ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

АВТОМАТИЗОВАНІ ТА ТЕЛЕМАТИЧНІ СИСТЕМИ НА ТРАНСПОРТІ

УДК 004.732:656.2

І. В. ЖУКОВИЦЬКИЙ[1*], І. О. ПЕДЕНКО[2*]

[1*]Каф. «Електронні обчислювальні машини», Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпро, Україна, 49010, тел. +38 (056) 373 15 89, ел. пошта ivzhukl@ua.fm, ORCID 0000-0002-3491-5976

[2*]Каф. «Електронні обчислювальні машини», Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпро, Україна, 49010, тел. +38 (056) 373 15 89, ел. пошта actek98@gmail.com, ORCID 0000-0001-8130-2657

АНАЛІЗ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ WI–FI В АВТОМАТИЗОВАНИХ СИСТЕМАХ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Мета. У роботі передбачено: проаналізувати основні механізми захисту, які наявні в бездротових мережах Wi–Fi; показати механізми атак на ці засоби захисту; виконати порівняльний аналіз ефективності механізмів захисту, надати рекомендації для використання цих механізмів в автоматизованих системах залізничного транспорту; побудувати демонстраційну модель атак на засоби захисту бездротової мережі Wi–Fi. **Методика.** На підставі огляду значної кількості вітчизняних та закордонних джерел проведено порівняльний аналіз механізмів захисту бездротової мережі Wi–Fi, у яких проаналізовано окремі стандарти захисту, виявлено їх сильні та слабкі сторони. Показано різноманітні атаки на засоби автентифікації та механізми гарантування безпеки інформаційного обміну. Для демонстрації атаки на ці засоби захисту розроблено алгоритм демонстраційної імітаційної моделі роботи протоколу захисту WPA2 з можливістю проведення атак на цей протокол. **Результати.** Виконано порівняльний аналіз основних стандартів механізмів захисту бездротової мережі Wi–Fi, зокрема WEP, WPA, WPA2, WPA3. Продемонстровано різноманітні атаки та ці засоби. Показано перевагу та слабкість окремих механізмів засобів захисту, надано рекомендації для їх використання. Побудовано демонстраційну модель атак на механізми захисту бездротової мережі, яка показує такі атаки, як атака на парольну фразу та атака KRACK. Для демонстрації в програмі обрано стандарт WPA2 з механізмом автентифікації PSK та механізмом криптографічного захисту CCMP–128. **Наукова новизна.** Наведено широкий спектр механізмів захисту бездротової мережі Wi–Fi, показано можливості окремих механізмів захисту, проведено порівняння стандартів захисту мережі Wi–Fi. В оригінальній програмній моделі показано, як помилкові дії користувача допомагають зловмиснику подолати сучасні механізми захисту. **Практична значимість.** Рекомендації щодо використання окремих засобів захисту бездротових мереж Wi–Fi можуть бути використані під час побудови системи захисту окремих елементів автоматизованих систем залізничного транспорту. Демонстраційна модель атаки на мережу Wi–Fi може бути використана в навчальному процесі для підготовки фахівців у галузі кібербезпеки.

Ключові слова: мережа Wi–Fi; стандарти захисту; безпека; автентифікація; шифрування

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

Вступ

В автоматизованих системах залізничного транспорту перспективним напрямом є використання бездротових мереж Wi–Fi, зокрема для зв'язку всередині пасажирських потягів [3], на станціях для використання персоналом, що перебуває за межами службових приміщень та має необхідність доступу до автоматизованих систем (наприклад, до баз даних АСК ВП УЗ–Є).

У США та деяких інших країнах світу з 2015 року запроваджується система позитивного контролю потяга (Positive Train Control – PTC) [3, 16], яка призначена для запобігання нещасним випадкам (рис. 1).

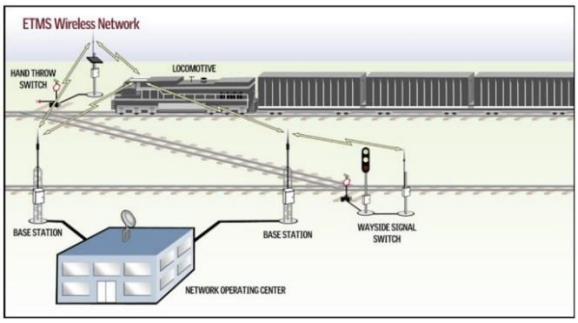

Рис. 1. Приклад архітектури PTC (взято з [16])

Fig. 1. Butt of PTC architecture (taken from [16])

Комунікації PTC складаються із системи обміну повідомленнями й декількох провідних і бездротових мереж, через які відбувається обмін повідомленнями між локомотивами, приколійними системами й серверами бек-офісу. Згідно з [3], «поїзди також обладнано 802.11x Wi–Fi, що особливо корисно у таких областях застосування, як технічне обслуговування вантажних дворів, або в межах станцій, тому що більша пропускна здатність мереж Wi-Fi дозволяє завантажувати діагностику, і здійснювати завантаження файлів, відновлення програмного забезпечення й запуск програмного забезпечення або комп'ютерну ініціалізацію при необхідності».

Є приклади, коли мережа Wi–Fi підтримує критично важливі системи залізничного транспорту. Так, інтелектуальна мережа Wi–Fi від компанії Ruckus [2] забезпечує бездротову передачу відеоінформації. Використовується охоронцями на об'єкті, а також для відеоконтролю рейкових колій станцій. Функція збору даних із RFID і оптичних сканерів дозволяє збирати таку, наприклад, інформацію, як дані про квитки, стан фрахту й місце розташування вантажів.

У [14] досліджено мережу Wi–Fi на сортувальній станції.

Інформація, що циркулює та зберігається в автоматизованих системах залізничного транспорту, повинна бути надійно захищена. І мова йде не тільки про недопущення порушення конфіденційності цієї інформації, а й про недопущення порушення її цілісності та доступності.

На відміну від дротових мереж, коли станції фізично з'єднані через кабель і наявна можливість контролю цих під'єднань, бездротова мережа є загальнодоступною. Контроль за під'єднанням станцій у цій мережі набагато складніший. Перехоплення інформації, що циркулює по WLAN, можливе без використання складного обладнання.

Досить часто вразливості з'являються через некоректну конфігурацію станцій та точок доступу. Деякі функції, додані розробниками для полегшення роботи, призводять до появи недоліків та вразливостей захисту.

Можна виділити такі групи загроз:

– несанкціоноване під'єднання до приладів та мереж;

– перехоплення та розкриття трафіка (прослуховування, злам шифрування);

– модифікація трафіка (підробка повідомлень, ін'єкції в кадри);

– порушення доступності (завади, захоплення ресурсів мережі).

В [1] описана вразливість бездротових клієнтів, згідно з якою зловмисник може від'єднати клієнтів від точки доступу, до якої вони під'єднані, і під'єднати до іншої точки доступу, менш безпечної.

