

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ТА ОПТИМІЗАЦІЇ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ДОМАШНІХ ІНФОРМАЦІЙНО- КОМУНІКАЦІЙНИХ МЕРЕЖ

Волошин М.Є., науковий керівник Лахно В.А.

У сучасному світі цифрові технології проникають у всі сфери життя, і особливо це помітно в умовах домашнього використання інтернету та мережевих пристроїв. Побутові інформаційно-комунікаційні мережі давно перестали бути простими засобами підключення одного-двох пристроїв до інтернету. Сьогодні вони являють собою складну інфраструктуру, яка включає в себе комп'ютери, смартфони, смарт-телевізори, принтери, IP-камери, розумні колонки, побутову техніку з підтримкою інтернету речей (IoT) та інші пристрої. З одного боку, це надає зручність, мобільність, автоматизацію побутових процесів. З іншого боку, чим більше пристроїв і сервісів задіяно, тим більше точок уразливості виникає для потенційних зловмисників [1].

Сучасні тенденції в кібербезпеці свідчать про зростання атак, орієнтованих саме на домашніх користувачів. Якщо раніше мішенню хакерів переважно ставали корпоративні структури, то сьогодні увага дедалі частіше звертається до звичайних користувачів, які, на жаль, часто нехтують базовими принципами безпеки або просто не мають достатніх знань. Недостатній рівень захисту домашнього Wi-Fi, використання стандартних паролів, відсутність шифрування, неконтрольований доступ до мережі сторонніх пристроїв — усе це створює серйозні загрози. До того ж багато користувачів навіть не підозрюють, що їхній принтер чи телевізор можуть бути використані як шлюз для доступу до решти мережі або як елемент ботнету [2].

Не менш актуальним є і питання ролі операційних систем у контексті мережевої безпеки. Саме ОС забезпечує виконання критично важливих функцій: контроль мережевих підключень, реалізацію міжмережевих екранів, шифрування трафіку, керування оновленнями тощо. За відсутності оновлень або при використанні застарілих систем, навіть найбільш просунуте обладнання може стати вразливим. Крім того, деякі платформи надають обмежені можливості з налаштування безпеки, що змушує користувача самостійно шукати способи підвищення захисту.

Суттєвий вплив на ситуацію мають і хмарні технології [3], які широко інтегруються в домашні інфраструктури. Хмарні сервіси дозволяють керувати пристроями віддалено, зберігати дані, автоматизувати процеси. Але водночас вони розширюють поверхню атаки: у випадку компрометації облікових записів користувача, зловмисник отримує контроль над великою частиною домашньої мережі. Це створює необхідність впровадження засобів двофакторної аутентифікації, моніторингу доступу, регулярної перевірки активності та сегментації мережі.

Актуальність проблематики захисту домашніх інформаційно-комунікаційних мереж [4] також зумовлена переходом до дистанційної роботи, навчання, телемедицини, онлайн-банкінгу — всі ці процеси здійснюються в умовах домашнього середовища, але потребують не меншого рівня захисту, ніж у корпоративному секторі. У сучасних умовах зловмисникам достатньо зламати слабкий пароль до маршрутизатора або зчитати незашифрований трафік, щоб отримати доступ до фінансової або персональної інформації користувача.

Метою цієї роботи є дослідження сучасного стану безпеки домашніх мереж, виявлення типових вразливостей та практичне моделювання методів захисту. У рамках дослідження буде розглянуто приклад домашньої мережі з декількома пристроями, проведено аналіз поточної конфігурації, оцінено рівень ризику та запропоновано комплекс заходів для її захисту. Зокрема, буде проаналізовано налаштування маршрутизатора, розмежування мережі для різних типів пристроїв, використання VPN,

шифрування з'єднань, а також реалізація базових правил кібергігієни для користувачів. Додатково, увагу буде приділено використанню інструментів тестування, таких як Wireshark, Aircrack-ng та інші, для імітації типових атак і перевірки ефективності впроваджених заходів.

Очікуваним результатом стане формування практичних рекомендацій, які можуть бути впроваджені в реальному побутовому середовищі з мінімальними витратами та без необхідності у складному обладнанні. Це дозволить підвищити загальний рівень захищеності інформаційно-комунікаційних систем у домогосподарствах та сприятиме формуванню культури цифрової безпеки серед широкого кола користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лихно Р. С. Забезпечення безпеки в системах пристроїв Інтернету речей. 2019. [Електронний ресурс]. Режим доступу: <https://ela.kpi.ua/items/aad84bab-316e-4591-9aa7-0160302b5126> (дата звернення: 20.04.2025)
2. 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). С. 9–21.
3. What Is Cloud Network Security? [Електронний ресурс], Режим доступу: <https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-network-security> (дата звернення: 20.04.2025)
4. Network Security Policy: Best Practices White Paper. [Електронний ресурс], Режим доступу: <https://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html> (дата звернення: 20.04.2025)

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів