УДК 332.12.658

Соснов І. І.
Igor.Sosnov@khpi.edu.ua, ORCID: 0000-0003-0027-5488
Researcher ID: U-7147-2019
к.т.н., доц., доцент кафедри підприємництва, торгівлі і логістики,
Національний технічний університет
«Харківський політехнічний інститут», м. Харків

Іпполітов Є. М.
Yevhenii.Ippolitov@emmb.khpi.edu.ua, ORCID ID: 0009-0001-3165-4141
Researcher ID: LKN-8500-2024
аспірант, Національний технічний університет
«Харківський політехнічний інститут», м. Харків

СТРАТЕГІЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Анотація. *У статті було проаналізовано стратегічні аспекти забезпечення інформаційної безпеки підприємства, акцентуючи увагу на економічній підсистемі. Обґрунтовано актуальність проблеми в контексті цифрової трансформації економіки та зростання кіберзагроз. Методологічною основою дослідження є системний, процесний та ризик-орієнтований підходи, використано комплекс загальнонаукових методів: аналіз і синтез, порівняльний аналіз, структурно-функціональний аналіз. Проведено літературний огляд праць вітчизняних та зарубіжних науковців, що досліджують питання економічної безпеки, забезпечення інформаційної безпеки та стратегічного управління ризиками. Визначено структуру загроз економічної інфраструктури підприємства, що включає зовнішні кіберзагрози та внутрішні ризики. Визначено стратегічні принципи забезпечення інформаційної безпеки: глибокорівневий захист, мінімальні привілеї, безперервність бізнесу та проактивне управління ризиками. Особливу увагу приділено економічному обґрунтуванню інвестицій у інформаційну безпеку та оцінюванню ефективності заходів захисту. Досліджено взаємозв'язок стратегії інформаційної безпеки із загальною корпоративною та конкурентною стратегіями підприємства. Сформульовано практичні рекомендації щодо стратегічного планування, організаційних механізмів, технологічних рішень та забезпечення безперервності економічної підсистеми. Під час надання рекомендацій було враховано специфіку українських підприємств, які зазнали збройної агресії та комбінованих кібератак. Зазначено, що забезпечення безперервності економічної підсистеми є критично важливим аспектом стратегії інформаційної безпеки. Стратегічний підхід до забезпечення інформаційної безпеки передбачає баланс між технічними засобами захисту та організаційними механізмами. Визначено, що економічне обґрунтування інвестицій у інформаційну безпеку повинно враховувати не лише прямі фінансові втрати від потенційних інцидентів, а й непрямі витрати. Результати дослідження мають практичне значення для формування ефективної стратегії захисту інфраструктури українських підприємств.*

Ключові слова: інформаційна безпека підприємства, економічна підсистема, стратегічне управління, кіберзагрози, управління ризиками, загальна стратегія підприємства.

Sosnov Igor
Igor.Sosnov@khpi.edu.ua, ORCID ID: 0000-0003-0027-5488
Researcher ID: U-7147-2019
PhD in Technical Sciences, Associate Professor, Associate Professor at the Department of Business, Trade and Logistics, National Technical University "Kharkiv Polytechnic Institute", Kharkiv

Ippolitov Yevhenii
Yevhenii.Ippolitov@emmb.khpi.edu.ua, ORCID ID: 0009-0001-3165-4141
Researcher ID: LKN-8500-2024
Postgraduate, National Technical University "Kharkiv Polytechnic Institute", Kharkiv

STRATEGIC INFORMATION SECURITY PROVISION FOR AN ENTERPRISE

Abstract. *The article analyzes strategic aspects of ensuring enterprise information security, focusing on the economic subsystem. The relevance of the problem is substantiated in the context of digital transformation of the economy and increasing cyber threats. The methodological foundation of the research comprises systemic, process-based, and risk-oriented approaches, utilizing a complex of general scientific methods: analysis and synthesis, comparative analysis, and structural-functional analysis. A literature review of works by domestic and foreign scholars investigating issues of economic security, information security provision, and strategic risk management has been conducted. The structure of threats to the enterprise's economic infrastructure has been identified, encompassing external cyber threats and internal risks. Strategic principles of information security provision have been determined: defense in depth, least privilege, business continuity, and proactive risk management. Particular attention is given to the economic justification of investments in information security and the assessment of protective measures' effectiveness. The relationship between information security strategy and the overall corporate and competitive strategies of the enterprise has been examined. Practical recommendations regarding strategic planning, organizational mechanisms, technological solutions, and ensuring continuity of the economic subsystem have been formulated. When providing recommendations, the specificity of Ukrainian enterprises that have experienced armed aggression and combined cyberattacks has been considered. Ensuring continuity of the economic subsystem is a critically important aspect of information security strategy. The strategic approach to ensuring information security presupposes a balance between technical protection means and organizational mechanisms. It has been determined that the economic justification of investments in information security must account for not only direct financial losses from potential incidents but also indirect costs. The research results have practical significance for forming an effective strategy for protecting the infrastructure of Ukrainian enterprises.*

