УДК 004.056

Струковський Б. Є.

ЯК ЗАХИСТИТИ ДАНІ ВІД ВИТОКУ

Вінницький національний технічний університет

Анотація

Захист даних є важливим, адже вони є частиною нашого особистого простору та впливають на безпеку й приватність. Відповідальне ставлення до інформації допомагає зберегти контроль над нею та уникнути можливих ризиків у цифровому середовищі.

Ключові слова: захист, дані, безпека, приватність, інформація, ризики, цифрове середовище.

Abstract

Data protection is important because data is part of our personal space and affects our security and privacy. A responsible attitude toward information helps us maintain control over it and avoid potential risks in the digital environment.

Keywords: protection, data, security, privacy, information, risks, digital environment.

Вступ

У сучасному світі інформація стала однією з найцінніших складових розвитку суспільства. Щодня люди створюють, передають і зберігають значні обсяги даних у різних сферах життя – від навчання й роботи до спілкування та дозвілля. Цифрові технології відкривають широкі можливості, однак водночас формують нові виклики, пов'язані з безпекою інформації. Збереження конфіденційності та цілісності даних стає важливою умовою стабільності, довіри й ефективної взаємодії в суспільстві. Саме тому питання захисту даних є актуальним і потребує усвідомленого підходу на різних рівнях.

Результати дослідження

Захист даних – це комплекс стратегій, політик та технічних заходів, які допомагають запобігти втраті, пошкодженню або несанкціонованому доступу до важливої інформації. Він забезпечує конфіденційність, цілісність та доступність даних впродовж усього їхнього життєвого циклу [1]. Захист даних є необхідним елементом кібербезпеки як для окремих людей, так і для організацій, оскільки витоки можуть спричиняти фінансові втрати, шкоду репутації, порушення приватності та прав людини. Головні правила, які допоможуть уникнути витоку даних:

1. Ніколи повторювати паролі. Запам'ятати один пароль та використовувати його для кожної соцмережі та на кожному сайті звичайно легко. Проте і зловмисники так само легко можуть дізнатись про єдиний пароль і отримати доступ до всіх соцмереж та облікових записів. Аби цього не сталось потрібно при кожній новій реєстрації вигадувати окремий пароль та логін. Фахівці також радять по можливості змінювати всі паролі кожні 30, 60 або 90 днів – залежно від того, що вони захищають [2]. Для створення особливо захищених паролів можна використовувати спеціальні сайти-генератори, менеджери паролів або браузерні системи зберігання паролів, які вигадують їх замість людини. Також для кращої безпеки і більшої впевненості рекомендується увімкнути двофакторну автентифікацію. З її допомогою сайт двічі переконується, що ви це ви.

2. Уникати підключення до публічних Wi-Fi. Незахищений публічний Wi-Fi може використовуватись шахраями для перехоплення особистих даних користувачів. Хакери також можуть створити шкідливі точки доступу для збору даних та перенаправлення жертв на небезпечні сайти. У разі нагальної потреби використати загальнодоступну мережу не відкривати жодних конфіденційних облікових записів. У будь-якому випадку використовувати VPN, щоб бути в безпеці.

3. Не зберігати дані платіжної картки та особисту інформацію при купівлі товарів в онлайнмагазинах. У такому разі у зловмисників буде менше можливостей для шахрайста у разі витоку даних цих компаній [3]. Крім того, варто вводити платіжні реквізити лише під час здійснення конкретної покупки та перевіряти надійність сайту перед оплатою. Обережне ставлення до своїх фінансових даних зменшує ризик несанкціонованих операцій і допомагає зберегти контроль над власними коштами.

4. Ніколи не відкривати електронні листи і не переходити за посиланням, якщо ви не впевнені в тому, від кого вони, і у жодному разі не завантажувати вкладення з таких листів. Якщо офіційна організація надсилає електронний лист із проханням завантажити щось або поділитися інформацією, вам слід зателефонувати їй безпосередньо, щоб підтвердити цей запит. Багато хто не надсилає електронну пошту як перший крок листування.