Для протидії атакам на бездротові мережі, які засновані на вищеназваних загрозах, використовують стандарти безпеки, створені організацією Wi–Fi Alliance: WPA (Wi–Fi Protected Access), WPA2, WPA3.

Вочевидь, для безпечної роботи бездротових мереж на залізничному транспорті необхідно використовувати весь спектр механізмів захисту цих стандартів.

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

Мета

Основною метою нашої роботи є порівняльний аналіз різноманітних заходів забезпечення захисту бездротових мереж Wi–Fi, з урахуванням останніх стандартів захисту, а також аналіз атак зловмисників на захисні заходи та стандарти, що допоможе ефективно обрати та застосувати ці механізми. Для означеного аналізу передбачено побудувати імітаційну програмну модель атак на засоби захисту бездротової мережі Wi–Fi, яка дозволить продемонструвати можливість атак за умови помилок користувача.

Методика

Автори виконали огляд світової літератури з теми дослідження з використанням повнотекстових і реферативних баз даних, повідомлень в Internet за період 2001–2020 рр., що висвітлюють стандарти захисту мереж Wi–Fi та атаки зловмисників на ці стандарти

Загальні відомості про технологію Wi–Fi. Wireless Fidelity (Wi–Fi) – технологія бездротової локальної мережі (Wireless Local Area Network, WLAN) на основі стандартів IEEE 802.11.

Стандартна схема роботи Wi–Fi передбачає наявність точок доступу (ТД) і станцій (клієнтів). Такий режим роботи мережі називається інфраструктурним, або Hot-spot. Також існують інші, менш поширені схеми роботи Wi–Fi (з прямим під'єднанням між клієнтами). У цій роботі розглянемо лише режим Hot-spot.

Аналіз механізмів захисту в бездротових мережах Wi–Fi. Під час використання будь-якого механізму захисту в мережах Wi–Fi існує певна послідовність роботи:

1. Клієнт дізнається про наявність бездротової мережі та її параметри.
2. Відбувається процес автентифікації клієнта та його асоціація (процес виділення ресурсів ТД для створення нової сесії, синхронізації з клієнтом та виділення йому відповідного ідентифікатора асоціації) з конкретною точкою доступу, після чого він стає учасником мережі.
3. Обмін інформацією між учасниками мережі відбувається з використанням механізмів криптографічного захисту (шифрування інформації).

Тобто для захисту бездротової мережі використовують два основних механізми: автентифікації та шифрування.

Механізми автентифікації. У мережах Wi–Fi можуть використовуватись такі типи автентифікації:

– відкритих систем (Open System authentication);

– із загальним ключем (Shared Key authentication);

– на основі стандарту IEEE 802.1X;

– на основі попередньо встановлених ключів (Pre–Shared key, PSK).

Автентифікація 802.11. Першим стандартом, який був розроблений для захисту мереж Wi–Fi, був стандарт IEEE 802.11 [10] під назвою WEP (Wired Equivalent Privacy – протокол безпеки бездротових локальних мереж). Ця версія стандарту передбачала два методи автентифікації: автентифікація відкритих систем та автентифікація із загальним ключем.

Автентифікація відкритих систем – метод автентифікації за замовчуванням. Цей метод також називають «відкрита», або «нульова» автентифікація. Він фактично не є механізмом автентифікації й не забезпечує ніякої перевірки. Автентифікація відбувається шляхом обміну двома повідомленнями у відкритому вигляді. Перше повідомлення – це запит автентифікації від клієнта. Друге повідомлення – це підтвердження автентифікації від ТД.

Автентифікація із загальним ключем (рис. 2) використовує криптографічні механізми (шифрування повідомлень автентифікаціїї), але буде вдалою лише за умови використання однакових ключів WEP клієнтом та ТД.

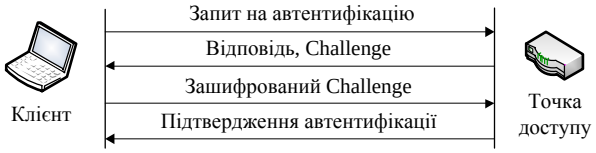

Рис. 2. Обмін повідомленнями Shared Key Authentication

Fig. 2. Messaging Shared Key Authentication

Автентифікація із загальним ключем за стандартом IEEE 802.11 легко може бути пройдена зловмисником. Знаючи Challenge і зашифрований Challenge, зловмисник може виконати над

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

ними операцію XOR та отримати ключовий потік. Використавши відомий ключовий потік, він зможе пройти автентифікацію.

Наступним кроком, що поліпшує процес автентифікації із загальним ключем, став стандарт IEEE 802.1X [12], який використовують у мережах високої безпеки (Robust Security Network, RSN) для взаємної автентифікації точки доступу та клієнта.

За стандартом виділено три ролі для учасників автентифікації:

– клієнт (Supplicant);

– автентифікатор (Authenticator);

– сервер автентифікації (Authentication, Authorization and Accounting, AAA).

Для передачі всієї інформації, необхідної для автентифікації, використовують протокол Extensible Authentication Protocol (EAP), який описано в RFC 3748.

Відповідно до [12], сервер автентифікації перевіряє справжність клієнта й інформує ТД про дозвіл або заборону надання доступу клієнту до мережі. У ході перевірки сервер передає клієнту унікальний ідентифікатор сесії (Master Session Key, MSK). На його основі станція та сервер генерують секрет PMK (Pairwise Master Key). Сервер передає PMK точці доступу.

Генерація парних ключів між ТД та станцією є останньою фазою автентифікації 802.1X, її називають «чотирьохстороннє рукостискання» (4–Way Handshake).

У результаті вдалого виконання цієї фази клієнт та точка доступу формують парний тимчасовий ключ (Pairwise Transient Key, PTK) та груповий тимчасовий ключ (Group Temporary Key, GTK).

Для захисту від модифікації даних під час обміну в процедурі «чотирьохстороннього рукостискання» використовується механізм криптографічного підпису, який отримав назву MIC (Message Integrity Check).

Існує атака на чотирьохстороннє рукостискання KRACK (Key Reinstallation Attack), яку відкрили в 2016 році Метью Ванхоф (Mathy Vanhoef) та Френк Піссен (Frank Piessens). Атака описана у [21]. У сценарії KRACK зловмисник повинен зайняти позицію посередника між клієнтом та ТД та перебувати в межах цільової мережі (Online).

Атака досить складна, її важко виконувати в реальних умовах. Загрозу атака містить лише за автентифікації PSK. Упровадження захисту від атаки залежить від рішення конкретних розробників.

Автентифікація на основі попередньо встановлених ключів. У стандарті 802.11i передбачений спеціальний режим для невеликих мереж, де не використовується сервер автентифікації. У разі застосування цього режиму взаємна автентифікація станції й мережі здійснюється за допомогою попередньо встановлених ключів (Pre–Shared key, PSK);

У цьому методі автентифікація проходить між станцією та ТД. З обох сторін має бути встановлена парольна фраза (PassPhrase). Секрет PSK формується на основі парольної фрази та ідентифікатора точки доступу (Service Set Identifier – SSID).