Keywords: enterprise information security, economic subsystem, strategic management, cyber threats, risk management, overall enterprise strategy.

JEL Classification: D81, L86, M15, M21
DOI: https://doi.org/10.32782/2522-1256-2025-47-16

Постановка проблеми. У сучасних умовах цифровізації економіки інформаційна безпека стає стратегічним пріоритетом підприємств. Економічна підсистема підприємства, яка включає фінансові системи, платіжні механізми, системи обліку та управління ресурсами, стає первинною мішенню кібератак через потенційну можливість отримання прямих фінансових вигод зловмисниками. Актуальність проблеми посилюється геополітичною нестабільністю, зростанням кількості кібератак, які спонсоруються іншими державами [1] та збільшенням складності інформаційних загроз. Для українських підприємств

питання захисту критичної інформаційної інфраструктури набуває особливого значення в контексті воєнного стану, посилених комбінованих атак та необхідності забезпечення економічної стійкості країни. Стратегічний підхід до забезпечення інформаційної безпеки передбачає не лише технічні рішення, а й комплексну систему організаційних, економічних та правових заходів, спрямованих на мінімізацію ризиків і забезпечення безперервності бізнес-процесів.

Аналіз останніх досліджень і публікацій. Теоретичні та практичні аспекти забезпечення інформаційної безпеки критичної інфраструктури досліджуються багатьма вітчизняними та зарубіжними науковцями. Проаналізуємо ключові напрацювання в цій галузі. Фундаментальні основи стратегічного управління інформаційною безпекою закладено в роботах Schneier B., який у своїх дослідженнях обґрунтовує як гіперпідключений світ Інтернету речей створює нові загрози безпеці, оскільки цифрові атаки тепер можуть безпосередньо впливати на фізичний світ через вразливі пристрої та критичну інфраструктуру. Автор пропонує системні рішення через державне регулювання та нагляд, оскільки ринок самостійно не може вирішити проблеми безпеки IoT-пристроїв [2].

Економічні аспекти інформаційної безпеки детально проаналізовано в працях Anderson R., який досліджує питання яким чином проектувати, впроваджувати та тестувати системи, які можуть протистояти як помилкам, так і атакам. Його напрацювання охоплює не лише технічні основи, а й демонструє через реальні кейс-стаді як використовувати технології безпеки на практиці. Це доводить, що недостатнє фінансування систем захисту може призвести до катастрофічних економічних наслідків, які в десятки разів перевищують економію на безпеці [3].

Питання захисту критичної інфраструктури розглядаються в роботах Rinaldi S.M., Peerenboom J.P., Kelly T.K., які запропонували концепцію взаємозалежності критичних інфраструктур. Автори доводять, що порушення в одному сегменті інфраструктури може викликати каскадний ефект в інших системах, особливо в економічній підсистемі. Ця концепція стала основою для розробки інтегрованих стратегій захисту, які враховують системні зв’язки між різними компонентами інфраструктури підприємства [4].

Українські науковці Медвідь В. Ю., Правдивець О. М., Кривчун Р. Ю. визначають, що модель системи інформаційної безпеки підприємства поєднує внутрішні та зовнішні фактори, які впливають на загальний стан інформаційної безпеки підприємства та забезпечення безпеки ресурсів. Формування надійної системи інформаційної безпеки підприємства передбачає широкий спектр процедур, спрямованих на мінімізацію внутрішніх та зовнішні хзагроз, які обмежені у часі та ресурсах [5].

