, важливо також звернути увагу на OWE – інноваційний підхід до забезпечення приватності у відкритих мережах. Цей протокол відіграє основну роль у захисті даних користувачів у громадських Wi-Fi мережах.

## 6. Безпека протоколу Opportunistic Wireless Encryption (OWE)

Традиційно, гарячі точки Wi-Fi та гостьові WLAN використовують відкритий захист без шифрування або автентифікації. Сертифікація Wi-Fi CERTIFIED Enhanced Open визначає покращену конфіденційність даних у мережах відкритого Wi-Fi. Ця сертифікація ґрунтується на протоколі Opportunistic Wireless Encryption (OWE). OWE визначений у документі IETF RFC 8110. Протокол OWE інтегрує встановлені механізми криптографії для надання кожному користувачеві унікального індивідуального шифрування, що захищає обмін даними між користувачем та точкою доступу.

Досвід для користувача аналогічний відкритому захисту, оскільки не потрібно вводити пароль або кодову фразу перед приєднанням до мережі. Зловмисні атаки прослуховування зменшуються, оскільки 802.11 кадри даних шифруються, але немає механізму аувтентифікації. Enhanced Open не є частиною WPA3 і є цілком іншою та необов'язковою сертифікацією безпеки. Є два режими роботи для OWE:

*Enhanced Open Only*

Цей режим використовує протокол OWE для надання шифрування CCMP/AES 128 біт для конфіденційності даних. 802.11 кадри даних шифруються, і також потрібен захист кадрів керування. Не використовується жоден протокол аутентифікації.

*Enhanced Open Transition*

Цей режим забезпечує зворотну сумісність з більшістю клієнтів, які не підтримують OWE, за допомогою використання двох SSID. Коли відкритий SSID налаштований на точці доступу з сертифікацією Enhanced Open, автоматично створюється другий прихований SSID, який використовує OWE.

Застарілі клієнти під'єднуються до відкритого SSID без шифрування. Однак у кадрі маяка відкритого SSID є елемент інформації OWE, який скеровує клієнтів Enhanced Open до прихованого SSID, що використовує OWE. SSID з OWE прихований для уникнення плутанини для драйверів застарілих клієнтів.

Enhanced Open відповідає лише наполовину вимогам до повноцінної безпеки Wi-Fi. OWE справді забезпечує шифрування та конфіденційність даних, але немає жодної форми автентифікації. Як вже зазначалося, Enhanced Open є додатковою сертифікацією з безпеки. Як наслідок багато виробників WLAN досі не підтримують OWE, а підтримка на боці клієнтів є мінімальною. Тому тактичні розгортання OWE наразі рідкісні. Однак коли в 2021 році з'явилися AP та клієнти на частоті 6 ГГц, підтримка OWE та Enhanced Open стала обов'язковою для сертифікації Wi-Fi 6E.

Використання OWE в контексті безпеки відкритих мереж дало можливість ширше побачити нагальність викликів у сфері захисту бездротових мереж. Нижче порівняємо основні характеристики та захисні механізми WPA2, WPA3 та OWE, щоб виділити їх сильні та слабкі сторони.

## 7. Порівняння протоколів WPA2, WPA3, OWE

Еволюція безпеки Wi-Fi від WPA2 до WPA3 та впровадження OWE відображає значний прогрес у забезпеченні захисту бездротових з'єднань. WPA3 з його покращеним шифруванням та додатковими функціями безпеки, як-от захист від повторного використання ключів і захист від атак на словник, є важливим кроком вперед порівняно з WPA2, забезпечуючи вищий рівень стійкості до різних видів кібератак. Особливість WPA3 у спрощенні процесу налаштування захищених з'єднань, особливо з Wi-Fi Easy Connect, робить його зручним для кінцевих користувачів, забезпечуючи високий рівень безпеки без потреби в складних налаштуваннях. OWE, з другого боку, робить свій внесок у забезпечення приватності в громадських Wi-Fi мережах, де автентифікація не потрібна, але важливо захистити дані користувачів. Плавний перехід для організацій та користувачів забезпечується завдяки зворотній сумісності WPA3 з WPA2, хоча для досягнення максимальної безпеки рекомендується використовувати пристрої та мережі, що повністю підтримують WPA3. Вибір між WPA2, WPA3 та OWE залежить від специфічних потреб безпеки, сумісності обладнання та контексту використання мережі, причому WPA3 пропонує найкращий захист і новітні технології для сучасних мереж, тоді як OWE відіграє основну роль у забезпеченні приватності в громадських місцях.

Розглянемо порівняльну таблиця протоколів WPA2, WPA3 та OWE.