Цей метод автентифікації вразливий до атаки KRACK. Треба зазначити, що вплив атаки KRACK на мережі з автентифікацією PSK більш руйнівний, ніж на мережі з автентифікацією 802.1X, де для кожної сесії оновлюється комплект секретних ключів [11].

Головний недолік методу PSK полягає в тому, що парольна фраза однакова для всіх пристроїв. Отже, її розкриття дозволяє зловмиснику маніпулювати всією інформацією, що циркулює в бездротовій мережі. Через це з'являється можливість атаки на парольну фразу.

Інший варіант цієї атаки – атака на параметр PMK Identifier (PMKID) – описаний у [10]. Для протидії цій атаці достатньо використовувати складний пароль (більше 15 символів зламати майже неможливо).

Швидкий перехід BSS. Швидкий перехід BSS також відомий як швидкий роумінг. Цей тип автентифікації описаний у стандарті IEEE 802.11r–2008. Його створено для перемикання мобільного клієнтського пристрою між точками доступу в межах однієї ESS без втрати з'єднання з мережею.

Стандарт IEEE 802.11r Fast BSS Transition (FT) дозволяє пришвидшити повторне під'єднання. Матеріал для формування PTK передається елементом Fast Transition Information Element (FTIE) всередині кадрів ав-

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

тентифікації й повторної асоціації стандарту 802.11.

Існує різновид атаки KRACK на автентифікацію 802.11r [21]. При цьому зловмиснику не потрібно займати позицію посередника.

Автентифікація з використанням пароля. У найбільш сучасному стандарті захисту бездротових мереж WPA3 використовують метод автентифікації, який має назву SAE (Simultaneous Authentication of Equals – одночасна автентифікація рівних). Цей метод базується на протоколі узгодження ключів Діффі–Геллмана (Diffie–Hellman). На відміну від інших протоколів автентифікації, у SAE сторони обміну є рівними. Теоретично кожна сторона може ініціювати протокол. На відміну від послідовного обміну повідомленнями PSK автентифікації, цей метод унеможливлює виконання атаки типу KRACK.

Процес автентифікації SAE наведено на рис. 3.

Протокол SAE має такі властивості:

– учасники взаємодії отримують ключ PMK;

– зловмисник не в змозі визначити пароль, або PMK, спостерігаючи за обміном або втручаючись у процес;

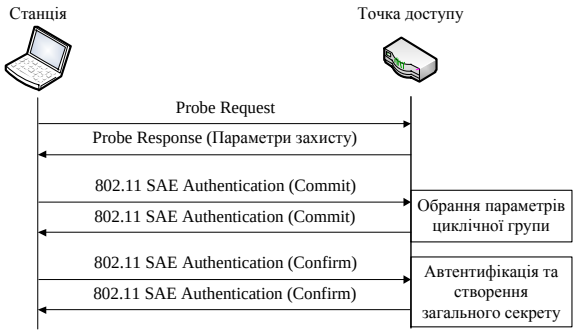

Рис. 3. Процес автентифікації SAE

Fig. 3. SAE authentication process

– зловмисник не в змозі зробити більше ніж одну здогадку про пароль за атаку. Це означає, що зловмисник не може зібрати дані, а потім в автоматичному режимі підбирати пароль за словником;

– розкриття PMK сесії не надає жодних переваг зловмиснику, який намагається визначити пароль, або PMK, від будь-якої іншої сесії.

Дослідники Метью Ванхоф та Еял Ронен (Eyal Ronen) виявили ряд недоліків у новій технології. Ці недоліки отримали загальну назву Dragonblood. Інформація про них була опублікована в 2019 році [22]. Wi–Fi Alliance розробили рекомендації [24] для протидії знайденим уразливостям. Розробники запропонували такі атаки:

– пониження рівня захисту й атака за словником;

– пониження рівня захисту групи;

– атака сторонніми каналами (side-channel) на основі часових затримок;

– атака сторонніми каналами на основі кеш-пам’яті;

– атака відмови в доступі.

Механізми гарантування безпеки інформаційного обміну. У початковій версії стандарту 802.11 [10] (Wired Equivalent Privacy – WEP) запропоновано два режими роботи: без шифрування та з використанням протоколу шифрування WEP.

Визначено дві версії протоколу: WEP–40 і WEP–104. Різниця була в довжині ключа: 40 і 104 біт відповідно. Разом із ключем використовується вектор ініціалізації (Initialization vector, IV) розміром 24 біти. Його можна встановити до чотирьох ключів.

В основі шифрування лежить потоковий шифр RC4 (Rivest cipher).

Перша серйозна вразливість шифру RC4 опублікована ще в 2001 році [7] Флурером (Fluhrer S.), Мантіном (Mantin I.) і Шаміром (Shamir A.). На основі вразливості створена атака [18].

Далі було розроблено ще велику кількість атак на цей протокол, наприклад, [6, 20].

WEP має безліч слабких місць:

– слабкий механізм автентифікації;

– некриптографічний механізм перевірки цілісності;

– відсутній механізм захисту від повторів (replay);

– мала розрядність секрету (ключа) й вектора ініціалізації;

– секрет використовується як ключ шифрування напряму;

– відсутній механізм керування ключами;

– вразливий алгоритм шифрування.

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

У наш час злам захисту WEP виконують протягом однієї хвилини [19], і використання цього протоколу еквівалентне незахищеній мережі.

Розуміючи важливість гарантування безпеки в бездротових мережах, у 2000 році об'єднання Wi–Fi Alliance розпочало програму сертифікації, яка мала би визначити вимоги до безпеки в мережах Wi–Fi. У 2003 році Wi–Fi Alliance представляє програму сертифікації WPA – Wi–Fi Protected Access. Серед нововведень були такі:

– нові методи автентифікації RSN: IEEE 802.1X, PSK;

– новий протокол для шифрування TKIP;

– ієрархії парних та групових ключів.

TKIP (Temporal Key Integrity Check – протокол цілісності тимчасового ключа) розроблений для посилення захисту пристроїв, апаратна частина яких підтримує лише протокол WEP. Посилює протокол WEP за рахунок використання криптографічного механізму гарантування цілісності даних MIC, а також перемішування ключових даних під час створення ключа шифрування.

Поява WPA не змогла повноцінно захистити мережу від вразливостей, знайдених у протоколі WEP, проте захист став більш надійним і змусив шукати нові підходи для проведення атак.

У 2008 році Мартін Бек (Martin Beck) та Ерік Тьюз (Erik Tews) знайшли спосіб нападу на WPA [19]. Атака використовує слабкі місця протоколу TKIP для розшифрування пакетів протоколу ARP (Address Resolution Protocol) та введення додаткового трафіка в мережу. Це дозволяє виконувати атаки типу «відмова в доступі» (Denial of Service, DoS), або «отруєння ARP» (ARP–poisoning). Пакети ARP обрані через прогнозованість значення більшості їх полів.

