УДК

Паф'янов Д. О.

КІБЕРБЕЗПЕКА В ІНТЕРНЕТІ

Вінницький національний технічний університет

Анотація

Кібербезпека в інтернеті спрямована на захист інформації, пристроїв і користувачів від цифрових атак. Вона включає використання надійних паролів, антивірусних програм, обережне ставлення до підозрілих посилань і повідомлень, а також дотримання правил безпечної поведінки в мережі. Знання основ кібербезпеки допомагає уникнути багатьох ризиків і зробити користування інтернетом безпечнішим.

Ключові слова: кібербезпека, інтернет, дані, мережа, правила, ризики.

Abstract

Cybersecurity on the internet aims to protect information, devices, and users from digital attacks. It includes using strong passwords, antivirus software, being cautious about suspicious links and messages, and following rules for safe online behavior. Knowing the basics of cybersecurity helps you avoid many risks and makes using the internet safer.

Keywords: cybersecurity, internet, data, network, rules, risks.

Вступ

У сучасному світі інтернет став невід'ємною частиною повсякденного життя. Люди використовують його для навчання, роботи, спілкування, зберігання інформації та проведення фінансових операцій. Проте разом із широкими можливостями мережі з'являються й нові загрози: віруси, фішинг, злам акаунтів, крадіжка персональних даних та інші кіберзлочини. Саме тому питання кібербезпеки набуває особливої актуальності.

Результати дослідження

Кібербезпека – це сукупність методів, технологій і організаційних заходів, спрямованих на захист інформаційних систем, комп'ютерних мереж і даних від кіберзагроз. Основною метою кібербезпеки є забезпечення конфіденційності, цілісності та доступності інформації.

У сучасному цифровому середовищі кібербезпека має важливе значення як для окремих користувачів, так і для організацій та держави. Вона допомагає запобігати витоку інформації, несанкціонованому доступу до даних і порушенню роботи комп'ютерних систем [1].

Серед найбільш поширених загроз у кіберпросторі можна виділити фішинг, шкідливе програмне забезпечення, DDoS-атаки та соціальну інженерію.

Фішинг є одним із найпоширеніших методів інтернет-шахрайства. Його метою є отримання конфіденційної інформації користувача, такої як паролі або дані банківських карток. Для цього зловмисники надсилають підроблені повідомлення або створюють фальшиві веб-сайти, які імітують офіційні ресурси.

Шкідливе програмне забезпечення, до якого належать віруси, троянські програми та шпигунські додатки, може пошкоджувати систему, викрадати інформацію або надавати зловмисникам віддалений доступ до пристрою користувача [2].

Також небезпечними є DDoS-атаки, під час яких сервер або веб-сайт перевантажується великою кількістю запитів, що призводить до тимчасової недоступності ресурсу [3]. Окрім технічних атак, часто використовується соціальна інженерія – метод психологічного впливу на користувачів з метою отримання конфіденційної інформації.

Соціальні мережі стали важливою частиною сучасного життя, однак вони також можуть становити певну небезпеку для користувачів. Часто люди публікують особисту інформацію, фотографії або місце перебування, що може бути використано зловмисниками. Тому важливо уважно ставитися до налаштувань конфіденційності та не поширювати надмірну кількість особистих даних.

Крім того, користувачам слід бути обережними щодо підозрілих повідомлень або посилань, які можуть надсилатися від невідомих осіб. Такі повідомлення можуть містити шкідливі файли або вести на фальшиві веб-сайти, створені для викрадення інформації.

Для забезпечення безпеки під час використання інтернету важливо дотримуватися певних правил цифрової безпеки. Одним із найефективніших способів захисту є використання надійних паролів. Паролі повинні бути складними та містити комбінацію літер різного регістру, цифр і спеціальних символів [2]. Крім того, рекомендується використовувати різні паролі для різних онлайн-сервісів.

Важливу роль у захисті комп'ютерних систем відіграє використання антивірусного програмного забезпечення. Антивірусні програми дозволяють виявляти, блокувати та видаляти шкідливі файли, які можуть потрапити на пристрій під час роботи в мережі. Не менш важливим є регулярне оновлення операційної системи та програм, оскільки оновлення містять виправлення вразливостей, які можуть використовуватися кіберзлочинцями [3].

Користувачам також слід обережно користуватися бездротовими мережами. Підключення до захищених Wi-Fi мереж значно зменшує ризик перехоплення особистих даних [2]. Крім того, важливим заходом безпеки є регулярне резервне копіювання важливих файлів, що дозволяє відновити інформацію у разі її втрати або пошкодження.

Забезпечення кібербезпеки є важливим завданням не лише для окремих користувачів, але й для держави. Багато країн створюють спеціальні органи та служби, які відповідають за захист інформаційної інфраструктури та боротьбу з кіберзлочинністю. В Україні питання кібербезпеки координується державними установами, такими як Державна служба спеціального зв'язку та захисту інформації [1].

Державні органи також розробляють закони та стратегії, спрямовані на підвищення рівня кіберзахисту. Важливим напрямом є підвищення цифрової грамотності населення та проведення інформаційних кампаній щодо безпечного користування інтернетом.

Висновки

Отже, кібербезпека є важливою складовою сучасного цифрового суспільства. З розвитком інформаційних технологій зростає і кількість кіберзагроз, що потребує відповідального ставлення до безпеки в інтернеті. Дотримання основних правил кібергігієни, використання захисного програмного забезпечення та підвищення цифрової грамотності користувачів сприяють зменшенню ризиків і забезпечують безпечне використання мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Дія.Освіта – Основи кібергігієни. Дія.Освіта. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene (дата звернення: 09.03.2026).

2. Міністерство цифрової трансформації України. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/ (дата звернення: 09.03.2026).

3. Що таке кібербезпека? Заходи забезпечення кібербезпеки. Ворожбянський заклад загальної середньої освіти І-ІІІ ступенів Лебединської міської ради Сумської області - вітаємо на офіційному веб-сайті. URL: https://vorozhba.lbd-osv.gov.ua/news/16-31-30-02-05-2025 (дата звернення: 09.03.2026).

4. Готовність до кібербезпеки. ENISA. URL: https://www.enisa.europa.eu (дата звернення: 09.03.2026).

Паф'янов Дмитро Олександрович – студент групи 1КІТС-24б кафедри менеджменту і безпеки інформаційних систем факультет менеджмент і інформаційна безпека, Вінницький національний технічний університет, Вінниця, dimas.pafanov@gmail.com

Pafyanov Dmitry Alexandrovich – student of group 1KITS-24b, department of management and information systems security, faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, dimas.pafanov@gmail.com