Проаналізувавши еволюцію та важливість протоколів WPA2, WPA3 та OWE для безпеки Wi-Fi мереж наступним кроком є глибше дослідження стійкості цих систем до сучасних кіберзагроз. У цьому контексті, особливо актуальним стає аналіз протоколу WPA3 з використанням утиліти Dragonblood. Це дасть змогу не тільки виявити потенційні вразливості в найновішому стандарті безпеки, але й оцінити ефективність запроваджених поліпшень порівняно з попередніми версіями. Перехід до практичної частини дослідження підкреслює значення постійного аналізу та оновлення захисних механізмів для адаптації до швидкозмінного ландшафту кіберзагроз.

**Порівняльна таблиця протоколів WPA2, WPA3 та OWE**

| Особливість | WPA2 | WPA3 | OWE |
|---|---|---|---|
| **Рік випуску** | 2004 | 2018 | 2018 |
| **Шифрування** | CCMP (AES) | GCMP-256 (AES) | Не застосовується |
| **Автентифікація** | PSK (персональний) та EAP (корпоративний) | SAE (персональний) та EAP (корпоративний) | Підвищена відкритість (без автентифікації) |
| **Захист від повторного використання** | Ні | Так | Так |
| **Захист від атак на словник** | Ні | Так | Не застосовується |
| **Захист керівних рамок** | Опціонально | Обов'язковий | Не застосовується |
| **Легкість налаштування** | Помірна | Покращена з Wi-Fi Easy Connect | Висока (без паролів) |
| **Сумісність** | Поширена | Зростає | Специфічні сценарії (громадські Wi-Fi тощо) |
| **Рекомендоване використання** | Загальне використання, де WPA3 недоступний | Нові пристрої, середовища з вищим рівнем безпеки | Громадські мережі, шифрування не потрібне, але потрібна приватність |

## 8. Аналіз безпеки протоколу WPA3 за допомогою здійснення атаки на основі утиліти Dragonblood

Аналіз безпеки протоколу WPA3 через реалізацію атаки на основі утиліти Dragonblood відкриває важливі аспекти щодо стійкості цього новітнього стандарту безпеки Wi-Fi. WPA3 був розроблений з метою подолання вразливостей, наявних у WPA2, зокрема через введення Simultaneous Authentication of Equals (SAE), який замінив WPA2 Pre-Shared Key (PSK) для підвищення стійкості проти атак брутфорсом та атак на повторне використання ключів.

Утиліта Dragonblood виявила декілька вразливостей у реалізації WPA3, зокрема, вразливості, пов'язані з методом SAE, який є основним складником WPA3. Ці вразливості дають можливість зловмисникам виконувати атаки бічними каналами, які можуть викривати інформацію про пароль або навіть дати можливість їм обійти процес аутентифікації. Це атаки, які використовують часові відмінності в обробці SAE-запитів, щоб зробити висновки про пароль або атаки на кеш, що використовують спостереження за використанням кеш-пам'яті процесора для витягування основної інформації.

Крім того, було виявлено, що деякі реалізації WPA3 дають можливість для атаки "downgrade", у якій зловмисник може примусити клієнтський пристрій використовувати менш безпечний протокол, наприклад, WPA2, де вже відомі вразливості можуть бути використані для компрометації безпеки.

Для захисту від виявлених утилітою Dragonblood вразливостей важливо, щоб розробники та виробники обладнання оновлювали свої системи та прошивку, зокрема застосування патчів безпеки та вдосконалення реалізації SAE. Користувачам своєю чергою треба впевнитись, що вони використовують останні версії програмного забезпечення для своїх бездротових пристроїв та активно стежать за оновленнями безпеки від своїх постачальників.

Підсумовуючи, атаки, виявлені за допомогою утиліти Dragonblood, підкреслюють потребу постійного аналізу та вдосконалення стандартів безпеки Wi-Fi. WPA3 представляє значний крок вперед у покращенні безпеки бездротових з'єднань, але виявлені вразливості нагадують про потребу відповідального підходу до реалізації та використання цих технологій.

Перейдемо до практичної частини. Метою цієї роботи є проведення детального аналізу безпеки протоколу WPA3, використовуючи утиліти Dragonblood для виявлення потенційних вразливостей в його реалізації. WPA3, який є останнім стандартом захисту бездротових мереж, вводить низку вдосконалень у безпеку Wi-Fi зв'язку, зокрема, покращену захищеність перед атаками брутфорсом та підвищену конфіденційність даних користувачів. Однак, як і будь-яка технологія,

WPA3 не є імунним до потенційних вразливостей, які можуть бути експлуатовані зловмисниками.