Вітчизняний дослідник Задоя В. О. [6] аналізує специфіку забезпечення економічної безпеки підприємств в умовах цифрової трансформації. Автор запропонував концептуальну модель узгодження цифрової стратегії розвитку підприємства із стратегією та механізмами управління його економічною безпекою. Особливу увагу приділено тому факту, що цифрові ініціативи повинні плануватися та реалізовуватися в тісній зв’язці з оцінкою ризиків і впровадженням захисних заходів, тобто цифрова трансформація та безпека мають розглядатися не окремо, а як єдиний процес.

Терзі О. зосередив свою увагу на обґрунтуванні концептуальних положень системи принципів в сфері забезпечення інформаційної безпеки України [7].

Аналіз літературних джерел свідчить про наявність потужної теоретичної бази для розробки стратегій інформаційної безпеки, водночас існує потреба в подальших дослідженнях, орієнтованих на специфіку економічної підсистеми українських підприємств в умовах сучасних викликів.

Постановка завдання. Незважаючи на значні напрацювання, здійснені науковцями, деякі аспекти стратегічного забезпечення інформаційної безпеки підприємства потребують подальшого розвитку та уточнення.

Метою статті є розробка концептуальних засад стратегічного забезпечення інформаційної безпеки підприємства та формування комплексу практичних рекомендацій щодо мінімізації ризиків і забезпечення економічної стійкості організації в умовах зростаючих кіберзагроз.

Виклад основного матеріалу дослідження. Економічна підсистема підприємства являє собою комплекс взаємопов'язаних інформаційних систем та бізнес-процесів, що забезпечують фінансово-господарську діяль-

ність організації. До критичних компонентів економічної інфраструктури належать: системи управління фінансами (ERP-системи), платіжні шлюзи та системи електронних розрахунків, бухгалтерські та податкові системи обліку, системи управління грошовими потоками та ліквідністю, банківські інтерфейси та системи дистанційного банківського обслуговування, системи управління договорами та дебіторською заборгованістю, системи бюджетування та фінансового планування, а також системи аналітики та прийняття управлінських рішень. Критичність цих компонентів визначається тим, що їх порушення або компрометація призводить до прямих фінансових збитків, втрати довіри контрагентів, порушення регуляторних вимог та втрати конкурентних позицій на ринку. Взаємозалежність елементів економічної підсистеми створює системний ризик, коли атака на один компонент може паралізувати всю фінансову діяльність підприємства.

Сучасна екосистема кіберзагроз економічної підсистеми підприємства характеризується високою динамічністю та складністю. Основні категорії загроз включають зовнішні кіберзагрози та внутрішні ризики, кожна з яких має специфічні характеристики та потребує відповідних механізмів протидії [8].

Зовнішні кіберзагрози представлені насамперед цільовими атаками на фінансові системи з метою крадіжки коштів або фінансової інформації. Шифрувальне програмне забезпечення стає дедалі більш поширеним інструментом атак на економічну інфраструктуру, оскільки дозволяє зловмисникам блокувати доступ до критичних фінансових даних та вимагати викуп за їх розблокування. Фішингові атаки, спрямовані на отримання облікових даних співробітників фінансових служб, залишаються одним із найефективніших методів проникнення в корпоративні мережі. DDoS-атаки на платіжні системи та онлайн-сервіси можуть призвести до значних фінансових втрат через неможливість проведення транзакцій. Атаки на ланцюги постачання через компрометацію програмного забезпечення постачальників стають дедалі більш популярними, оскільки дозволяють обійти периметральний захист підприємства. Крадіжки інтелектуальної власності та конфіденційної фінансової інформації можуть нанести довгостроковий збиток конкурентоспроможності підприємства.

Внутрішні загрози не менш небезпечні і часто недооцінюються в корпоративних стратегіях безпеки. Зловмисні дії співробітників, які мають санкціонований доступ до фінансових систем, можуть призвести до значних фінансових зловживань. Випадкові помилки персоналу, викликані недостатньою кваліфікацією або невідповідністю процедур, є однією з найпоширеніших причин інцидентів інформаційної безпеки [9, С. 12]. Недотримання політик безпеки та процедур захисту інформації створює вразливості, які можуть бути використані зовнішніми зловмисниками. Технологічні вразливості інфраструктури, такі як застаріле програмне забезпечення, невстановлені оновлення безпеки, неналежна конфігурація систем, також відносяться до внутрішніх загроз, оскільки виникають внаслідок недостатньої уваги до питань інформаційної безпеки всередині організації.

