Міністерство освіти і науки України

Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки,
управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали IX Міжнародної
науково-практичної конференції

15 травня 2025 р.

Полтава
2025

https://www.fsisac.com/hubfs/Knowledge/NavigatingCyber/2024/FSISAC-NavCyber24-Report.pdf

3. Про підвищення рівня захищеності інформаційних систем банків. Постанова Правління Національного банку України №95 від 09 трав. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/v0095500-22#Text

УДК 338:004.7.056

Глушко Аліна Дмитрівна,
кандидат економічних наук, доцент
Тесля Олександр Дмитрович, Лукаш Ілля Миколайович,
студенти
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ЯК БАЗИС ЙОГО ЕКОНОМІЧНОЇ СТІЙКОСТІ

В умовах цифровізації економіки та глобального інформаційного середовища питання забезпечення інформаційної безпеки набуває критично важливого значення для підприємств усіх галузей. Сучасні компанії стикаються з безпрецедентним зростанням кіберзагроз, витоків даних, шахрайських дій та інших інформаційних ризиків, які безпосередньо впливають не лише на операційну діяльність, а й на загальну фінансову стабільність та конкурентоспроможність. Інформаційна безпека сьогодні розглядається не лише як технічна складова IT-інфраструктури, а як стратегічний ресурс, що визначає здатність підприємства адаптуватися до змін, реагувати на зовнішні загрози та зберігати свою економічну сталість у довгостроковій перспективі.

Комплексне управління інформаційною безпекою, що поєднує технічні, організаційні та правові інструменти,

дозволяє формувати ефективну систему ризик-менеджменту. Така система сприяє зменшенню втрат від інцидентів, оптимізації витрат на страхування та резервування, підвищенню інвестиційної привабливості підприємства, а також розширює можливості для впровадження інноваційних бізнес-моделей. Відтак, інформаційна безпека виступає ключовим фактором економічної стійкості, що забезпечує не лише захист активів, але й підтримку стратегічного розвитку підприємства в умовах нестабільного зовнішнього середовища.

Інформаційні активи в сучасних умовах набувають стратегічного значення. Інформація є основою для прийняття управлінських рішень, аналітики, автоматизації бізнес-процесів та розвитку клієнтських сервісів. У цьому контексті забезпечення їх захисту стає необхідною умовою економічної стійкості підприємства. Згідно з аналітичними звітами IBM, у 2024 році середня вартість одного інциденту витоку даних перевищила 4,4 млн доларів США, а середній час виявлення та реагування (Mean Time to Respond, MTTR) залишався на рівні 277 днів за відсутності інвестицій у передові засоби захисту [1, 2]. Водночас впровадження сучасних платформ, таких як SIEM (Security Information and Event Management) та EDR (Endpoint Detection and Response), дозволяє скоротити цей показник до 50–60 днів, що відповідно знижує середню вартість інциденту майже вдвічі – до 2 млн доларів [3].

Наслідки порушень інформаційної безпеки не обмежуються лише витратами на усунення технічних збоїв. Простої IT-систем завдають значних фінансових збитків у вигляді втрат доходу, витрат на відновлення репутації та компенсацій клієнтам. Зокрема, за даними Forbes, середня вартість простою великої організації становить близько 9 000 доларів США за хвилину, або понад 540 000 доларів за годину, включаючи штрафні санкції, втрати продуктивності та репутаційні ризики [4]. У таких умовах навіть базові заходи, зокрема регулярне резервне копіювання та побудова системи

аварійного відновлення, виправдовують себе вже після першого серйозного інциденту.

Організаційні заходи з кібербезпеки — включаючи розробку внутрішніх політик, регламентів та матриць відповідальності — формують безпекову культуру на підприємстві, де кожен працівник розуміє потенційні ризики та наслідки своїх дій. Згідно з дослідженням Invenio IT, попри те, що 62 % компаній у 2024 році скоротили бюджети на IT, підприємства, які спрямували щонайменше 15 % цих витрат на навчання персоналу з питань кібербезпеки, зменшили кількість інцидентів на 45 % [5].