Утиліти Dragonblood були спеціально розроблені для тестування безпеки протоколу WPA3, і їх використання дасть змогу не тільки ідентифікувати слабкі місця у захисті, але й оцінити ефективність механізмів шифрування та автентифікації, які використовуються у межах цього стандарту. Через проведення цілеспрямованих атак і симуляцій атак, що використовуються в реальному світі, буде можливо виявити можливі шляхи незаконного проникнення в захищені бездротові мережі, що використовують WPA3, та розробити рекомендації щодо посилення захисту і запобігання таким атакам.

Ця робота має на меті не тільки виявлення технічних вразливостей, але й забезпечення глибшого розуміння принципів роботи та захисту, які лежать в основі протоколу WPA3, таким способом сприяючи розвитку безпечніших рішень для захисту бездротових мереж від потенційних кібератак.

Розглянемо основні кроки роботи:

1. Підготовка системи:

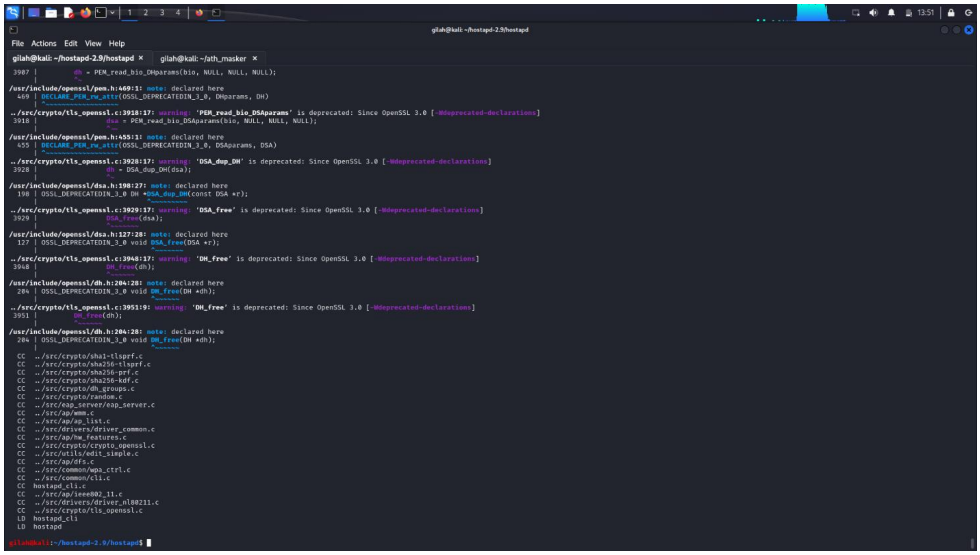

*Рис. 1. Тестова компіляція hostapd без змін*

2. Модифікація коду hostapd

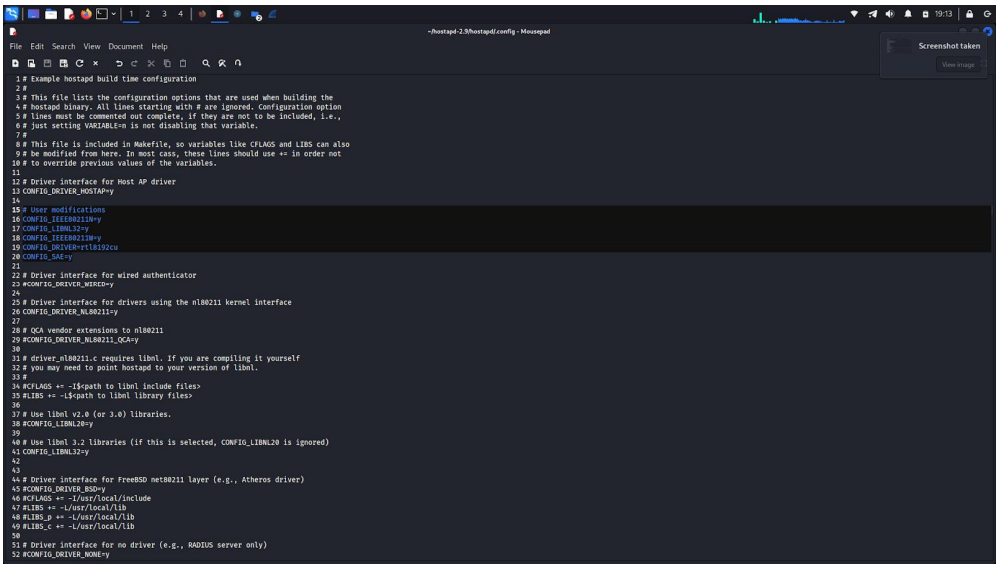

*Рис. 2. Модифікація конфігурації збірки hostapd*

*Рис. 3. Заміна файлу ieee802_11.c на модифікований*

3. Запуск модифікованого hostapd

На цьому етапі роботи було проведено детальну підготовку системи для тестування безпеки протоколу WPA3 за допомогою модифікації коду сервера безпровідних точок доступу hostapd. Зміни становили модифікацію конфігурації збірки hostapd та заміну файлу ieee802_11.c на модифікований варіант, що давало можливість здійснити атаку деавтентифікації на мережі зі стандартом шифрування WPA3.