Атака потребує багато часу. Інструмент для виконання атаки – Aircracking. Для захисту достатньо встановити час оновлення ключа PTK менше 15 хвилин.

У 2014 році дослідники виявили у стандарті WPA вразливість Hole196 (ключовий потік RC4 значною мірою залежний від значення двох молодших байт TSC) і запропонували статистичну атаку [15]. Вразливість Hole196 дозволяє розшифровувати весь трафік користувача, який надсилається від клієнта до шлюзу мережі.

Для захисту можна використати: клієнтські системи виявлення атак; ізоляцію клієнтів; сегментацію (точка доступу створює окремі BSS для різних користувачів).

Підсумуємо позитивні зміни, надані стандартом WPA:

– набагато краще захищені механізми автентифікації;

– криптографічний алгоритм перевірки цілісності Michael;

– для захисту від повторення кадрів використовується лічильник TSC;

– визначено ієрархії парних та групових ключів;

– визначено механізм керування ключами.

Підсумуємо недоліки:

– використовується вразливий метод шифрування RC4;

– алгоритм перевірки цілісності Michael має вади, які дозволяють дізнатися ключ автентифікації даних;

– механізми автентифікації 802.1X та PSK мають недоліки, які можуть бути використані для розкриття ключів;

– протокол TKIP вразливий до наслідків атаки KRACK;

– стандарт IEEE 802.11i має концептуальну вразливість Hole196.

У 2004 році був ратифікований стандарт IEEE 802.11i [8] (WPA2). У ньому впроваджені нововведення, які майже цілком усунули вразливості протоколу WEP. Стандарт WPA2 використовує протоколи автентифікації 802.1X та PSK.

Основним нововведенням став новий протокол шифрування CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol – протокол блочного шифрування з кодом автентичності повідомлення MAC і режимом зчеплення блоків і лічильника). Як блоковий шифр використовується шифр AES (Advantes Encrypt Standard) – стандарт блокового шифрування, який використовує вхідні блоки розміром 128 біт та ключі шифрування довжиною 128, 192 та 256 біт. У [13] офіційно доведено високу захищеність протоколу CCMP.

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

Згідно з [8], протокол CCMP регламентує використання нового ключа шифрування для кожної сесії та унікальні дані (Nonce) для кожного кадру. Для цього застосовують лічильник пакетів (Packet Number, PN). PN має розмір 48 біт і забезпечує захист від атаки повторення.

У 2014 році із впровадженням стандарту IEEE 802.11ac з'явилася потреба в більш швидкому протоколі шифрування. Це протокол GCMP, який заснований на використанні режиму GCM (Galois Counter Mode) шифру AES. На відміну від режиму CCM, який визнано стійким, режим GCM, навпаки, визнають досить слабким та ненадійним [9].

Програма сертифікації WPA2 витіснила вразливості, які були знайдені в протоколах шифрування WEP та TKIP, однак залишилася вразливою до атак проти методів автентифікації 802.1X та PSK. Актуальною є вразливість Hole196, оскільки це фундаментальна вразливість усього стандарту 802.11i. Використання механізму WPS надзвичайно послаблює захищеність мережі. Актуальною залишається й атака KRACK. Її вплив на можливості зловмисника за використання протоколу CCMP мінімальний, проте GCMP дуже вразливий до цієї атаки.

Незважаючи на всі виявлені вразливості, розробники активно створюють рекомендації щодо їх нейтралізації. Мережу, захищену за стандартом WPA2, можливо налаштувати таким чином, щоб гарантувати високий рівень безпеки для користувачів.

Підсумуємо позитивні зміни, надані стандартом WPA2:

– захищений алгоритм блочного шифрування CCMP;

– надійний механізм підтвердження автентичності даних.

Підсумуємо недоліки:

– механізми автентифікації 802.1X та PSK мають недоліки, які можуть бути використані для розкриття ключів;

– протокол GCMP має вади і вразливий до наслідків атаки KRACK;

– стандарт IEEE 802.11i має концептуальну вразливість Hole196.

Новітні методи захисту. Вразливості та можливі атаки, які накопичилися з моменту появи стандарту WPA2, змусили об'єднання Wi–Fi Alliance приступити до розробки серії нових стандарт сертифікації. Анонс нових стандартів відбувся у 2018 році. Серед нововведень можна виділити такі:

– WPA3–Personal для автентифікації використовує протокол SAE замість 4-стороннього рукостискання;

– WPA3–Enterprise використовує протоколи EAP зі збільшеними ключами шифрування (еквівалент 192-бітної безпеки);

– програма сертифікації відкритих мереж Wi–Fi Enhanced Open (WEO);

– метод спрощеного під'єднання до мережі Wi–Fi Easy Connect (WEC);

– захист кадрів управління Management Frame Protection (MPF).

Програма сертифікації WEO описана у [23] і має замінити публічні мережі Wi–Fi, у яких вся інформація шифрувалася відомим усім ключем, та відкриті мережі, де шифрування відсутнє. Стандарт WEO використовує механізм Opportunistic Wireless Encryption (OWE), який описаний у документі RFC 8110. Під'єднання до мережі за протоколом OWE наведено на рис. 4.

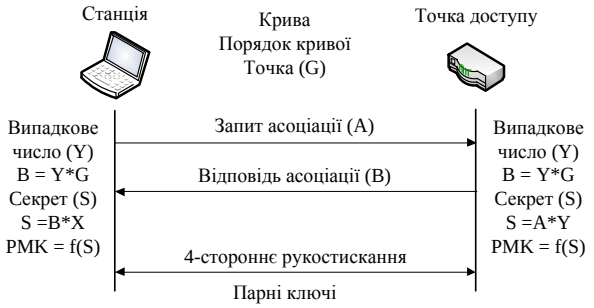

Рис. 4. Під'єднання до мережі за протоколом OWE

Fig. 4. OWE network connection

Під час використання режиму OWE користувач не повинен вводити пароль. Створення ключів відбувається за алгоритмом Діффі–Геллмана на основі еліптичних кривих. Протокол реалізує механізм автентифікації, який не дозволяє виконати атаку MITM (Mem In The Middle – людина посередині) під час приєднання клієнта до мережі й отримувати доступ до всього трафіка, який проходить між клієнтом і ТД.

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

Стандарт WEO не є частиною WPA3, проте знайшов широку підтримку серед розробників бездротового забезпечення.