Водночас соціоінженерні атаки залишаються найбільш поширеною формою загроз: Федеральне бюро розслідувань США у 2024 році зафіксувало понад 193 000 випадків фішингових атак, загальні збитки від яких сягнули 16 млрд доларів США [6].

Правове регулювання інформаційної безпеки є критично важливим елементом системного захисту [7]. Зокрема, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» передбачає імплементацію міжнародних стандартів ISO та рекомендацій NIST, а його порушення тягне за собою адміністративну або кримінальну відповідальність. Водночас підприємства, які пройшли сертифікацію за стандартом ISO/IEC 27001, на 30 % рідше потрапляють під перевірки контролюючих органів та на 20 % менше витрачають на юридичний супровід завдяки дотриманню чітких процедур управління ризиками [8].

Слід відмітити, що проактивне управління інформаційними ризиками не лише підвищує рівень кіберзахищеності підприємства, а й забезпечує істотні економічні переваги. Зокрема, страхові компанії враховують наявність систем SIEM (Security Information and Event Management) та планів аварійного відновлення (Disaster Recovery Plan, DRP) у понад 70 % випадків при розрахунку

страхових тарифів, що дозволяє підприємствам знизити витрати на страхування кіберризиків на 25–35 % [9].

Більш того, наявність сертифікації ISO/IEC 27001 слугує сигналом зрілості системи управління інформаційною безпекою та суттєво підвищує інвестиційну привабливість. За даними досліджень Secureframe, компанії з впровадженим стандартом демонструють на 50 % вищу ймовірність залучення венчурного капіталу завдяки довірі інвесторів до механізмів контролю ризиків [9].

Таким чином, інтеграція технічних, організаційних та нормативно-правових засобів інформаційного захисту забезпечує не лише зменшення втрат від кіберінцидентів, але й формує стійке середовище для сталого функціонування та розвитку підприємства в умовах зростаючих цифрових загроз.

Література

1. IBM Security. Cost of a Data Breach Report 2024. URL: https://www.ibm.com/reports/data-breach

2. Atlassian. Calculating the Cost of Downtime. URL: https://www.atlassian.com/incident-management/kpis/cost-of-downtime

3. Microsoft. What is a SIEM? URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

4. The True Cost Of Downtime (And How To Avoid It) / Forbes. URL: https://www.forbes.com/councils/forbestechcouncil/2024/04/10/the-true-cost-of-downtime-and-how-to-avoid-it/

5. Invenio IT. 25 Business Continuity Statistics You Need to Know. URL: https://invenioit.com/continuity/business-continuity-statistics/

6. FBI Internet Crime Complaint Center. 2024 Internet Crime Report. URL: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

7. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., & Cherviak, A. (2023). Cybersecurity And Improvement Of The Information Security System. *Journal of the Balkan Tribological*

Association, 29(5), 818-835.

8. ENISA. ENISA Threat Landscape 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

9. PECB. Benefits of ISO 27001 Certification. URL: https://pecb.com/article/the-main-benefits-of-isoiec-27001-certification

10. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. Economic and cyber security. Kharkiv: PC TECHNOLOGY CENTER, 30–58.

УДК 336.01

Крекотень Ірина Михайлівна,
кандидат економічних наук, доцент
Токар Олександр Олександрович,
студент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ФІНАНСОВА ГРАМОТНІСТЬ НАСЕЛЕННЯ ЯК МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Фінансова грамотність населення України, а саме обізнаність населення в економічній сфері, раціональне та правильне використання фінансової інформації, застосування фінансових знань, є одним із головних механізмів забезпечення економічної безпеки нашої держави. Національна економіка прямо залежить від рівня економічної обізнаності громадян, оскільки обізнаність допомагає зрозуміти ключові фінансові поняття і використовувати їх для ухвалення рішень про доходи, витрати і заощадження, для вибору відповідних фінансових інструментів, планування бюджету, нагромадження коштів на майбутні цілі.