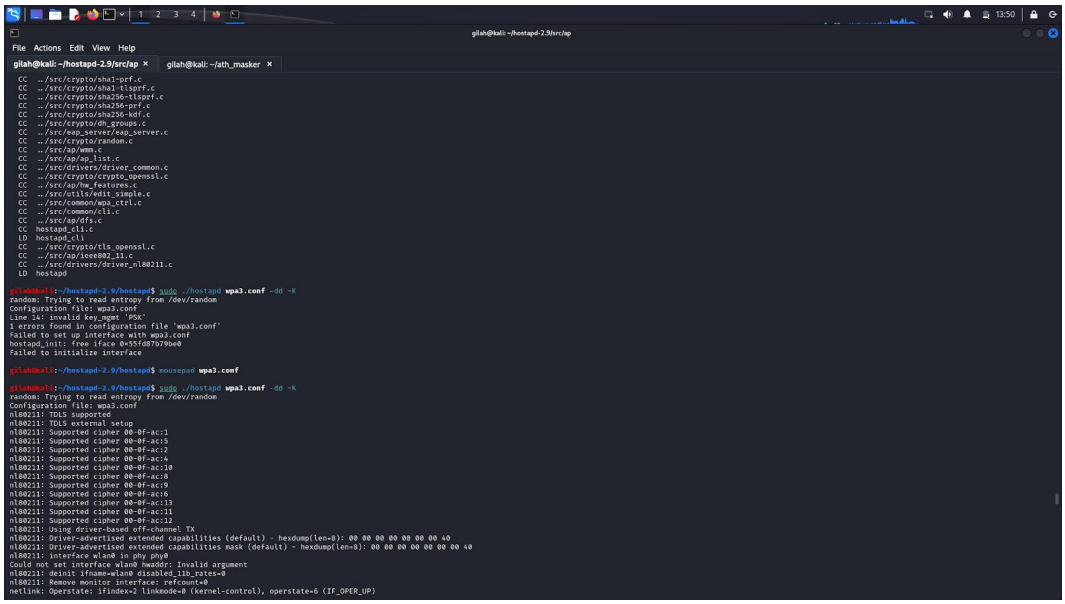

*Рис. 4. Компіляція модифікованого hostapd та спроба запуску*

Незважаючи на технічні труднощі, такі як невдала спроба запуску модифікованого hostapd через внутрішню помилку, дослідження продемонструвало, що застосована модифікація здатна створювати інтенсивний шквал пакетів деавтентифікації. Це вказує на потенціал такої модифікації, як інструменту для проведення атак на бездротові мережі, незважаючи на покращену стійкість стандарту WPA3 до атак деавтентифікації.