На заміну мережам WPA2–Personal, заснованим на вразливій автентифікації PSK, у мережах WPA3–Personal використовується механізм автентифікації SAE. Він призначений прибирати всі вразливості, знайдені в 4-сторонніх рукостисканнях автентифікації PSK, і повинен гарантувати високий рівень захищеності навіть за використання слабкого пароля [25]. Режим WPA3–Personal уже активно впроваджують розробники у сфері бездротових мереж. Загалом стандарт сертифікації WPA3–Personal надає користувачам такі можливості:

– дозволяє встановлювати легкі паролі, які легше запам’ятати;

– забезпечує посилений захист без зміни способу під’єднання користувача до мережі (на стороні інтерфейсу користувача);

– механізм perfect forward secrecy, який гарантує, що навіть якщо ключ буде скомпрометовано, зловмисник не зможе розшифрувати дані, які були передані раніше.

У WPA3–Enterprise, згідно з [25], застосовують рекомендації Commercial National Security Algorithms (CNSA), що означає гарантування еквівалента 192-бітної безпеки на етапі автентифікації. Повноцінна реалізація та впровадження WPA3–Enterprise планується протягом кількох років. Цей режим, порівняно з WPA2–Enterprise, передбачає такі зміни:

– шифрування (використовується протокол GCMP–256);

– встановлення та автентифікація ключів (використовується еліптична крива Діффі–Геллмана (Elliptic Curve Diffie–Hellman, ECDH) та алгоритм підпису на еліптичних кривих (Elliptic Curve Digital Signature Algorithm, ECDSA) з використанням 384-бітної еліптичної кривої);

– захист кадрів управління MFP (використовується 256-розрядний Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP–GMAC–256), що запобігає маніпуляціям із кадрами управління).

Основні виявлені на цей момент вразливості пов’язані з протоколом автентифікації SAE.

Незважаючи на виявлені вразливості, стандарт WPA3 має суттєво підняти рівень захищеності в мережах із режимом Enterprise. Поліпшення в мережах із режимом Personal досить двоякі, через виявлення слабкостей протоколу SAE.

Підсумуємо позитивні зміни, надані стандартом WPA3:

– підвищена розрядність ключів шифрування для режиму WPA3–Enterpise;

– новий метод автентифікації SAE вирішив проблеми, які були актуальними для автентифікації PSK;

– кадри управління отримали додатковий механізм захисту.

Підсумуємо недоліки:

– метод автентифікації SAE має ряд вразливостей, які повині бути виправлені конкретними розробниками;

– багато корисних технологій та ідей винесено в окремі стандарти.

Демонстраційна програма. Для забезпечення наочного демонстрування механізму найбільш розповсюджених атак на мережу Wi–Fi було розроблено демонстраційну програму [5], яка дає змогу моделювати атаки. Для цього в програмі обрано стандарт сертифікації WPA2 з механізмом автентифікації PSK та механізмом криптографічного захисту CCMP–128. Для демонстрації в програмі обрано такі атаки: атаку на пароль на етапі 4-стороннього рукостискання на основі параметру PMKID та атаку KRACK.

У процесі моделювання надається можливість користуватися механізмами захисту стандарту WPA2. Користувач може переконатися, що його помилкові дії, наприклад, вибір невдалого пароля, дають змогу зловмиснику провести вдалу атаку. У той же час програма демонструє, що за умови правильних дій користувача атаці зловмисника запобігають засобами стандарту захисту.

Результати

У результаті аналізу ряду літературних джерел було порівняно стандарти захисту мережі Wi–Fi, показано можливі типи атак на ці стандарти, засоби, які допомагають зменшити ризики цих атак, розроблено рекомендації щодо використання стандартів під час експлуатації ме-

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

реж Wi–Fi. Порівняння стандартів захисту мереж Wi–Fi наведено в табл. 1.

Розроблено імітаційну програмну модель атак на засоби захисту бездротової мережі Wi–Fi, яка дозволяє продемонструвати можливість атак за умови помилок користувача та запобігання атакам за умови правильних дій користувача.

Наукова новизна та практична значимість

Проведено порівняння стандартів захисту бездротової мережі Wi–Fi, включаючи найбільш сучасні механізми захисту цих стандартів. Проаналізовано атаки на механізми захисту мережі Wi–Fi та механізми протидії цим атакам. В оригінальній програмній моделі показано, як помилкові дії користувача допомагають зловмиснику подолати сучасні механізми захисту.

Рекомендації щодо використання окремих засобів захисту бездротових мереж Wi–Fi можуть бути використані під час побудови системи захисту окремих елементів автоматизованих систем залізничного транспорту. Демонстраційна модель атаки на мережу Wi–Fi може бути використана в навчальному процесі для підготовки фахівців у галузі кібербезпеки.

Висновки

Мережі Wi–Fi є перспективними для їх застосування в автоматизованих системах залізничного транспорту. Проаналізовано стандарти механізмів захисту, які використовуються в мережах Wi–Fi на різних етапах роботи, їх вразливості та наявні методики атак. Загальновідомо, що перший стандарт захисту WEP (IEEE 802.11) має багато вразливостей і не може бути рекомендований для застосування. Щодо сімейства стандартів WPA зроблено такі висновки:

Таблиця 1

Порівняння стандартів захисту мереж Wi–Fi

Table 1

Comparison of Wi–Fi protection standards

	WEP	WPA	WPA2	WPA3
Загальний опис	Перший протокол захисту мереж Wi–Fi	Посилення захисту без заміни обладнання. Нові протоколи автентифікації	Новий протокол шифрування	Посилення ключів. Заміна протоколу автентифікації PSK
На якому документі засновано	IEEE 802.11–1997	Початкова версія IEEE 802.11i	IEEE 802.11i–2004	WPA3 Specification Version 1.0
Автентифікація	Open system Shared key	Enterprise – 802.1X Personal – PSK	Enterprise – 802.1X Personal – PSK	Enterprise – 802.1X Personal – SAE
Шифрування	Шифр RC4	TKIP (шифр RC4)	CCMP / GCMP (шифр AES)	CCMP / GCMP (шифр AES)
Ключ шифрування, біт	64 / 128	128	128 / 256	128 / 256
Захист цілісності (автентичності) даних	CRC–32 (32 біт)	Michael (64 біт)	CBC-MAC (64 / 128 біт) / GCM (128 біт)	CBC-MAC (64 / 128 біт) / GCM (128 біт)

doi: https://doi.org/10.15802/stp2020/213042

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 4 (88)

Продовження табл. 1

Continuation of Table 1

	WEP	WPA	WPA2	WPA3
Захист цілісності (автентичності) даних	CRC–32 (32 біт)	Michael (64 біт)	CBC-MAC (64 / 128 біт) / GCM (128 біт)	CBC-MAC (64 / 128 біт) / GCM (128 біт)
Додатковий захист керуючих кадрів	–	Management Frame Protection (не обов'язково)	Management Frame Protection (не обов'язково)	Management Frame Protection
Управління ключами	–	802.1X / 4-way handshake	802.1X / 4-way handshake	802.1X / SAE
Захист від атак повторення (reply)	–	Лічильник послідовності транзакцій (48 біт)	Номер пакета (48 біт)	Номер пакета (48 біт)
Можливі атаки	Відновлення ключа; атака фрагментації; Chop–Chop; DoS	Бека і Тьюза; Охігаші і Морі; KRACK; підбір пароля за словником; Hole196; DoS	KRACK; підбір пароля за словником; Hole196; DoS	Пониження до WPA2; пониження групи сторонніми каналами; DoS
Рівень безпеки	Не захищено	Слабкий / Середній	Середній / Високий	Високий

1. Кожний стандарт безпеки Wi–Fi визначає ряд компонентів захисту: протоколи автентифікації та їх параметри, протоколи шифрування та їх параметри, додаткові механізми забезпечення безпеки. Саме на захищеності вказаних компонентів може бути визначена захищеність самого стандарту.

2. Стандарт WPA (WPA1) регламентує використання протоколу автентифікації IEEE 802.1X із сервером автентифікації й спрощеного режиму PSK. Протокол 802.1X, за використання ненадійних протоколів сімейства EAP (LEAP, EAP–FAST), уразливий до крадіжки пароля. Протокол PSK уразливий до декількох типів атаки на пароль та атаки перевстановлення ключа KRACK, яка дозволяє розшифровувати й підробляти пакети в мережі.

3. Від атак на режим PSK протоколу WPA можна захиститися за допомогою надійного пароля й програмно-технічних засобів, у яких застосовані рекомендації розробників IEEE 802.11 (Wi–Fi) з нейтралізації атаки KRACK.

4. Для шифрування стандарт WPA визначає протокол TKIP, який є надбудовою над уразливим потоковим шифром WEP. TKIP забезпечує криптографічний захист цілісності повідомлень за алгоритмом Michael. Алгоритм уразливий, що дозволяє роздобути ключ підпису даних і підробляти повідомлення. Повноцінного захисту від уразливостей протоколу TKIP досягти не можна.

5. Стандарт WPA2 використовує протоколи автентифікації, аналогічні WPA, а також успадковує всі супутні вразливості. Стандарт регламентує використання блокових протоколів шифрування CCMP і GCMP. Кожний із протоколів забезпечує захист цілісності повідомлень і надійне шифрування. Багато дослідників указують на потенційні слабості протоколу GCMP. Використання атаки KRACK дозволяє реалізувати ці слабості, що веде до розкриття інформації, підроблення повідомлень.

6. Стандарт WPA3 регламентує використання механізму захисту кадрів керування, який раніше не був обов'язковим, що приводило до можливості маніпуляції зловмисником діями учасників мережі. Режим автентифікації PSK може бути замінений на автентифікацію SAE. Протокол SAE дозволяє забезпечити високий рівень захищеності навіть за слабких паролів,

doi: https://doi.org/10.15802/stp2020/213042

а також запобігає вразливостям режиму PSK. Дослідники виявили ряд уразливостей цього протоколу (Dragonblood), однак усі ці вразливості не критичні.

7. У протоколі SAE змінений підхід до генерації парних тимчасових ключів. Замість використання функцій кешування в SAE використовується криптографія на еліптичних кривих. Для захисту автентифікації стандарт 802.1X регламентує використання лише таких реалізацій протоколу EAP, криптостійкість яких еквівалентна 192-бітному захисту.

8. Спочатку в стандарт WPA3 планували включити ряд корисних нововведень, наприклад: заміна автентифікації PSK на SAE, захист кадрів керування, заміна вразливого WPS, збільшення розміру ключів шифрування й посилений захист у відкритих мережах. У робочій специфікації більшість обіцяних функцій стали необов’язкові або були випущені як окремі стандарти, не пов'язані з WPA3.

9. У ході аналізу визначено, що новий стандарт WPA3 дозволить підвищити рівень захисту мереж Wi–Fi, але не дає можливості гарантувати повноцінну безпеку у зв’язку з необов’язковістю застосування декількох важливих поліпшень. Рівень безпеки буде варіюватися залежно від реалізації конкретного виробника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранова Е. А., Зарешин С. В. Анализ защищенности беспроводных клиентов. *Современные информационные технологии и ИТ-образование*. 2018. Т. 14, № 4. С. 938–946. DOI: https://doi.org/10.25559/SITITO.14.201804.938-946
2. Интеллектуальная сеть Wi-Fi для транспортных систем. URL: https://deps.ua/system-integration/wireless-solutions/wi-fi/transport.html (дата звернення: 15.05.2020).
3. Куприяновский В. П., Суконников Г. В., Синягов С. А., Намиот Д. Е., Евтушенко С. Н., Федорова Н. О. Интернет цифровой железной дороги. *International Journal of Open Information Technologies*. 2016. Vol. 4, № 12. С. 53–68.
4. Морозов А. В., Шахов В. Г. Анализ безопасности доступа беспроводных сетей по технологии wi-fi, применяемой в объектах инфраструктуры железнодорожного транспорта. *Известия Транссиба.* 2014. № 3 (19). С. 92–96.
5. Педенко І. О. *Дослідження і розробка демонстраційної програми захисту бездротових мереж : дипломна робота*. Дніпро, 2019. 130 с.
6. Bittau A., Handley M., Lackey J. The Final Nail in WEP’s Coffin. *2006 IEEE Symposium on Security and Privacy* (Berkeley/Oakland, 21–24 May 2006). Oakland, 2006. P. 386–400. DOI: https://doi.org/10.1109/SP.2006.40
7. Fluhrer S., Mantin I., Shamir A. *Weaknesses in the Key Scheduling Algorithm of RC4.* Lecture Notes in Computer Science. 2001. Vol. 2295. P. 1–24. DOI: https://doi.org/10.1007/3-540-45537-X_1
8. Frankel S., Eydt B., Owens L., Kent K. *Establishing Wireless Robust Security Networks : A Guide to IEEE 802.11i.* Gaithersburg, 2006. 156 p.
9. Gueron S., Krasnov V. The Fragility of AES-GCM Authentication Algorithm. *2014 11th International Conference on Information Technology : New Generations*. (Las Vegas, 7–9 April 2014). Nevada, 2014. P. 333–337. DOI: https://doi.org/10.1109/ITNG.2014.31
10. IEEE 802.11-1999 – 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. URL: https://standards.ieee.org/standard/802_11-1999.html#Additional
11. IEEE 802.11ah-2016 – 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 Amendment 2 : Sub 1 GHz License Exempt Operation. DOI: https://doi.org/10.1109/IEEESTD.2017.7920364. URL: https://ieeexplore.ieee.org/document/7920364
12. 802.1X-2010 – IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control. URL: https://standards.ieee.org/standard/802_1X-2010.html
13. Jonsson J. On the Security of CTR + CBC-MAC. *Lecture Notes in Computer Science.* 2003. Vol. 2595. P. 76–93. DOI: https://doi.org/10.1007/3-540-36492-7_7

doi: https://doi.org/10.15802/stp2020/213042

14. Pakhomova V. M., Nazarova D. I. Organizing Wireless Network at Marshalling Yards Using the Bee Method. *Наука та прогрес транспорту*. 2020. № 2 (86). P. 60–73. DOI: https://doi.org/10.15802/stp2020/204005
15. Paterson K. G., Poettering B., Schuldt J. C. N. Plaintext Recovery Attacks Against WPA/TKIP. *Lecture Notes in Computer Science*. 2015. Vol. 8540. P. 325–349. DOI: https://doi.org/10.1007/978-3-662-46706-0_17
16. Positive Train Control (PTC) : Overview and Policy Issues. Congressional Research Service. URL: https://crsreports.congress.gov (дата звернення: 15.05.2020).
17. Steube J. New attack on WPA/WPA$_2$ using PMKID. *Hashcat : website.* URL: https://hashcat.net/forum/thread-7717.html (дата звернення: 15.05.2020).
18. Stubblefield A., Ioannidis J., Rubin A. D. *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.2068&rep=rep1&type=pdf (дата звернення: 15.05.2020).
19. Tews E., Beck M. Practical attacks against WEP and WPA. *Proceedings of the second ACM conference on Wireless network security – WiSec '09* (Zurich, March 2009). Zurich, 2009. P. 79–86. DOI: https://doi.org/10.1145/1514274.1514286
20. Tews E., Weinmann R.-P., Pyshkin A. Breaking 104 BIT WEP in Less Than 60 Seconds. *Lecture Notes in Computer Science.* 2007. Vol. 4867. P. 188–202. DOI: https://doi.org/10.1007/978-3-540-77535-5_14
21. Vanhoef M., Piessens F. Key Reinstallation Attacks : Forcing Nonce Reuse in WPA$_2$. *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (Dallas, October 2017). Dallas, 2017. P. 1313–1328. DOI: https://doi.org/10.1145/3133956.3134027
22. Vanhoef M., Ronen E. Dragonblood : Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. *2020 IEEE Symposium on Security and Privacy (SP)* (San Francisco, 18–21 May 2020). San Francisco, 2020. P. 517–533. DOI: https://doi.org/10.1109/sp40000.2020.00031
23. Wi-Fi CERTIFIED Enhanced Open delivers data protection in open Wi-Fi networks : web-site. URL: https://cutt.ly/9fRxxoT (дата звернення: 15.05.2020).
24. WPA3 Security Considerations. *Wi-Fi Alliance*. 2019. P. 1–7.
25. WPA3 Specification Version 1.0. *Wi-Fi Alliance*. 2018. P. 1–7.

И. В. ЖУКОВИЦКИЙ[1*], И. А. ПЕДЕНКО[2*]

[1*]Каф. «Электронные вычислительные машины», Днипровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днипро, Украина, 49010, тел. +38 (056) 373 15 89, эл. почта ivzhukl@ua.fm, ORCID 0000-0002-3491-5976

[2*]Каф. «Электронные вычислительные машины», Днипровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днипро, Украина, 49010, тел. +38 (056) 373 15 89, эл. почта actek98@gmail.com, ORCID 0000-0001-8130-2657

АНАЛИЗ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ WI–FI В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Цель. В работе предусмотрено: проанализировать основные механизмы защиты, имеющиеся в беспроводных сетях Wi–Fi; показать механизмы атак на эти средства защиты; выполнить сравнительный анализ эффективности механизмов защиты, предоставить рекомендации для использования этих механизмов в автоматизированных системах железнодорожного транспорта; построить демонстрационную модель атак на средства защиты беспроводной сети Wi–Fi. **Методика.** На основании обзора значительного количества отечественных и заграничных источников проведен сравнительный анализ механизмов защиты беспроводной сети Wi–Fi, в которых проанализированы отдельные стандарты защиты, выявлены их сильные и слабые стороны. Показаны разнообразные атаки на средства аутентификации и механизмы обеспечения безопасности информационного обмена. Для демонстрации атаки на эти средства защиты разработан алгоритм демонстрационной имитационной модели работы протокола защиты WPA2 с возможностью проведения атак на этот протокол. **Результаты.** Выполнен сравнительный анализ основных стандартов механизмов защиты беспроводной сети Wi–Fi, в частности WEP, WPA, WPA2, WPA3. Продемонстрировано разные атаки на эти стандарты. Показано преимущество и слабости отдельных механизмов средств защиты, предо-

doi: https://doi.org/10.15802/stp2020/213042

ставлены рекомендации для их использования. Построена демонстрационная модель атак на механизмы защиты беспроводной сети, которая показывает такие атаки, как атака на парольную фразу и атака KRACK. Для демонстрации в программе избран стандарт WPA2 с механизмом аутентификации PSK и механизмом криптографической защиты CCMP–128. **Научная новизна.** Приведен широкий спектр механизмов защиты беспроводной сети Wi–Fi, показаны возможности отдельных механизмов защиты, проведено сравнение стандартов защиты сети. В оригинальной программной модели показано, как ошибочные действия пользователя помогают злоумышленнику преодолеть современные механизмы защиты. **Практическая ценность.** Рекомендации относительно использования отдельных средств защиты беспроводных сетей Wi–Fi могут быть использованы при построении системы защиты отдельных элементов автоматизированных систем железнодорожного транспорта. Демонстрационная модель атаки на сеть Wi–Fi может быть использована в учебном процессе для подготовки специалистов в области кибербезопасности.

Ключевые слова: сеть Wi–Fi; стандарты защиты; безопасность; аутентификация; шифрование

I. V. ZHUKOVYTS'KYI[1*], I. A. PEDENKO[2*]

[1*]Dep. «Electronic Computing Machines», Dnipro National University of Railway Transport named after Academician V. Lazaryan, Lazaryana St., 2, Dnipro, Ukraine, tel. +38 (056) 373 15 89, e-mail ivzhukl@ua.fm, ORCID 0000-0002-3491-5976
[2*]Dep. «Electronic Computing Machines», Dnipro National University of Railway Transport named after Academician V. Lazaryan, Lazaryana St., 2, Dnipro, Ukraine, tel. +38 (056) 373 15 89, e-mail actek98@gmail.com, ORCID 0000-0001-8130-2657