Ефективна стратегія забезпечення інформаційної безпеки економічної підсистеми підприємства повинна базуватися на фундаментальних принципах, які забезпечують комплексний та системний підхід до захисту інфраструктури. Серед принципів необхідно виділити такі:

1. Принцип глибокорівневого захисту, який передбачає створення багаторівневої системи безпеки, де кожен рівень захищає від специфічних загроз і компенсує можливі вразливості попередніх рівнів.

2. Принцип мінімальних привілеїв, який полягає в наданні користувачам та системам лише тих прав доступу, які абсолютно необхідні для виконання їхніх функціональних обов'язків. Особливо важливим цей принцип є для економічної підсистеми, де доступ до фінансової інформації повинен бути ретельно контрольованим.

3. Принцип забезпечення безперервності функціонування бізнесу критично важливий для економічної підсистеми, оскільки навіть короткочасна недоступність фінансових систем може призвести до значних збитків. Цей принцип реалізується через розробку та регулярне тестування планів відновлення після аварій, створення резервних копій критичних даних з можливістю швидкого відновлення, впровадження відмовостійких систем з дублюванням критичних компонентів, географічно розподілену інфраструктуру для забезпечення стійкості та наявність альтерна-

тивних каналів зв'язку та резервних механізмів виконання критичних операцій.

4. Принцип проактивного управління ризиками. Він передбачає систематичну ідентифікацію, оцінку та обробку ризиків інформаційної безпеки. Для економічної підсистеми це означає регулярне проведення аудитів безпеки та оцінки вразливостей, моніторинг загроз та адаптацію захисних механізмів, впровадження систем управління подіями безпеки та інцидентами, проведення імітаційних вправ та тестування на проникнення, а також постійне вдосконалення процесів забезпечення безпеки на основі аналізу інцидентів.

Також стратегічний підхід до забезпечення інформаційної безпеки вимагає економічного обґрунтування інвестицій та демонстрації їх впливу на фінансові результати підприємства. Традиційний погляд на інформаційну безпеку як на витратний центр поступово змінюється розумінням її ролі як інструменту управління ризиками та забезпечення конкурентних переваг.

Оцінка економічної ефективності заходів інформаційної безпеки базується на методології управління ризиками, яка передбачає визначення вартості інформаційних активів економічної підсистеми, оцінку ймовірності реалізації загроз та потенційного збитку, розрахунок очікуваних втрат без впровадження засобів захисту і порівняння з вартістю впровадження та експлуатації засобів захисту. Ключовим показником має стати коефіцієнт співвідношення вигод і витрат, який визначається як відношення зменшення очікуваних втрат до вартості впровадження та експлуатації засобів захисту. Проте економічне обґрунтування не повинно обмежуватися лише прямими фінансовими втратами від інцидентів. Непрямі витрати часто значно перевищують прямі збитки і включають втрату репутації та довіри клієнтів, штрафні санкції за порушення регуляторних вимог, витрати на розслідування інцидентів та відновлення систем, втрату продуктивності та простої бізнес-процесів, а також довгострокові наслідки для ринкової позиції підприємства.

Для економічної підсистеми особливо важливо враховувати вартість втрати конфіденційної фінансової інформації, яка може включати комерційні таємниці, стратегічні плани, інформацію про угоди та контракти. Компрометація такої інформації може нанести стратегічний збиток конкурентоспроможності підприємства, який важко оцінити кількісно, але який може бути катастрофічним для бізнесу. Оптимальна стратегія інвестування в інформаційну безпеку передбачає балансування між рівнем захисту та економічними можливостями підприємства. Це досягається через пріоритизацію заходів захисту на основі оцінки ризиків, етапне впровадження засобів захисту відповідно до бюджетних можливостей, використання економічно ефективних рішень, таких як хмарні сервіси безпеки, та регулярний перегляд та оптимізацію портфелю інвестицій у безпеку.

Крім того, необхідно зауважити, що технічні засоби захисту є необхідною, але недостатньою умовою забезпечення інформаційної безпеки економічної підсистеми. Ефективна стратегія повинна включати комплекс організаційних механізмів, які створюють культуру безпеки на підприємстві та забезпечують системний підхід до управління інформаційними ризиками.

Створення служби інформаційної безпеки з чітко визначеними повноваженнями та відповідальністю є фундаментом організаційного забезпечення. Керівник служби безпеки повинен мати прямий доступ до вищого керівництва підприємства та достатні повноваження для впровадження політик безпеки. Організаційна структура повинна забезпечувати покриття всіх аспектів інформаційної безпеки, включаючи технічний захист, управління інцидентами, навчання персоналу та забезпечення відповідності регуляторним вимогам.