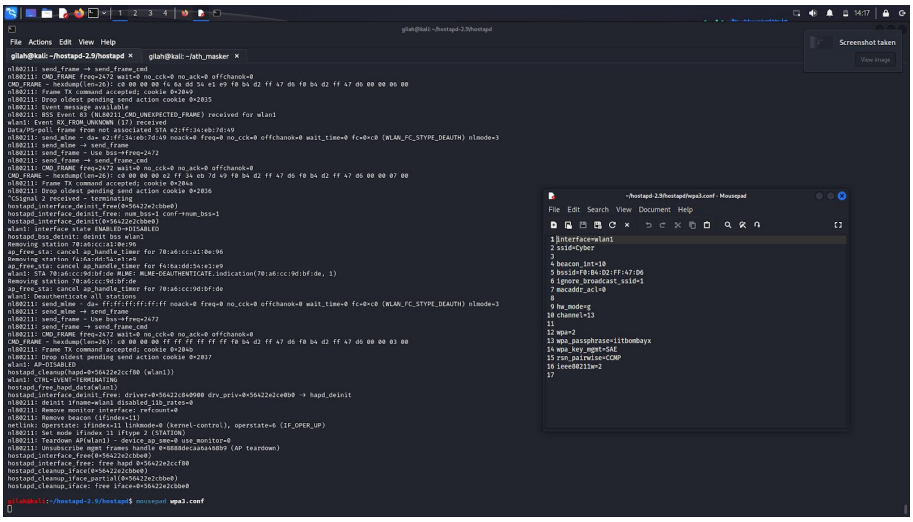

*Рис. 5. Зміст файлу конфігурації атаки*

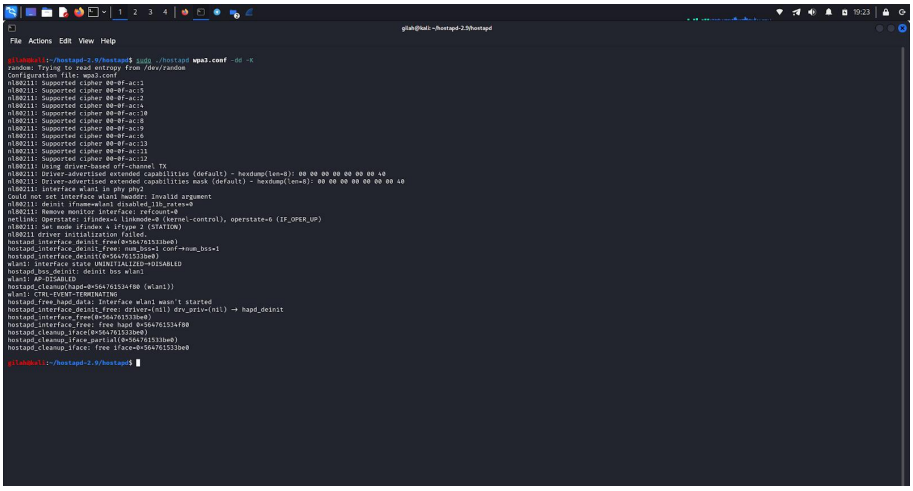

*Рис. 6. Невдала спроба запуску hostapd у зв'язку з невідомою внутрішньою помилкою*

