УДК 004.056:004.77

ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ INTERNET ТА СОЦІАЛЬНИХ МЕРЕЖАХ

Бурцева К.О.
Науковий керівник – ст. викл. Олейнікова О.І.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
e-mail: kateryna.burtseva1@nure.ua

The paper highlights the importance of cybersecurity in today's world, where the Internet is the primary platform for communication, work, and entertainment. It details various threats, such as hacking attacks, phishing, and malware, which can lead to the loss of sensitive data and financial losses. Additionally, the paper discusses security measures, including data encryption, secure network access protocols, and two-factor authentication, as key elements in protecting information on the Internet and social networks.

У сучасному світі, де інтернет став основним місцем для спілкування, роботи та розваг, питання захисту конфіденційної інформації набуває надзвичайної важливості. Недостатній захист може призвести до серйозних наслідків, включаючи крадіжку особистих даних, фінансові втрати та порушення особистої приватності. Це не тільки стосується індивідуальних користувачів, але й великих організацій. Хакерські атаки, віруси, фішинг і шпигунські програми стають більш досконалими, що створює реальну загрозу конфіденційності та безпеці даних. Такі інциденти можуть призвести не тільки до фінансових збитків, але й до серйозного підриву довіри до цифрових систем. Тому розробка та впровадження ефективних стратегій кібербезпеки є ключовими для захисту цінної інформації в онлайн-просторі.

У соціальних мережах користувачі часто стикаються з різноманітними загрозами, серед яких широко поширеним є фішинг. Зловмисники вдаються до обману та маніпуляцій, аби отримати конфіденційну інформацію, таку як паролі чи банківські дані, часто використовуючи для цього підроблені повідомлення або вебсайти. Шкідливе програмне забезпечення також є значною загрозою, оскільки воно може бути поширене через соціальні мережі під виглядом невинних посилань або вкладень, що призводить до компрометації особистих даних та систем безпеки. Щоб забезпечити свою безпеку, користувачам важливо уважно ставитися до налаштувань конфіденційності в соціальних мережах, також регулярно оновлювати свої паролі та використовувати надійне антивірусне програмне забезпечення [1].

Шифрування даних є одним з основних методів захисту конфіденційної інформації в Інтернеті. Ця технологія полягає у перетворенні інформації в код, який неможливо зрозуміти без відповідного

ключа розшифровки. Існує два основних типи шифрування: симетричне, де використовується один і той же ключ для шифрування та розшифровки, і асиметричне, де застосовуються два різні ключі (публічний і приватний). Шифрування використовується у багатьох аспектах онлайн-діяльності, включаючи безпечну передачу даних через Інтернет, захист електронних повідомлень, а також у фінансових транзакціях [2].

Безпечні протоколи мережевого доступу, такі як HTTPS (Hypertext Transfer Protocol Secure), VPN (Virtual Private Network) та SSL/TLS (Secure Sockets Layer/Transport Layer Security), є ключовими елементами в захисті даних, переданих через Інтернет. HTTPS захищає інформацію, передану між веб-браузером користувача та сервером, запобігаючи її перехопленню та зміні. VPN створює зашифрований канал для передачі даних, який захищає інформацію від перехоплення, навіть якщо користувач підключений через незахищену мережу. Використання цих технологій є важливим для забезпечення конфіденційності інформації у глобальній мережі.

Двофакторна аутентифікація (2FA) є методом забезпечення додаткового рівня безпеки при вході в обліковий запис або систему. Основний принцип двофакторної аутентифікації полягає у використанні двох різних типів даних для верифікації особи, що намагається увійти в систему. Зазвичай, перший елемент - це пароль, а другий може включати SMS-коди, телефонні дзвінки, електронні токени, або біометричні дані. Це значно ускладнює несанкціонований доступ до акаунту, оскільки потенційному зловмиснику потрібно буде отримати як пароль, так і фізичний доступ до другого елемента, що суттєво знижує ризики витоку даних та несанкціонованого доступу [3].

Отже, захист конфіденційної інформації в мережі Internet та соціальних мережах є важливим процесом у сучасному світі. Оскільки, зростає кількість загроз, таких як хакерські атаки, фішинг та шкідливе програмне забезпечення, стає особливо актуальним розроблення та впровадження ефективних стратегій кібербезпеки. Використання сучасних методів шифрування, безпечних протоколів для мережевого доступу та двофакторної аутентифікації є ключовими елементами для забезпечення безпеки та збереження конфіденційності в онлайн-середовищі.

Список використаних джерел:

1. Безпека в Інтернеті: вебсайт. URL: https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html (дата звернення: 09.02.2024).
2. Шифрування: типи і алгоритми: вебсайт. URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms (дата звернення: 10.02.2024).
3. Що таке двофакторна автентифікація або 2FA?: вебсайт. URL: https://experience.dropbox.com/uk-ua/resources/what-is-2fa (дата звернення: 10.02.2024).