Розробка та впровадження політик і процедур інформаційної безпеки створює нормативну базу для забезпечення захисту інформаційних активів. Для економічної підсистеми критично важливими є політики управління доступом до фінансових систем, процедури виконання фінансових операцій з механізмами контролю, правила обробки та зберігання конфіденційної фінансової інформації, процедури реагування на інциденти інформаційної безпеки і вимоги до безпеки при роботі з постачальниками та партнерами. Система навчання та підвищення обізнаності персоналу є критично важливим організаційним механізмом, оскільки людський фактор залишається найслабшою ланкою в більшості систем безпеки.

Наступною вимогою є сформована ефективна технологічна стратегія, яка передбачає

інтеграцію різних засобів захисту в єдину систему безпеки з централізованим управлінням та моніторингом. Сучасні рішення передбачають впровадження багатофакторної автентифікації для доступу до фінансових систем, що значно підвищує рівень захисту від несанкціонованого доступу. Централізоване управління обліковими записами дозволяє оперативно надавати та відкликати права доступу, що особливо важливо при звільненні співробітників або зміні їх посадових обов'язків. Системи єдиного входу спрощують управління доступом користувачів до множини економічних застосунків, підвищуючи як безпеку, так і зручність роботи.

Мережеві засоби захисту включають сучасні міжмережеві екрани нового покоління, які здійснюють глибоку інспекцію трафіку та виявляють аномальну активність. Системи запобігання вторгненням аналізують мережевий трафік у реальному часі та блокують підозрілі з'єднання. Технологія мережевої сегментації дозволяє ізолювати економічні системи від інших компонентів корпоративної мережі, обмежуючи можливості латерального переміщення зловмисників у разі компрометації периметру. Системи виявлення аномалій на основі машинного навчання здатні ідентифікувати нетипову поведінку в мережі, яка може свідчити про атаку.

Захист інформації на рівні даних включає технології шифрування даних у базах даних та файлових системах, що забезпечує конфіденційність інформації навіть у разі несанкціонованого доступу до носіїв. Шифрування каналів передачі даних захищає фінансову інформацію під час обміну між системами. Системи запобігання витоку даних контролюють переміщення конфіденційної інформації та блокують спроби її несанкціонованої передачі за межі організації. Технології маскування та знеособлення даних дозволяють використовувати реальні дані для тестування та розробки без ризику їх компрометації.

Системи моніторингу та аналітики безпеки забезпечують централізований збір та аналіз подій безпеки з усіх компонентів інфраструктури. Захист кінцевих точок включає антивірусне програмне забезпечення нового покоління, яке використовує поведінковий аналіз та машинне навчання для виявлення невідомих загроз. Системи управління мобільними пристроями забезпечують захист корпоративної інформації на смартфонах та планшетах співробітників. Технології контейнеризації та віртуалізації дозволяють ізолювати економічні застосунки та обмежувати вплив можливої компрометації на інші системи.

Важливого значення в процесі стратегічного забезпечення інформаційної безпеки відіграє забезпечення відповідності регуляторним вимогам та міжнародним стандартам інформаційної безпеки. Для українських підприємств актуальними є вимоги національного законодавства, зокрема Закону України про захист інформації в інформаційно-телекомунікаційних системах [10], вимог Національного банку України щодо кібербезпеки для фінансових установ, положень Закону України про критичну інфраструктуру і вимог щодо захисту персональних даних відповідно до національного законодавства та GDPR для компаній, що працюють з європейськими партнерами [11].

Міжнародні стандарти, зокрема родина стандартів ISO/IEC 27000, надають систематизований підхід до побудови системи управління інформаційною безпекою [12]. Впровадження цих стандартів дозволяє підприємству не лише підвищити рівень захисту, а й продемонструвати відповідність міжнародним вимогам, що важливо для роботи з іноземними партнерами та інвесторами. Стандарти PCI DSS є обов'язковими для підприємств, що обробляють платіжні картки, і встановлюють детальні вимоги до захисту інформації про платіжні картки [13].