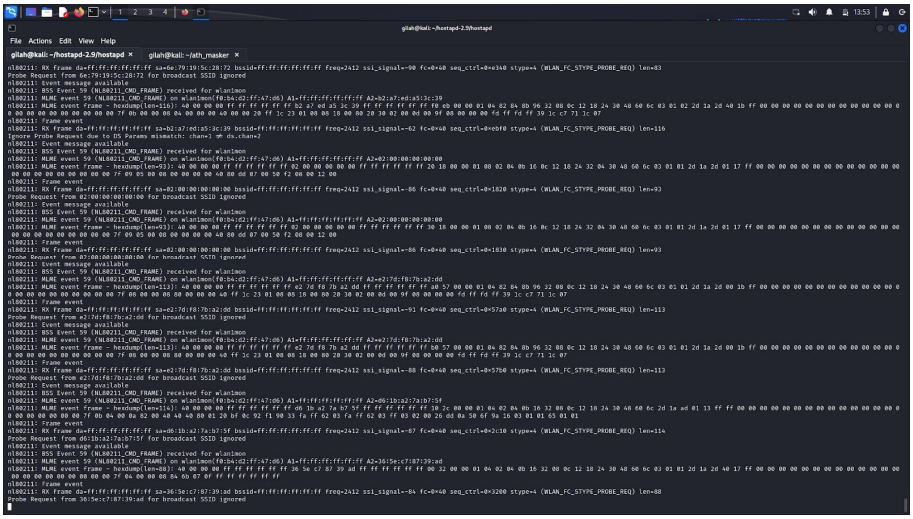

*Рис. 7. Робота атаки, надсилання фреймів деавтентифікації*

4. Аналіз файлу Wireshark

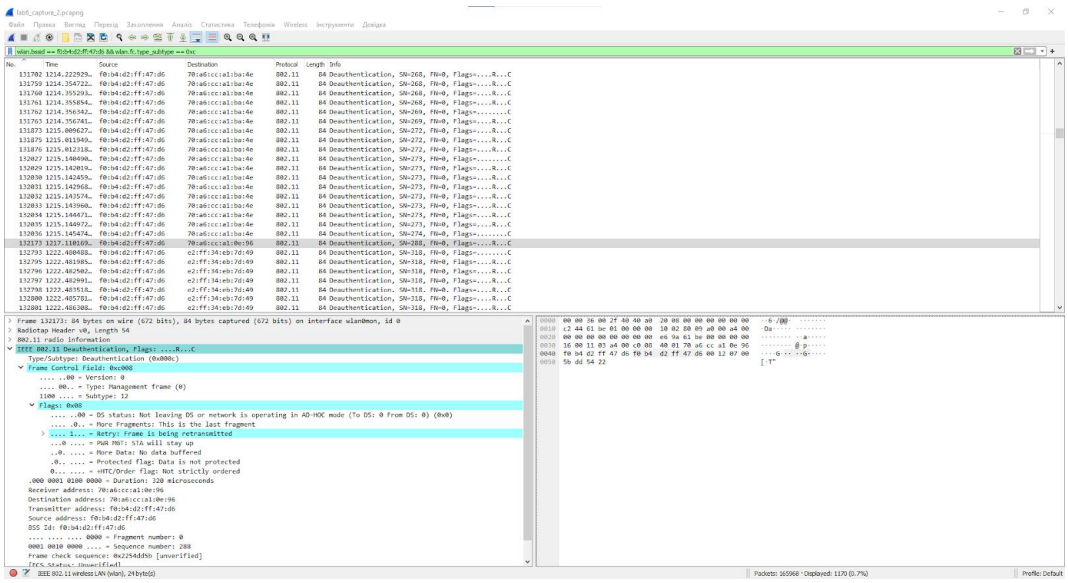

*Рис. 8. Шквал фреймів деавтентифікації на різні клієнтські BSSID*

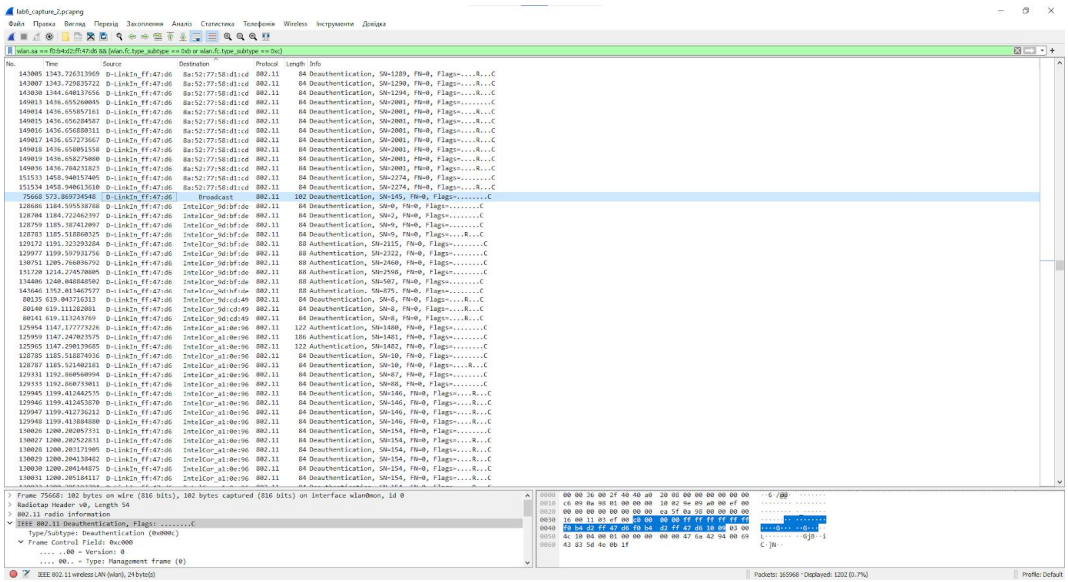

*Рис. 9. Послідовність автентифікації та деавтентифікації*

Аналіз файлу Wireshark підтвердив, що атака справді викликає значну кількість пакетів деавтентифікації, які спрямовані на різні клієнтські BSSID, що демонструє здатність такої атаки впливати на процес автентифікації в мережі. Однак, як показало дослідження, мережа зі стандартом WPA3 продемонструвала покращену стійкість до таких атак, зберігаючи свою функціональність, незважаючи на спроби деавтентифікації.

Висновки з цього експерименту свідчать про успішну модифікацію hostapd для проведення атаки деавтентифікації, а також підтверджують важливість подальших досліджень у сфері безпеки бездротових мереж, зокрема з використанням стандарту WPA3. Це дасть можливість краще розуміти потенційні вразливості та розробляти ефективні засоби захисту від можливих атак.

## 9. Результати дослідження

Дослідження безпеки протоколу WPA3 з використанням утиліти Dragonblood дало можливість виявити кілька основних аспектів, які важливі для забезпечення міцності та надійності бездротових мереж. Аналіз показав, що хоча SAE було введено для підвищення безпеки проти атак брутфорсом та повторного використання ключів, існують серйозні вразливості. Спеціальні атаки бічними каналами могли викривати інформацію про пароль та обходити процес аутентифікації. Це містить атаки, які використовують часові відмінності в обробці SAE-запитів, та атаки на кеш, що здійснюють спостереження за використанням кеш-пам'яті процесора.

Було виявлено, що недоліки у реалізації WPA3 дають можливість проведення атак "downgrade", де зловмисник може примусити клієнтський пристрій використовувати менш безпечний протокол, як WPA2, що спрощує доступ до мережі через відомі вразливості. В процесі практичної частини дослідження з модифікацією коду сервера бездротових точок доступу (hostapd) було підтверджено, що механізми шифрування та автентифікації, які використовуються у WPA3, залишаються стійкими проти атак деавтентифікації. Втім залишається потенціал для покращення захисту від атак бічними каналами.