WIRELESS WI-FI SECURITY ANALYSIS IN AUTOMATED RAILWAY SYSTEMS

Purpose. The article is aimed to analyze the basic security mechanisms available in Wi-Fi networks; show the mechanisms for attacking these defenses; carry out a comparative analysis of the effectiveness of protection mechanisms; provide recommendations for the use of these mechanisms in automated rail transport systems; build a demonstration model of attacks on Wi–Fi network security. **Methodology**. Based on the review of a significant number of domestic and foreign sources, a comparative analysis of the security mechanisms of the Wi–Fi network is carried out, where individual protection standards are analyzed, their strengths and weaknesses appear. A variety of attacks on authentication tools and mechanisms for ensuring the security of information exchange are shown. To demonstrate an attack on these security features, an algorithm has been developed for a demonstration simulation model of the WPA2 security protocol with the ability to attack this protocol. **Findings.** The basic standards of Wi–Fi security mechanisms have been compared. In particular, WEP, WPA, WPA2, WPA3. Different attacks on these standards have been demonstrated. The advantages and weaknesses of individual mechanisms of protective means are shown, recommendations for their use are provided. A demonstration model of attacks on wireless network protection mechanisms has been built, which demonstrates such attacks as an attack on a passphrase and a KRACK attack. To demonstrate in the program, the WPA2 standard with the PSK authentication mechanism and the cryptographic protection mechanism CCMP-128 is chosen. **Originality.** A wide range of Wi–Fi network security mechanisms is presented, the capabilities of individual security mechanisms are shown, and Wi–Fi network security standards are compared. The original software model shows how erroneous user actions help an attacker overcome modern security mechanisms. **Practical value.** Recommendations for the use of separate Wi-Fi security features can be used to build a security system for individual components of automated rail systems. A demonstration model of an attack on a Wi-Fi network can be used in a training process to train cybersecurity specialists.

Keywords: Wi–Fi network; security standards; security; authentication; encryption

REFERENCES

1. Baranova, Ye. A., & Zareshin, S. V. (2018). Analiz zashchishchennosti besprovodnykh klientov. *Modern Information Technologies and IT-education, 14*(4), 938-946. DOI: http://dx.doi.org/10.25559/sitito.14.201804.938-946 (in Russian)
2. Intellektualnaya set wi-fi dlya transportnykh sistem. Retrieved from https://deps.ua/system-integration/wireless-solutions/wi-fi/transport.html (in Russian)

doi: https://doi.org/10.15802/stp2020/213042

3. Kupriyanovsky, V. P., Sukonnikov, G. V., Sinyagov, S. A., Namiot, D. Ye., Evtushenko, S. N., & Fedorova, N. O. (2016). On internet of digital railway. *International journal of open information technologies, 4*(12), 53-68 (in Russian)
4. Morozov, A. V., & Shakhov, V. G. (2014). Analiz bezopasnosti dostupa besprovodnykh setey po tekhnologii wi-fi, primenyaemoy v obektakh infrastruktury zheleznodorozhnogo transporta. *Journal of transsib railway studies, 3*(19), 92-96. (in Russian)
5. Pedenko, I. O. (2019). *Doslidzhennia i rozrobka demonstratsiinoi prohramy zakhystu bezdrotovykh merezh: dyplomna robota*. Dnipro. (in Ukrainian)
6. Bittau, A., Handley, M., & Lackey, J. (2006, May). The final nail in wep's coffin. *2006 IEEE Symposium on Security and Privacy* (pp. 386-400). Oakland, USA. DOI: https://doi.org/10.1109/sp.2006.40 (in English)
7. Fluhrer, S., Mantin, I., & Shamir, A. (2001). *Weaknesses in the key scheduling algorithm of RC4.* Lecture notes in computer science. (pp. 1-24). DOI: https://doi.org/10.1007/3-540-45537-x_1 (in English)
8. Frankel, S., Eydt, B., Owens, L., & Kent, K. (2006). *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*. Gaithersburg. (in English)
9. Gueron, S., & Krasnov, V. (2014). The Fragility of AES-GCM Authentication Algorithm. *2014 11th International Conference on Information Technology: New Generations* (pp. 333-337). Nevada, USA. DOI: https://doi.org/10.1109/itng.2014.31 (in English)
10. IIEEE 802.11-1999-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. Retrieved from https://standards.ieee.org/standard/802_11-1999.html#additional (in English)
11. IEEE 802.11ah-2016-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 Amendment 2: Sub 1 GHz License Exempt Operation. DOI: https://doi.org/10.1109/ieeestd.2017.7920364. Retrieved from https://ieeexplore.ieee.org/document/7920364 (in English)
12. 802.1X-2010-IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control. Retrieved from https://standards.ieee.org/standard/802_1x-2010.html (in English)
13. Jonsson, J. (2003). On the Security of Ctr + CBC-MAC. *Lecture Notes In Computer Science, 2595*, 76-93. DOI: https://doi.org/10.1007/3-540-36492-7_7 (in English)
14. Pakhomova, V. M., & Nazarova, D. I. (2020). Organizing Wireless Network at Marshalling Yards Using the Bee Method. *Science and Transport Progress, 2*(86), 60-73. doi: https://doi.org/10.15802/stp2020/204005 (in English)
15. Paterson, K. G., Poettering, B., & Schuldt, J. C. N. (2015). Plaintext Recovery Attacks Against WPA/TKIP. *Lecture Notes in Computer Science, 8540*, 325-349. DOI: https://doi.org/10.1007/978-3-662-46706-0_17 (in English)
16. Positive Train Control (PTC): Overview and Policy Issues. Congressional Research Service. Retrieved from https://crsreports.congress.gov (in English)
17. Steube, J. New attack on WPA/WPA$_2$ using PMKID. *Hashcat: website*. Retrieved from https://hashcat.net/forum/thread-7717.html (in English)
18. Stubblefield, A., Ioannidis, J., & Rubin, A. D. *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.2068&rep=rep1&type=pdf (in English)
19. Tews, E., & Beck, M. (2009, March). Practical attacks against WEP and WPA. *Proceedings of the second ACM conference on Wireless network security-WiSec '09.* (pp. 79-86). Zurich, Switzerland. DOI: https://doi.org/10.1145/1514274.1514286 (in English)
20. Tews, E., Weinmann, R.-P., & Pyshkin, A. (2007). Breaking 104 Bit WEP in Less Than 60 Seconds. *Lecture Notes in Computer Science, 4867*, 188-202. DOI: https://doi.org/10.1007/978-3-540-77535-5_14 (in English)
21. Vanhoef, M., & Piessens, F. (2017, October). Key Reinstallation Attacks: Forcing Nonce Reuse in WPA$_2$. *CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. (pp. 1313-1328). Dallas, USA. DOI: https://doi.org/10.1145/3133956.3134027 (in English)

doi: https://doi.org/10.15802/stp2020/213042

22. Vanhoef, M., & Ronen, E. (2020, May). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. 2*020 IEEE Symposium on Security and Privacy (SP).* (pp. 517-533). San Francisco, USA. DOI: https://doi.org/10.1109/sp40000.2020.00031 (in English)
23. Wi-Fi CERTIFIED Enhanced Open delivers data protection in open Wi-Fi networks [web-site]. Retrieved from https://cutt.ly/9frxxot (in English)
24. WPA3 Security Considerations. (2019). *Wi-Fi Alliance*, 1-7. (in English)
25. WPA3 Specification Version 1.0. (2018). *Wi-Fi Alliance*, 1-7. (in English)

Надійшла до редколегії: 02.03.2020
Прийнята до друку: 03.08.2020

doi: https://doi.org/10.15802/stp2020/213042