УДК 004.056

ДОСЛІДЖЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В КОРПОРАТИВНИХ МЕРЕЖАХ З ВІДДАЛЕНИМ ДОСТУПОМ

Козак С. О.
e-mail: svitlana.kamenetska@nure.ua
Науковий керівник – к.т.н. Харченко Н. А.
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна

This work is devoted to the study of information security threats in corporate networks with remote access. The main threats are analyzed, including data interception, weak passwords, malware, phishing and social engineering, as well as risks related to the uncontrolled use of artificial intelligence by employees and attackers. The study shows that without a comprehensive approach and the implementation of modern technical and organizational security measures, ensuring the safety of corporate networks is impossible.

Сьогодні багато компаній дозволяють співробітникам підключатися до корпоративної мережі з дому або з інших віддалених локацій. Це підвищує гнучкість роботи, проте одночасно створює нові загрози для інформаційної безпеки [1]. Зловмисники можуть скористатися віддаленим доступом і спробувати отримати несанкціонований доступ до конфіденційних даних, фінансової інформації та внутрішніх ресурсів компаній.

Метою даного дослідження є вивчення основних загроз інформаційній безпеці в корпоративних мережах з віддаленим доступом та розробка способів для їх зменшення, використовуючи сучасні технічні та організаційні заходи.

Однією з головних загроз для корпоративних мереж з віддаленим доступом є перехоплення даних. Зловмисники можуть перехоплювати трафік між користувачем і мережею компанії, отримуючи доступ до логінів, паролів та інших даних. Щоб захиститися, застосовуються шифровані з’єднання через VPN, використання сучасних протоколів шифрування та багатофакторна автентифікація користувачів [1].

Іншою поширеною загрозою є використання слабких паролів та повторне використання облікових даних. Зловмисники можуть підбирати паролі автоматично або використовувати дані з попередніх витоків. Для захисту необхідно впроваджувати складні унікальні паролі, політики їх регулярної зміни та обов’язкову багатофакторну аутентифікацію [2].

Не менш важливою є загроза шкідливого програмного забезпечення, яке може потрапляти через особисті пристрої користувачів. Якщо співробітник підключається до корпоративної мережі з ноутбука або смартфона, зараженого вірусами чи троянами, шкідливі програми можуть поширюватися на внутрішні ресурси компанії [3]. Захист включає встановлення антивірусного програмного забезпечення, обмеження прав доступу для віддалених пристроїв та моніторинг активності в мережі.

Велику небезпеку становлять фішингові атаки та соціальна інженерія. Зловмисники можуть надсилати електронні листи з підробленими посиланнями або повідомленнями, які імітують офіційні запити від компанії. Їхня мета – отримати доступ до облікових записів та внутрішніх систем. Для протидії цьому використовуються поштові фільтри, навчання персоналу та політики перевірки достовірності повідомлень [2].

Наразі головною загрозою є активне використання штучного інтелекту як зловмисниками, так і співробітниками. Зловмисники застосовують його для автоматизації атак і створення правдоподібних фішингових повідомлень, що ускладнює їх виявлення. Водночас неконтрольоване використання ШІ працівниками може призводити до витоку конфіденційної інформації. Для зниження ризиків необхідно впроваджувати інтелектуальні системи моніторингу, контроль доступу, аналіз поведінки користувачів та регулярне навчання персоналу.

Крім технічних заходів, важливими є організаційні методи захисту. Вони включають розробку політик безпеки для віддалених співробітників, регулярне резервне копіювання даних, інструктажі з кібергігієни та тестування системи на наявність вразливостей [1]. Це дозволяє мінімізувати наслідки атак і швидко відновити працездатність корпоративної мережі.

Таким чином, дослідження загроз інформаційній безпеці в корпоративних мережах з віддаленим доступом показує, що без комплексного підходу забезпечити безпеку даних неможливо. Впровадження сучасних технологій захисту та навчання персоналу дозволяє знизити ризики й забезпечити надійну роботу корпоративних інформаційних систем. Також необхідно враховувати динаміку в розвитку видів загроз, що призводить до необхідності постійного вдосконалення методів захисту. Тому системи безпеки даних мають не тільки враховувати всі рівні захисту інформації, а й швидко виявляти нові види загроз.

Список використаних джерел:

1. Носок С. О., Коломицев М. В., Стьопочкіна І. В. Управління інформаційною безпекою : навч. посіб. Київ : КПІ, 2025. 88 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/78ac6951-65ee-4a76-8acf-ba0554c5de4c/content (дата звернення: 23.02.2026).

2. Рекомендації для медіа з підвищення рівня кібербезпеки : вебсайт. URL: https://cybersec.net.ua/statti/941-rekomendatsii-dlia-media-z-pidvyshchennia-rivnia-kiberbezpeky.html (дата звернення: 23.02.2026).

3. Магдаліна М. І. Методика аналізу вразливостей до кібератак сучасних інформаційних систем; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2023. – 85 с.