Процес забезпечення відповідності включає регулярні аудити відповідності вимогам законодавства та стандартів, впровадження контролів безпеки відповідно до вимог регуляторів, документування політик, процедур та доказів виконання вимог, регулярне тестування ефективності впроваджених контролів і підготовку звітності для регуляторних органів та зацікавлених сторін. Відповідність регуляторним вимогам не повинна розглядатися як формальна процедура, а має бути інтегрована в загальну стратегію інформаційної безпеки. Багато вимог регуляторів відображають найкращі практики безпеки і їх виконання об’єктивно підвищує рівень захисту економічної інфраструктури підприємства.

Отже, ефективне стратегічне управління інформаційною безпекою економічної підсистеми вимагає систематичного підходу до планування, впровадження та постійного вдосконалення заходів захисту. Стратегія інфор-

маційної безпеки повинна бути узгоджена із загальною бізнес-стратегією підприємства та підтримувати досягнення його стратегічних цілей. Процес стратегічного планування включає аналіз поточного стану інформаційної безпеки та ідентифікацію прогалин у захисті. Це передбачає проведення комплексного аудиту безпеки економічних систем, оцінку відповідності існуючих заходів захисту від загроз, аналіз інцидентів минулого періоду та їх причин і порівняння з найкращими практиками та стандартами галузі.

На основі аналізу поточного стану формується цільова архітектура безпеки, яка визначає бажаний стан системи захисту економічної інфраструктури. Цільова архітектура повинна відображати баланс між рівнем безпеки, функціональними потребами бізнесу та доступними ресурсами. Розробка дорожньої карти переходу від поточного до цільового стану включає визначення пріоритетних проєктів та ініціатив, етапність впровадження з урахуванням бюджетних обмежень, розподіл відповідальності та ресурсів і встановлення ключових показників ефективності та контрольних точок.

Саме тому, стратегія забезпечення інформаційної безпеки не може розглядатися ізольовано від загальної корпоративної стратегії підприємства. Вибір підходів до захисту економічної інфраструктури має бути узгоджений зі стратегічними цілями організації, її конкурентною позицією на ринку та обраною моделлю бізнесу. Інтеграція стратегії інформаційної безпеки з корпоративною стратегією забезпечує оптимальне використання ресурсів та максимальну підтримку бізнес-цілей.

На основі проведеного дослідження можна сформулювати комплекс практичних рекомендацій для підприємств щодо стратегічного забезпечення інформаційної безпеки економічної підсистеми критичної інфраструктури:

1. Підприємствам рекомендується розглядати інформаційну безпеку як стратегічний пріоритет, що вимагає уваги вищого керівництва. Стратегія інформаційної безпеки повинна бути невід'ємною частиною корпоративної стратегії та узгоджуватися з бізнес-цілями організації. Необхідно обирати підхід до забезпечення безпеки економічної підсистеми відповідно до загальної конкурентної стратегії підприємства: підприємства-лідери за витратами мають фокусуватися на економічно ефективних стандартизованих рішеннях, компанії з стратегією диференціації – інвестувати в передові технології безпеки як елемент конкурентної переваги, організації зі стратегією фокусування – створювати спеціалізовані рішення для своєї ніші, інноваційні підприємства – впроваджувати безпеку у процеси розробки, а глобальні корпорації – розробляти уніфіковані стандарти з урахуванням місцевої специфіки. Стратегічне планування безпеки повинно базуватися на систематичній оцінці ризиків з урахуванням специфіки економічної підсистеми та включати сценарне планування для підготовки до різних типів кризових ситуацій.

2. Критично важливим є формування культури безпеки на всіх рівнях організації через регулярне навчання персоналу, особливо співробітників економічних служб. Необхідно розробити та впровадити чіткі політики та процедури інформаційної безпеки, адаптовані до специфіки економічних процесів підприємства. Рекомендується створити спеціалізовану команду реагування на інциденти з чітко визначеними ролями, відповідальністю та процедурами ескалації.

3. Підприємствам рекомендується впроваджувати багаторівневий захист інфраструктури, що включає захист периметру, сегментацію мережі, захист на рівні застосунків та захист даних. Критично важливим є впровадження систем централізованого моніторингу та аналізу подій безпеки для оперативного виявлення аномалій у роботі економічних систем. Необхідно забезпечити шифрування конфіденційних фінансових даних як у спокої, так і під час передачі.

4. Інвестиції в інформаційну безпеку повинні базуватися на економічному обґрунтуванні через оцінку ризиків та потенційних збитків. Рекомендується розглядати витрати на інформаційну безпеку не як непродуктивні витрати, а як інвестиції в управління ризиками та забезпечення безперервності бізнесу.

