

УДК 339:004.738.5:004.056:316.6

ЗАХИСТ ДАНИХ ТА ДОВІРА КОРИСТУВАЧІВ В ІНФОРМАЦІЙНОМУ БІЗНЕСІ

Гнатенко М.М.

e-mail: maryna.hnatenko@nure.ua

Науковий керівник – старший викладач Прібильнова І.Б.

Харківський національний університет радіоелектроніки, кафедра ЕК
м. Харків, Україна

This work examines data protection and user trust as interdependent foundations of sustainable development in the information business. In the digital economy, data represent a strategic asset, and organizations generate value through collecting, processing, and analyzing personal information. Data protection is defined as a legal, organizational, and technical measures ensuring confidentiality, integrity, and availability of information. User trust is conceptualized as a socio-economic phenomenon reflecting confidence in transparent and secure data practices. The study analyzes key components of data protection systems and factors shaping trust. It concludes that robust security mechanisms and transparency enhance competitiveness and reputation.

У сучасну епоху цифровізації дані стали основним активом для інформаційного бізнесу, оскільки організації отримують дохід шляхом збору, обробки та аналізу великого обсягу персональної інформації. Захист даних загалом означає сукупність правових, організаційних та технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації при її зберіганні, обробці і передачі з використанням сучасних ІТ-рішень [1, с.32]. У контексті бізнес середовища захист інформації передбачає запобігання несанкціонованому доступу до чутливих даних, їхньому викраденню або некоректному використанню, що прямо впливає на репутацію компанії та безпеку користувачів.

Довіра користувачів – це психологічно-соціальний і економічний феномен, який визначає ступінь переконаності споживачів у тому, що платформи та сервіси обробляють їхні дані безпечно, прозоро та відповідно до встановлених норм і стандартів. У сфері інформаційного бізнесу довіра відіграє роль фундаментального елементу, оскільки без неї користувачі не будуть готові надавати свої персональні дані або здійснювати дії, пов'язані з електронними транзакціями. Саме ці два поняття – захист даних та довіра – тісно взаємопов'язані, оскільки ефективний захист даних виступає основою для формування та підтримки довіри аудиторії. При цьому важливою складовою є не тільки технічна безпека, а й прозорість політик щодо даних, зручність управління згодою та правами доступу користувачів [2, с.189].

В інформаційному бізнесі забезпечення захисту даних тісно корелює з правовим регулюванням, зокрема з дотриманням вимог законодавства

щодо обробки персональних даних, використанням хмарних технологій та належним оформленням інформованої згоди користувачів на обробку їхньої інформації.

Довіра користувачів формується через технічний захист та рівень прозорості організації, її здатність пояснювати користувачам, як їхні дані використовуються, та гарантувати виконання політик конфіденційності. У середовищах електронної комерції та бізнес-платформ довіра прямо впливає на рішення користувачів здійснювати покупки або співпрацювати з сервісом, оскільки питання приватності та безпеки стають важливішими за зручність використання сервісу.

Захист даних у інформаційному бізнесі складається з кількох основних компонентів [2, с.189]:

- політики безпеки даних, документованих правил та процедур безпеки;
- технічних механізмів захисту, застосування шифрування, аутентифікації та контролю доступу;
- навчання співробітників основам кібербезпеки;
- системи виявлення порушень безпеки;
- відповідності законам про персональні дані;
- прозорості політик для користувачів, чіткого інформування про обробку даних.

Довіра користувачів, у свою чергу, формується через аспекти, наведені на рис. 1.

Прозорість політик та практик щодо даних	Захист приватності й можливість контролю за своїми даними	Репутація платформи та відгуки інших користувачів
Наявність сертифікацій безпеки та стандартів	Надійність технологічних рішень, які запобігають витоку даних	Комунікація та підтримка при інцидентах безпеки

Рисунок 1 – Фактори, які покращують довіру користувачів у інформаційному бізнесі

Джерело: складено автором на основі [3]

У контексті інформаційного бізнесу захист даних є невід’ємною частиною бізнес-моделі, оскільки порушення конфіденційності може призвести до значних фінансових та репутаційних втрат для компаній. Компанії, які не можуть гарантувати належного рівня безпеки даних,

ризикують втратити користувачів, які усе більше усвідомлюють важливість приватності своїх даних. Окрім цього, рівень довіри користувачів формує вагому конкурентну перевагу, оскільки цифрові сервіси, які впроваджують прозорі політики обробки даних і підтверджують відповідність стандартам безпеки відповідними сертифікаціями, є більш привабливими для клієнтів, зокрема у сфері електронної комерції та хмарних рішень. Сьогодні у сфері захисту даних основними викликами залишаються зростання кіберзагроз, витоки персональних даних та недостатня цифрова обізнаність персоналу. В умовах воєнного стану дані ризики посилюються, тому ефективною відповіддю є впровадження багаторівневих систем кіберзахисту, навчання персоналу, регулярний аудит безпеки та тісна взаємодія з державними органами для забезпечення відповідності нормативним вимогам.

Отже, захист даних та довіра користувачів є взаємопов'язаними елементами успішного функціонування інформаційного бізнесу в цифрову епоху. Ефективний захист ґрунтується на поєднанні політик безпеки, технічних рішень і правових норм, які забезпечують конфіденційність, доступність і цілісність інформації. У свою чергу, формування довіри вимагає прозорості, контролю доступу до даних користувачів та репутаційних гарантій. В умовах зростання кібератак та ризиків витоку даних компанії повинні постійно вдосконалювати стратегії захисту і комунікаційні практики для підтримки довіри клієнтів. Ефективно вибудована система захисту даних істотно знижує ймовірність кіберінцидентів, витоків інформації та фінансових втрат, водночас належний рівень інформаційної безпеки формує передумови для довгострокового розвитку бізнесу, оскільки забезпечує передбачуваність операційних процесів і мінімізує репутаційні ризики.

Список використаних джерел

1. Богом'я В., Черемісіна Л., Ярмолатій А. Безпечна обробка даних в бізнес-інтернет платформах та системах електронної комерції. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2024. № 4. С. 29-34.
2. Діброва І. С., Січко Т. В. Безпека та конфіденційність у базах даних. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса. Природничі та технічні науки*. 2023. Том 2. № 15. С. 187-190. URL: <https://jvestnik-sss.donnu.edu.ua/article/view/14711> (дата звернення: 27.02.2026).
3. Saxena C., Thakur P. Mediating role of trust and privacy concerns between web assurance mechanism and purchase intention of online products. *Telematics and Informatics Reports*. 2024. Volume 16. URL: <https://www.sciencedirect.com/science/article/pii/S277250302400063X> (дата звернення: 27.02.2026).