Для захисту від ідентифікованих вразливостей потрібно регулярно оновлювати системи та прошивку, використовувати патчі безпеки та вдосконалювати реалізацію SAE. Також важливо, щоб користувачі були впевнені в останніх версіях програмного забезпечення для своїх пристроїв та активно стежили за оновленнями безпеки. Результати дослідження підкреслюють потребу постійного аналізу та вдосконалення стандартів безпеки Wi-Fi. Незважаючи на значні покращення, які внесла технологія WPA3, виявлені вразливості наголошують на потребі відповідального підходу до реалізації та використання цих технологій для забезпечення вищого рівня безпеки бездротових з'єднань.

## Висновки

Як висновок, треба підкреслити важливість постійного аналізу та оновлення стандартів безпеки для бездротових мереж у відповідь на щораз більші кіберзагрози. За результатами детального розгляду протоколів WPA2, WPA3 та OWE виявлено, що впровадження WPA3 значно підвищує стійкість бездротових мереж до атак порівняно з WPA2, особливо завдяки запровадженню покращеного механізму автентифікації та захисту від атак на повторне використання ключів. Однак використання утиліт Dragonblood демонструє, що навіть найновіші стандарти не є повністю імунітетними до потенційних вразливостей, що потребує регулярного перегляду та оновлення захисних механізмів.

Протокол OWE робить важливий внесок у забезпечення конфіденційності в мережах відкритого Wi-Fi, пропонуючи базовий рівень шифрування без потреби в аутентифікації. Це розширює можливості захисту даних для користувачів у громадських місцях, хоча і не забезпечує повного спектру захисту, порівняно з повнофункціональними рішеннями, як WPA3.

Ми також акцентуємо увагу на потребі комплексного підходу до безпеки мережі, що охоплює не тільки застосування найновіших стандартів шифрування та автентифікації, але й регулярне оновлення програмного забезпечення, фізичний захист мережевого обладнання, моніторинг мережевого трафіку та освіту користувачів щодо потенційних загроз і методів захисту.

Покращення безпеки бездротових мереж є неперервним процесом, який потребує від постачальників обладнання, розробників програмного забезпечення, адміністраторів мереж та кінцевих користувачів активної участі в процесі забезпечення захисту інформації в умовах швидко змінювального кіберпейзажу.

Аналітичний огляд даних, зібраних за допомогою Wireshark, виявив, що атака деавтентифікації спричиняє значне збільшення обсягу пакетів деавтентифікації, цілеспрямованих на різноманітні клієнтські BSSID. Це спостереження підтверджує ефективність таких атак у перешкоджанні процесу автентифікації в мережі, що може призвести до зниження загальної продуктивності та доступності мережевих ресурсів.

Попри виявлену активність атак, мережі, що використовують стандарт безпеки WPA3, продемонстрували сильну стійкість, здатність підтримувати стабільну функціональність навіть в умовах інтенсивних спроб деавтентифікації. Це свідчить про значні покращення у захисті, впроваджені в межах WPA3, що забезпечують ефективніший захист проти атак, які спрямовані на переривання процесу автентифікації.

Експеримент з модифікацією hostapd для імітації атаки деавтентифікації не лише продемонстрував технічну можливість такої атаки, але й підкреслив важливість подальших досліджень у сфері безпеки бездротових мереж. Зокрема, застосування стандарту WPA3 відкриває нові горизонти для поглибленого вивчення потенційних вразливостей та розробки комплексних методів захисту, спрямованих на протидію атакам, які можуть становити загрозу для мережевої інфраструктури.

Беручи до уваги результати цього експерименту, можна зробити висновок про критичну потребу інвестування в розвиток та впровадження передових стандартів безпеки, таких як WPA3, які забезпечують значно більшу стійкість до сучасних кібератак, таким способом підвищуючи надійність та доступність бездротових мережевих сервісів.