5. Критично важливим є розробка та регулярне тестування планів забезпечення безперервності бізнесу та відновлення після аварій для економічної підсистеми. Необхідно визначити цільові показники часу відновлення та максимально допустимої втрати даних для кожної критичної економічної системи. Рекомендується створити резервні потужності та альтернативні канали виконання критичних фінансових операцій.

6. Підприємствам рекомендується систематично відслідковувати зміни в регуляторних вимогах та своєчасно адаптувати системи захисту. Доцільно розглянути можливість сертифікації системи управління інформаційною безпекою згідно з ISO/IEC 27001, що демонструє відповідність міжнародним стандартам.

7. Інформаційна безпека є не одноразовим проєктом, а безперервним процесом. Рекомендується регулярно проводити аудити безпеки та тестування на проникнення для виявлення вразливостей. Необхідно аналізувати всі інциденти інформаційної безпеки та впроваджувати коригувальні заходи для запобігання повторенню.

8. В умовах збройної агресії проти України особливої актуальності набувають питання забезпечення стійкості інфраструктури підприємства до цільових кібератак. Рекомендується розглянути можливість географічно розподіленої інфраструктури з розміщенням критичних систем поза територією України. Необхідно підготувати сценарії роботи в умовах обмеженої доступності.

Висновки і перспективи подальших досліджень у даному напрямі. Стратегічне забезпечення інформаційної безпеки критичної інфраструктури підприємства, зокрема економічної підсистеми, є комплексним завданням, що вимагає системного підходу та інтеграції технічних, організаційних та економічних механізмів захисту. Економічна підсистема підприємства є пріоритетною метою кіберзагроз через потенціал прямих фінансових втрат та високу цінність інформації. Захист від кіберзагроз повинен розглядатися як стратегічний пріоритет, що вимагає постійної уваги вищого керівництва та адекватних інвестицій. Крім того, ефективна стратегія інформаційної безпеки не може бути універсальною, вона повинна бути узгоджена із загальною корпоративною та конкурентною стратегією підприємства. Стратегічний підхід до забезпечення інформаційної безпеки передбачає баланс між технічними засобами захисту та організаційними механізмами. Найсучасніші технології захисту не будуть ефективними без відповідної культури безпеки, чітких політик та процедур, навченого персоналу та ефективних процесів управління інцидентами. Економічне обґрунтування інвестицій у інформаційну безпеку повинно враховувати не лише прямі фінансові втрати від потенційних інцидентів, а й непрямі витрати, такі як втрата репутації, регуляторні санкції, втрата конкурентних позицій. Методологія управління ризиками дозволяє приймати обґрунтовані рішення щодо інвестицій в захист на основі оцінки ймовірності реалізації загроз та потенційного збитку. Також забезпечення безперервності економічної підсистеми є критично важливим аспектом стратегії інформаційної безпеки. Навіть короткочасна недоступність фінансових систем може призвести до значних втрат та порушення довіри стейкхолдерів. Відповідність регуляторним вимогам та міжнародним стандартам інформаційної безпеки не повинна розглядатися як формальна процедура. Для українських підприємств особливо актуальною є гармонізація з європейськими стандартами в контексті євроінтеграції. Стратегія інформаційної безпеки повинна бути динамічною та адаптивною до змін у бізнес-середовищі, ключових загроз та технологічних можливостей. Регулярний перегляд та оновлення стратегії, моніторинг нових загроз, впровадження нових технологій захисту є необхідними елементами ефективного стратегічного управління безпекою. Для українських підприємств стійкість економічної підсистеми до цільових атак є не лише питанням корпоративної безпеки окремого підприємства, а й елементом економічної безпеки держави. Активна співпраця бізнесу, державних органів та міжнародних партнерів у сфері кібербезпеки є критично важливою для забезпечення стійкості економіки країни. Перспективи подальших досліджень передбачають розробку галузевоспецифічних моделей оцінки ризиків для економічних підсистем підприємств різних секторів економіки.

ЛІТЕРАТУРА

1. Softlist. Кібератаки в Україні: зростання на 70% та як захистити бізнес у 2025 році. 2025. URL: https://softlist.ua/cases/cyberattacksinukraine

2. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W. W. Norton & Company, 2019. 336 p.

