**Література:**

1. 45 Omnichannel Statistics & Trends (New 2025 Data). *Wiser Notify*. URL: https://wisernotify.com/blog/omnichannel-stats/ (дата звернення: 25.05.2025).
2. B2B Content Marketing Benchmarks, Budgets, and Trends: Outlook for 2025. *Content Marketing Institute*. URL: https://contentmarketinginstitute.com/articles/content-marketing-statistics (дата звернення: 25.05.2025).
3. Leading social media platforms used by marketers worldwide as of January 2024. *Statista*. URL: https://www.statista.com/statistics/259379/social-media-platforms-used-by-marketers-worldwide/ (дата звернення: 25.05.2025).

**Іпполітов Є.М.**

*здобувач третього (освітньо-наукового) рівня вищої освіти*

**Мащенко М.А.**

*д.е.н., професор*
*Національний технічний університет «Харківський політехнічний інститут»,*
*Харків, Україна*

# РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАБЕЗПЕЧЕННІ СТАЛОГО РОЗВИТКУ ПІДПРИЄМСТВА

В умовах глобалізації та диджиталізації економічних процесів питання сталого розвитку підприємств стає все більш актуальним. Концепція сталого розвитку, що базується на гармонійному поєднанні економічних, соціальних та екологічних аспектів діяльності, вимагає від сучасних підприємств формування нових підходів до управління ризиками та забезпечення довгострокової стабільності. Саме тому інформаційна безпека перетворюється з технічної функції на стратегічний чинник, що визначає здатність підприємства досягати цілей сталого розвитку.

Інформаційні активи підприємств становлять значну частину їх загальної вартості та є критично важливими для забезпечення конкурентних переваг. Порушення інформаційної безпеки може призвести не лише до прямих фінансових втрат, але й до довгострокових наслідків, що підривають основи сталого функціонування підприємства. Це зумовлює необхідність розгляду інформаційної безпеки як невід'ємної складової стратегії сталого розвитку підприємства.

Сталий розвиток підприємства характеризується здатністю організації зберігати та нарощувати свій потенціал у довгостроковій перспективі, забезпечуючи при цьому збалансованість економічних, соціальних та екологічних інтересів. Ключовими принципами сталого розвитку є системність, збалансованість, інноваційність, адаптивність та відповідальність перед майбутніми поколіннями [1, с. 55-56].

Дослідники Кицюк В.М., Пупинін О.С. провели аналіз найбільш поширених визначень поняття «інформаційна безпека» [2]. За їх визначенням інформаційна безпека підприємства – це «стан інформаційного середовища господарюючого суб'єкта, при якому зберігаються властивості інформації й інформаційних потоків, та створюються умови протистояння впливу внутрішніх і зовнішніх загроз з метою досягнення бізнес-цілей підприємства» [2]. Тому у контексті сталого розвитку інформаційна безпека виконує роль системоутворюючого фактора, що дозволяє підприємству ефективно управляти знаннями, підтримувати довіру стейкхолдерів та забезпечувати стабільність операційних процесів.

Взаємозв'язок між інформаційною безпекою та сталим розвитком проявляється через декілька ключових механізмів. По-перше, надійний захист інформаційних активів забезпечує стабільність бізнес-процесів та мінімізує ризики операційних збоїв. По-друге, ефективна

система інформаційної безпеки сприяє формуванню довіри з боку клієнтів, партнерів та інвесторів, що є критично важливим для довгострокового успіху підприємства. По-третє, захист інтелектуальної власності та комерційної таємниці дозволяє зберігати конкурентні переваги та забезпечувати інноваційний розвиток.

Економічна складова сталого розвитку підприємства безпосередньо пов'язана з ефективністю використання ресурсів, забезпеченням прибутковості та фінансової стійкості організації. Інформаційна безпека впливає на економічні показники підприємства через декілька основних каналів. Захист від кіберзагроз дозволяє уникнути прямих фінансових втрат, пов'язаних з кіберінцидентами [3].

Інвестиції в інформаційну безпеку сприяють підвищенню операційної ефективності підприємства. Захищені інформаційні системи характеризуються вищою надійністю та продуктивністю, що позитивно впливає на загальні показники діяльності організації. Автоматизація процесів безпеки та впровадження сучасних технологій захисту дозволяють оптимізувати витрати на управління IT-інфраструктурою. Забезпечення високого рівня інформаційної безпеки створює передумови для розширення бізнесу та освоєння нових ринків. Довіра клієнтів до надійності систем захисту їх персональних даних та конфіденційної інформації є важливим конкурентним фактором.

Таким чином, можна зазначити, що успішна інтеграція інформаційної безпеки в систему стратегічного управління підприємства для досягнення сталого розвитку вимагає підходу, що включає довгострокове планування, ефективне управління ризиками, розвиток організаційної культури та постійне вдосконалення. Цей процес передбачає узгодження цілей кібербезпеки з довгостроковими цілями сталого розвитку, створюючи синергетичний ефект, де кожен елемент посилює дію інших компонентів системи. Ключовою передумовою успішної інтеграції є розуміння інформаційної безпеки не як ізольованої технічної функції, а як стратегічного активу, що впливає на економічну ефективність та стійкість підприємства. Подолання існуючих викликів та використання нових можливостей дозволить підприємствам максимізувати синергетичний ефект від поєднання інформаційної безпеки та принципів сталого розвитку.

**Література:**

1. Тарасюк О.В. Теоретичні засади формування концепції сталого розвитку та її практична реалізація на сучасному етапі розвитку суспільства. *Економіка, управління та адміністрування*, 2025. №(111), С. 51–63. DOI: https://doi.org/10.26642/ema-2025-1(111)-51-63 (дата звернення: 28.05.2025).
2. Кицюк В.М., Пупинін О.С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації.* 2024. 2(58), С. 103–108. DOI: https://doi.org/10.31673/2409-7292.2024.020012 (дата звернення: 28.05.2025).
3. Волот О.І. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання. *Центральноукраїнський науковий вісник. Економічні науки.* 2019. № 3(36). С. 238–247. DOI: https://doi.org/10.32515/2663-1636.2018.3(36).238-247 (дата звернення: 28.05.2025).