5. Ознайомитись з усіма параметрами конфіденційності даних свого облікового запису та застосувати їх, де це можливо [4]. Якщо це неможливо, намагатись не розкривати занадто багато інформації, а саме – не використовувати своє повне ім’я, не вказувати дату народження, не поширювати свої контактні дані і не розголошувати своє місце проживання.

6. Регулярне оновлення програмного забезпечення. Застаріле програмне забезпечення може містити вразливості, які зловмисники використовують для доступу до ваших даних [5]. Рекомендується регулярно оновлювати операційну систему, антивірусні програми та інші додатки.

Захист даних – це постійний процес, що потребує систематичного підходу. Дотримуючись наведених порад, вдасться мінімізувати ризики втрати даних і забезпечити безпеку в цифровому світі. Головним елементом безпеки є обізнаність та відповідальність. Відповідальний підхід до зберігання конфіденційних файлів та даних допоможе завчасно попередити витоки важливих даних, які можуть спричинити багато проблем.

Значна частина нашого життя пов’язана з використанням цифрових технологій. Ми зберігаємо особисті дані, спілкуємося, здійснюємо фінансові операції та навчаємося онлайн, тому будь-яка необережність може призвести до витоку інформації. Розуміння основ кібербезпеки допомагає вчасно розпізнати потенційні загрози, уникнути шахрайських дій і зберегти конфіденційність своїх даних. Обізнаність у цій сфері формує відповідальне ставлення до інформації та сприяє безпечній поведінці в цифровому середовищі.

Висновки

Отже, захист даних у сучасному цифровому світі є надзвичайно важливим для збереження приватності та безпеки. Усвідомлення загроз та базові знання з кібербезпеки допомагають людям уникати витоків інформації та шахрайських дій. Відповідальне ставлення до особистих даних, обережність під час користування онлайн-сервісами та дотримання правил безпеки зменшують ризики втрати інформації. Таким чином, обізнаність і уважність у цифровому середовищі стають важливою складовою безпечного життя в сучасному світі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке захист даних? | Захисний комплекс Microsoft. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-data-protection?utm_source=chatgpt.com (дата звернення: 26.02.2026).
2. Як захистити себе онлайн: 8 поширених способів викрадення особистих даних. ESET. URL: https://www.eset.com/ua/about/newsroom/blog/data-protection/yak-zakhystyty-sebe-onlayn-8-poshyrenykh-sposobivvykradennyaosobystykh-danykh/ (дата звернення: 26.02.2026).
3. Як захистити свої дані в Інтернеті: кілька дієвих порад | Сьомий апеляційний адміністративний суд. Сьомий апеляційний адміністративний суд. URL: https://7aac.gov.ua/yak-zaxistiti-svoï-dani-v-interneti-kilka-diyevix-porad/ (дата звернення: 26.02.2026).
4. Як захистити особисту інформацію в Інтернеті. Dropbox. URL: https://www.dropbox.com/uk_UA/resources/protectingpersonal-info-online (дата звернення: 26.02.2026).
5. Як захистити дані від несанкціонованого доступу? Поради | CyberCalm. CyberCalm | Кіберзахист та кібербезпека простою мовою. URL: https://cybercalm.org/yak-zahystyty-dani-vid-nesanktsionovanogo-dostupu-porady/ (дата звернення: 26.02.2026).

Струковський Богдан Євгенович – студент групи 1КІТС-24б кафедри менеджменту і безпеки інформаційних систем факультет менеджмент і інформаційна безпека, Вінницький національний технічний університет, Вінниця, halksantone@gmail.com

Науковий керівник **– Шелепало Галина Василівна** – доцент кафедри ЗІ, к.фз-мат.н., Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: hv.shelepalo@vntu.edu.ua

Strukovsky Bohdan Yevgenyevich – student of group 1KITS-24b, department of management and information systems security, faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, halksantone@gmail.com

Supervisor **– Shelepalo Halyna Vasylivna –** associate Professor of the Department of Information Technology, Candidate of Physical and Mathematical Sciences, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: hv.shelepalo@vntu.edu.ua