УДК 004.056.5

К. В. Козак
Т. Г. Кирилащук

КІБЕРБЕЗПЕКА КОРПОРАТИВНИХ МЕРЕЖ: ТИПОВІ ЗАГРОЗИ ТА СПОСОБИ ПРОТИДІЇ

Вінницький національний технічний університет

Анотація

У дослідженні розглянуто головні аспекти кібербезпеки корпоративних мереж в умовах збільшення кількості кібератак. Проаналізовано типові небезпеки, зокрема шкідливе програмне забезпечення, фішинг та неавторизований доступ. Окреслено ключові методи протидії цим небезпекам, включаючи технічні та організаційні міри захисту. Підкреслено потребу комплексного підходу до гарантування безпеки корпоративних мереж.

Ключові слова: кібербезпека; корпоративні мережі; кіберзагрози; фішинг; шкідливе програмне забезпечення; захист інформації.

Abstract

The study examines the main aspects of cybersecurity of corporate networks in the context of an increase in the number of cyberattacks. It analyzes typical threats, including malware, phishing, and unauthorized access. It outlines key methods for countering these threats, including technical and organizational protection measures. It emphasizes the need for a comprehensive approach to ensuring the security of corporate networks.

Keywords: cybersecurity, corporate networks, cyber threats, phishing, malware, information security.

Вступ

У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації бізнес-процесів корпоративні мережі відіграють вирішальну роль у забезпеченні ефективної діяльності організацій. Вони є фундаментом для зберігання, обробки й передачі значних обсягів відомостей, у тому числі конфіденційної та комерційно важливої інформації. Водночас зростання кількості та складності кібератак, поява нових векторів загроз і розширення периметра мережі суттєво підвищують небезпеки порушення інформаційної безпеки. Наслідками таких подій можуть бути фінансові втрати, витік даних, зупинка бізнес-процесів і репутаційні збитки. У зв'язку з цим питання забезпечення кібербезпеки корпоративних мереж набуває особливої значущості та потребує комплексного підходу, що поєднує технічні, організаційні та управлінські заходи захисту.

Метою дослідження є розгляд типових небезпек кібербезпеки корпоративних мереж та окреслення головних методів протидії їм з метою зростання рівня охоронності інформаційних активів установ.

Результати дослідження

1. Типові загрози корпоративних мереж

Корпоративні мережі – це одна з головних мішеней кіберзлочинців, адже вони містять життєво важливу інформацію та забезпечують роботу бізнес-процесів. Найбільш типовою небезпекою залишається шкідливе програмне забезпечення, яке може проникати у систему через інфіковані файли, електронну пошту або недоліки програмного забезпечення. Особливу загрозу являють програми-вимагачі, що заблоковують доступ до відомостей і вимагають відкуп за їх дешифрування.

Фішингові спроби, що ґрунтуються на соціальній інженерії, націлені на працівників компанії. Зловмисники формують повідомлення, які копіюють достовірні джерела, спонукаючи людей розкривати паролі або завантажувати шкідливі програми. Людський чинник у цьому випадку стає головним елементом успішності нападу.

Не менш небезпечними є напади на мережеву інфраструктуру, зокрема DDoS, які перевантажують сервери та спричиняють зупинку роботи сервісів. Атаки типу «людина посередині» дозволяють перехоплювати та змінювати трафік між користувачем і сервером, що створює небезпеку витоку конфіденційної інформації.

2. Стратегія протидії та захисту

Для дієвого захисту корпоративних мереж треба використовувати багатошаровий підхід, який злучає технічні та управлінські заходи. На технічному рівні значущим є захист кінцевих точок за допомогою антивірусних програм, систем виявлення та унеможливлення вторгнень, а також періодичне оновлення програмного забезпечення. Це дає змогу знизити небезпеку використання знаних вразливостей.

Організаційні заходи охоплюють навчання персоналу основам кібергігієни, проведення тренувань та симуляцій фішингових атак. Формування культури безпеки всередині компанії є головним чинником у зменшенні ризику людських помилок.

Охорона мережі вимагає застосування міжмережевих екранів, VPN, сегментування мережі та безперервного відстеження трафіку. Ключовим складником є регулювання доступу – запровадження багатофакторної автентифікації, засади обмежених привілеїв та спільного управління обліковками. Тільки цілісний підхід, що об’єднує технічні засоби та упорядковані кроки, здатний гарантувати належний рівень кібербезпеки підприємницьких мереж [2].

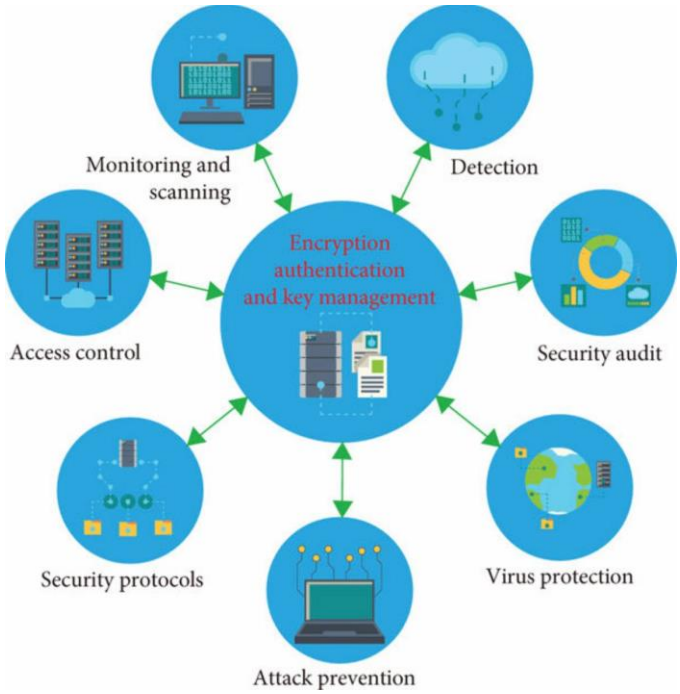

Рис. 1. Типові загрози та основні напрями захисту корпоративної мережі [1]

На рисунку 1 представлено схематичне відображення основних компонентів кібербезпеки корпоративної мережі, що включають моніторинг, виявлення загроз, контроль доступу та управління ключами.

Висновки

Корпоративні мережі залишаються вразливими до великого спектра кіберзагроз, серед яких значну роль відіграють зловмисне програмне забезпечення, фішинг та напади на мережеву інфраструктуру. Більшість успішних інцидентів постають через комбінацію технічних вразливостей та людського фактора. Дієвий захист можливий лише за умови всебічного підходу, що поєднує сучасні технічні засоби, неперервний моніторинг та збільшення обізнаності працівників.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Liu C., Babar M. A. Corporate cybersecurity risk and data breaches: A systematic review of empirical research. Australian Journal of Management, Vol. 51, №1, 2026, pp. URL: https://journals.sagepub.com/doi/10.1177/03128962211058465 (дата звернення: 27.02.2026).
2. Програмний захист даних. *Офіційний сайт CIOU*. URL: https://ciou.lissa.cx.ua/articles/programnij-zahist-danih-e.html (дата звернення: 27.02.2026).

Костянтин Вячеславович Козак – студент групи 1КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: kkozak256@gmail.com

Науковий керівник: ***Тетяна Генадіївна Кирилащук*** – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Konstantin V. Kozak – student of group 1KITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: kkozak256@gmail.com

Supervisor: ***Tetiana H. Kyrylashchuk*** – assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia