УДК 004.056:621.396.946

ВИКОРИСТАННЯ СЦЕНАРНОГО ПІДХОДУ В ОЦІНЦІ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БЕЗДРОТОВОЇ МЕРЕЖІ ОФІСУ

Реутова Є.С.
e-mail: yevheniia.didenko@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ
ім. В.В. Поповського
м. Харків, Україна

The study analyzes the application of a scenario-based approach to risk assessment in wireless office networks. Modern Wi-Fi infrastructures are exposed to multi-stage attacks such as Evil Twin, deauthentication, and man-in-the-middle. The study proposes a formalized risk assessment model based on ISO/IEC 27005 and NIST SP 800-30. The approach enables modeling attacker behavior, identifying critical vulnerabilities, and improving risk estimation accuracy. Scenario-based modeling supports detection of complex attack chains and enhances decision-making in cybersecurity management. The results demonstrate that wireless networks remain high-risk environments requiring adaptive protection strategies.

В часи розвитку технологій невід'ємною складовою будь-якої сучасної інформаційної інфраструктури є використання бездротових мереж. Однією з найпоширеніших є технологія бездротової локальної мережі Wireless Fidelity (Wi-Fi). Водночас, не дивлячись на те, що технологія застосовується давно і достатньо поширена, проблемою є відкритий радіоканал, який в свою чергу створює додаткові вектори атак.

Аналіз загроз на бездротові мережі показує, що найпоширенішими є:

- несанкціонований доступ;
- перехоплення трафіку;
- фальшиві точки доступу;
- DoS-атаки;
- вразливості обладнання;
- неавторизовані пристрої;
- витік даних.

Однак, слід зауважити, що сучасні атаки мають комбінований характер і включають в себе кілька послідовних атак, наприклад: деаутентифікація (Deauth), створення підробленої точки доступу (Evil Twin), атака man-in-the-middle (MITM) та подальше проникнення у внутрішню мережу [1, 2].

Традиційні підходи до оцінки ризиків часто не забезпечують врахування взаємозв'язків між окремими фазами атак. У цьому контексті доцільно застосовувати сценарний метод, що передбачає моделювання поведінки порушника [3, 4, 5].

Відповідно до запропонованої методики [3], ризик визначається на основі ймовірності реалізації сценарію та рівня вразливості системи.

Ймовірність сценарію визначається за формулою [3]:

$$P_{c_x} = \sum_{y=1}^{Y} P_x^y \cdot P_y$$

Згідно обраної методики [3], вразливість пропонується розраховувати за допомогою методичного апарату стандарту Національного інституту стандартів і технологій США Common Vulnerability Scoring System (CVSS) v3.1 приведеного в шкалу [0,1]:

$$V_x = \frac{CVSS}{10}$$

Ризик для кожного сценарію розраховуватиметься за формулою [3]:

$$R_x = P_{c_x} \cdot V_x$$

Для прикладу розглянемо три типи порушників, які наведені в Таблиці 1 та приведемо результати розрахунків в Таблиці 2 рівень ризику для трьох типових сценаріїв атак: Evil Twin, деаутентифікація та комбінований сценарій.

Таблиця 1 - Визначення ймовірності атаки згідно з типами порушників.

Тип	Опис	Ймовірність атаки
y_1	Порушник з низьким рівнем технічної підготовки	0.5
y_2	Внутрішній порушник	0.3
y_3	Порушник з високим рівнем технічної підготовки	0.2

Ймовірності типів порушників визначені експертним методом на основі аналізу сучасних кіберзагроз. Найбільша частка припадає на низькокваліфікованих порушників через доступність інструментів атак, тоді як цільові атаки мають меншу ймовірність через їх складність і вимогу до ресурсів.

Таблиця 2 - Результати розрахунків оцінки ризиків

Сценарій	Ймовірність сценарію	Вразливість	Ризик	Рівень
Evil Twin	0.79	0.85	0.67	Високий
Deauth	0.75	0.60	0.45	Середній
Комбінована	0.83	0.95	0.78	Критичний

Отримані результати показали, що найбільший рівень ризику має комбінований сценарій атаки, оскільки він включає декілька етапів та дозволяє обійти механізми захисту [1].

Список використаних джерел:

1. Curwell P. Evil Twin Attacks: A Hidden Threat to Your IP and Data Security // Paul Curwell Blog. 2025. URL: https://paulcurwell.com/2025/03/04/evil-twin-attacks-a-hidden-threat-to-your-ip-and-data-security/ (дата звернення: 24.03.2026).
2. Hern A. Man used fake Wi-Fi networks to steal personal data at airports // The Guardian. 2024. URL: https://www.theguardian.com/technology/article/2024/jun/28/wa-man-fake-free-wifi-airports-data-theft-ntwnfb (дата звернення: 24.03.2026).
3. Guide for Conducting Risk Assessments (NIST SP 800-30 Rev.1). Gaithersburg : National Institute of Standards and Technology, 2012. 95 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (дата звернення: 24.03.2026).
4. ISO/IEC 27005:2022 Information security risk management. Geneva : International Organization for Standardization, 2022. URL: https://www.iso.org/standard/80585.html (дата звернення: 24.03.2026).
5. Снігуров А. В., Слюсар Н. М., Діденко Є. С. Оцінка ризиків інформаційної безпеки на основі сценарного підходу // Матеріали міжнародної науково-практичної конференції. 2022. С. 117–119. URL: https://ice.nure.ua/wp-content/uploads/2022/12/37_Snihurov-A.V.-Sliusar-N.M.-Didenko-Ie.S._Str.117-119.pdf (дата звернення: 24.03.2026).