УДК 004.056
Брюхов Б.Р.[1], Киричек Г.Г.[2]
[1] студ. гр. КНТ-513м НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ ТА ШИФРУВАННЯ В БЕЗДРОТОВИХ МЕРЕЖАХ

На даний час, швидке впровадження технологій бездротових мереж передачі даних і їх використання у різних сферах, веде до зростання кількості загроз, які виникають і впливають на параметри безпеки [1]. В мережах, здійснення атак різного функціонального впливу: перехоплення даних; атаки на автентифікацію; перехоплення облікових даних тощо є поширеним. Тому забезпечення надійного захисту інформації в бездротових мережах є досить актуальним питанням, яке передбачає впровадження передових методів та технологій, таких як багатофакторна автентифікація і сучасні методи шифрування [2].

Метою роботи є проведення досліджень, вибір методів, реалізація моделі і впровадження системи захисту бездротових мереж, яка: застосовує багатофакторну автентифікацію; сучасні методи шифрування; підтримує безпечний обмін даними і захищає мережу від несанкціонованого доступу. Об'єктом дослідження є процеси автентифікації та передачі даних у бездротових мережах. Предметом є моделі, методи, технології, стандарти та програмні засоби підвищення рівня безпеки бездротових мереж. Для досягнення основної мети визначено ряд завдань, це:

- проведення аналізу сучасних загроз, які виникають і створюють проблеми користувачам бездротових мереж;
- дослідження існуючих алгоритмів шифрування (AES, RSA) і методів багатофакторної автентифікації, включаючи одноразові коди та біометричні дані;
- реалізація моделі системи, яка поєднує багатофакторну автентифікацію і шифрування, забезпечуючи надійний захист мережі.

Система передбачає застосування декількох рівнів підтвердження та автентифікації, що гарантує підтримку високого рівня безпеки. Багатофакторна автентифікація включає:

- захист першого, початкового рівня автентифікації – вхід за паролем;
- використання одноразових кодів, які генеруються в реальному часі і є дійсними лише протягом короткого проміжку часу. Найчастіше надсилаються на зареєстрований мобільний пристрій або генеруються додатком;

- використання біометричних даних додає ще один рівень захисту, забезпечуючи підтвердження ідентичності за фізичними характеристиками, ускладнюючи несанкціонований доступ до мережі.

Даний метод дозволяє захистити мережеву систему від несанкціонованого доступу навіть у випадку компрометації одного із способів автентифікації. Згідно із даними досліджень компанії Cisco, впровадження багатофакторної автентифікації може знижувати ризики компрометації облікових даних на 99%. А шифрування гарантує, що навіть у випадку перехоплення даних зловмисник не зможе розшифрувати їх без відповідного ключа. Дослідження IBM Security демонструють, що такий підхід знижує ризик втрат від кібератак на 45%.

В подібних системах для шифрування переданих даних, найчастіше використовується алгоритм AES (Advanced Encryption Standard) із довжиною ключа 256 біт і вище [3]. Тому в процесі реалізації системи його обрано як алгоритм, що забезпечує:

- високий рівень захисту: AES-256 вважається одним із найбільш стійких симетричних алгоритмів шифрування і є достатньо надійним для використання в бездротових мережах;

- ефективність: AES підтримує високу швидкість шифрування і дешифрування, що є важливим при обробці даних у реальному часі.

Застосування даного методу гарантує, що інформація, яка передається в бездротових мережах є зашифрованою на всьому шляху її передачі та доступна для розшифрування лише з відповідним ключем.

В системі для обміну ключами застосовується алгоритм RSA. Він є основним для підтримки захищеної передачі ключів і забезпечує:

- захищений обмін ключами між клієнтськими та серверними пристроями, дозволяє передавати симетричні ключі у зашифрованому вигляді;

- автентифікацію сторін, методом використання значної обчислювальної складності та ефективних алгоритмів, зменшуючи ймовірність злому асиметричного ключа.

Запропонована система інтегрує багатофакторну автентифікацію та шифрування на рівні мережевих шлюзів та точок доступу забезпечуючи:

- безпечну автентифікацію користувачів: користувачі повинні пройти кілька рівнів автентифікації для доступу до мережі;

- шифрування всіх переданих даних між користувачами та мережею, що гарантує захист інформації на всіх етапах передачі.

На рисунку 1 наведено основні результати, які підтверджують актуальність досліджень щодо методів підвищення безпеки бездротових мереж. Використання багатофакторної автентифікації знижує ризик компрометації облікових даних на 99%, а сучасні методи шифрування

забезпечують конфіденційність даних і знижують втрати, пов'язані з кібератаками [4].

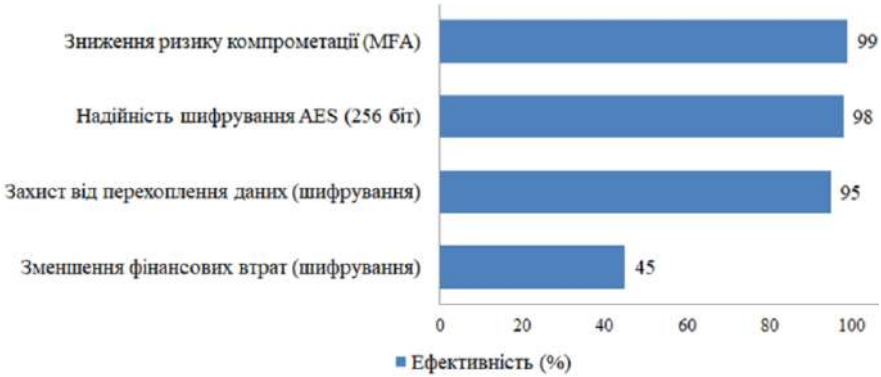

Рисунок 1 – Ефективність багатофакторної автентифікації та шифрування

Впроваджена система, яка поєднує багатофакторну автентифікацію та шифрування, демонструє свою ефективність при вирішенні завдань захисту бездротових мереж. Застосування наведених методів підвищує рівень безпеки, забезпечуючи автентифікацію і конфіденційність, що дозволяє знизити ризики несанкціонованого доступу та перехоплення інформації в бездротових мережах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kirichek G., Skrupsky S., Tiahunova M., Timenko A., Implementation of web system optimization method. In CMIS-2020: The Third International Workshop on Computer Modeling and Intelligent Systems, Zaporizhzhia, Ukraine, April 27-May1. CEUR Workshop Proceedings 2608, 2020, pp. 199–210.

2. Крівенко С., Ротаньова Н., Лазаревська Ю. Дослідження системи на уразливість до мітм атаки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2021. Т. 1, № 13. С. 29–38. DOI: https://doi.org/10.28925/2663-4023.2021.13.2938.

3. Network and system security / ed. by J. K. Liu, X. Huang. Cham : Springer International Publishing, 2019. DOI: https://doi.org/10.1007/978-3-030-36938-5.

4. Гальчинський Л. Ю., Корольова В. Р. Оцінка захищеності бездротових мереж у міському середовищі з урахуванням використання протоколів безпеки. Інфокомунікаційні та комп’ютерні технології, 2024, 2(06), 9-21. https://doi.org/10.36994/2788-5518-2023-02-06-01.