3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Wiley, 2020. 1232 p.

4. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*. 2001. Vol. 21. No. 6. P. 11–25. DOI: https://doi.org/10.1109/37.969131

5. Медвідь В.Ю., Правдивець О.М., Кривчун Р.Ю. Теоретико-методичні засади формування системи управління інформаційною безпекою підприємства. *Агросвіт*. 2023. № 1. С.24–30. DOI: https://doi.org/10.32702/2306-6792.2023.1.24

6. Задоя В.О. Інституційні та управлінські аспекти забезпечення економічної безпеки бізнесу в умовах цифрової економіки. *Ефективна економіка.* 2025. № 7. DOI: https://doi.org/10.32702/2307-2105.2025.7.71%20

7. Терзі О. Принципи забезпечення інформаційної безпеки держави: досвід України та зарубіжних країн. *Право та державне управління.* 2024. № 3. С. 51–57. DOI: https://doi.org/10.32782/pdu.2024.3.7

8. Топалов В. М. Стратегічні орієнтири забезпечення інформаційної безпеки суб'єктів малого підприємництва. *Економіка та суспільство.* 2025. Вип. 75. DOI: https://doi.org/10.32782/2524-0072/2025-75-92

9. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. Київ, 2025. № 10. 166 с.

10. «Про захист інформації в інформаційно-телекомунікаційних системах». Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/sho/80/94-вр

11. «Про критичну інфраструктуру». Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization, 2022.

13. Payment Card Industry Data Security Standard (PCI DSS) v4.0. PCI Security Standards Council, 2022. 362 p.

REFERENCES

1. Softlist (2025), "Cyberattacks in Ukraine: 70% increase and how to protect business in 2025", available at: https://softlist.ua/cases/cyberattacksinukraine

2. Schneier, B. (2019), *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W. W. Norton & Company, New York, USA.

3. Anderson, R. (2020), *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd ed., Wiley, Hoboken, USA.

4. Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K. (2001), "Identifying, understanding, and analyzing critical infrastructure interdependencies", *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, DOI: https://doi.org/10.1109/37.969131

5. Medvid, V. Yu., Pravdyvets, O. M. and Kryvchun, R. Yu. (2023), "Theoretical and methodological principles of forming an information security management system for an enterprise", *Ahrosvit*, vol. 1, pp. 24–30, DOI: https://doi.org/10.32702/2306-6792.2023.1.24

6. Zadoia, V.O. (2025), "Institutional and managerial aspects of ensuring economic security of business in the digital economy", *Efektyvna ekonomika*, vol. 7, DOI: https://doi.org/10.32702/2307-2105.2025.7.71

7. Terzi, O. (2024), "Principles of ensuring state information security: experience of Ukraine and foreign countries", *Pravo ta derzhavne upravlinnia*, vol. 3, pp. 51–57, DOI: https://doi.org/10.32782/pdu.2024.3.7

8. Topalov, V. M. (2025), "Strategic guidelines for ensuring information security of small business entities", *Ekonomika ta suspilstvo*, vol. 75, DOI: https://doi.org/10.32782/2524-0072/2025-75-92

9. Dovhan, O., Lytvynova, L. and Dorohykh, S. (2025), *Kiberbezpeka v informatsiinomu suspilstvi: Informatsiino-analitychnyi daidzhest* [Cybersecurity in the Information Society: Information and Analytical Digest], Derzhavna naukova ustanova "Instytut informatsii, bezpeky i prava NAPrN Ukrainy"; Natsionalna biblioteka Ukrainy im. V.I.Vernadskoho, Kyiv, Ukraine, vol. 10, 166 p.

10. The Verkhovna Rada of Ukraine (1994), The Law of Ukraine "On the protection of information in information and telecommunication systems", available at: https://zakon.rada.gov.ua/laws/show/80/94-вр

11. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine "On critical infrastructure", available at: https://zakon.rada.gov.ua/laws/show/1882-20

12. ISO/IEC 27001:2022 (2022), Information security, cybersecurity and privacy protection – Information security management systems – Requirements, International Organization for Standardization, Geneva, Switzerland.

13. PCI Security Standards Council (2022), Payment Card Industry Data Security Standard (PCI DSS) v4.0, PCI Security Standards Council, Wakefield, USA, 362 p.

Стаття надійшла: 21.11.2025
Стаття прийнята: 09.12.2025
Стаття опублікована: 30.12.2025