## Список літератури


1. *Wi-Fi Alliance. (2022). Wi-Fi Easy Connect™ Specification v3.0. [Online]. Available at: https://www.wi-fi.org/system/files/Wi-Fi_Easy_Connect_Specification_v3.0.pdf*
2. *Wi-Fi Alliance. (May 2021). Wi-Fi Protected Access® Security Considerations. [Online]. Available at: https://www.wi-fi.org/system/files/Security_Considerations_20210511.pdf*
3. *Wi-Fi Alliance. (n.d.). WPA3™ Specification Version 3.1. Available at: https://www.wi-fi.org/system/files/WPA3%20Specification%20v3.3.pdf*
4. *IEEE Standards Association. (n.d.). Available at: https://standards.ieee.org/news/ieee_802_11ak-2018/*
5. *Vanhoef M., & Ronen E. (2019). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. New York University Abu Dhabi; Tel Aviv University & KU Leuven. [Online]. Available at: https://papers.mathyvanhoef.com/dragonblood.pdf*
6. *White Paper: Networking | Security. Seamless Next-generation Wi-Fi Security Through Multivendor End-to-end WPA3 Verification. (2021). Available at: https://www.intel.com/content/dam/support/us/en/documents/wireless/intel-whitepaper-wifi-security-through-wpa3-verification.pdf*
7. *Stallings W. (2005). Wireless Communications and Networks (2nd ed.). Upper Saddle River, NJ: Pearson Prentice Hall. ISBN 0-13-191835-4. Available at: http://182.74.60.194/opac-tmpl/bootstrap/images/link/ebook/Computer%20Science/Wireless%20Communications%20and%20Networking.pdf*
8. *Pothuganti K., & Chitneni A. (2014). A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. Advance in Electronic and Electric Engineering, 4(6), 655-662. Available at:https://www.researchgate.net/publication/312471356_A_comparative_study_of_wireless_protocols_Bluetooth_UWB_ZigBee_and_Wi-Fi*
9. *Sharma K., & Dhir N. (2014). A Study of Wireless Networks: WLANs, WPANs, WMANs, and WWANs with Comparison. International Journal of Computer Science and Information Technologies, 5(6), 7810-7813. Available at: https://www.academia.edu/25106472/A_Study_of_Wireless_Networks_WLANs_WPANs_WMANs_and_WWANs_with_Comparison*
10. *Ciubotaru B., & Muntean G. M. (2013). Advanced Network Programming: Principles and Techniques. London: Springer-Verlag. ISBN 978-1-4471-5292-7. Available at: https://www.iqytechnicalcollege.com/Advanced%20Network%20Programming%20-%20Principles%20and%20Techniques.pdf*
11. *Digi International Inc. (2007–2008). An Introduction to Wi-Fi. Rabbit Product Manual. Available at: https://ftp1.digi.com/support/documentation/0190170_b.pdf*
12. *Wi-Fi Alliance. (April 2023). Generational Wi-Fi® User Guide. [Online]. Available at: https://www.wi-fi.org/system/files/Generational_Wi-Fi_User_Guide_202304.pdf*
13. *Kaveh Pahlavan, Prashant Krishnamurthy. (November 2020). Historical Perspective. International Journal of Wireless Information Networks, 28(6), pp. 1–17. [Online]. Available at: DOI: 10.1007/s10776-020-00501-8 https://www.researchgate.net/publication/347057817_Evolution_and_Impact_of_and_Impact_of_Wi-Fi_Technology_and_Applications_A_Historical_Perspective*

# SECURITY ANALYSIS OF MODERN WI-FI NETWORK PROTECTION PROTOCOLS: ASSESSMENT OF WPA3 PROTOCOL RESISTANCE DURING ATTACKS BASED ON DRAGONBLOOD UTILITY

**O. Mykhaylova, A. Stefankiv, Y. Nakonechnyi**

Lviv Polytechnic National University,
Department of Information Protection



**With the constant development of information technology and the growing threat of cyber attacks, the security of Wi-Fi wireless networks is of particular relevance. This article aims to provide an in-depth analysis of modern Wi-Fi security protocols such as WPA2, WPA3, and OWE, focusing on their strengths and weaknesses in securing the network against the most common types of attacks.**

**This paper looks at wireless network security threats, including man-in-the-middle attacks, Wi-Fi access point phishing, and exploits that target specific security mechanisms. An important part of the research is a description of test methods, attack tools such as Aircrack-ng and Wireshark, and a detailed analysis of the results obtained.**

**This work focuses on a detailed security analysis of the WPA3 protocol, using Dragonblood utilities to identify possible vulnerabilities in its implementation. Through targeted attacks and simulations that mimic real-world cyberattacks, the goal is to identify potential breaches of secure wireless networks using WPA3. This allows us to evaluate the effectiveness of the encryption and authentication mechanisms used within the framework of this standard and develop recommendations for increasing the level of security of information systems. During the study, practical experiments will be conducted to modify the code of the wireless access point server, and data obtained using the Wireshark program will be analyzed to assess the impact of attacks on the functionality of the network. The results of the work highlight the need for continuous improvements in Wi-Fi security technologies to provide reliable security in the face of growing cyber threats.**

**Keywords: Wireless networks, Wi-Fi security protocols, WPA2, WPA3, attacks on Wi-Fi, methods of protecting against attacks, information system security, vulnerability analysis, attack tools, increasing the level of security, user education, network component software, data encryption, VPN.**