https://doi.org/10.12958/1817-3772-2026-2(84)-220-232

УДК 004.056:005.2

Олексій Миколайович Гуцалюк,
академік АЕН України, д-р екон. наук, професор,
ORCID 0000-0002-6541-4912
e-mail: alex-g.88@ukr.net;
Яна Миколаївна Манькута,
канд. екон. наук, доцент,
ORCID 0000-0003-1623-5149
e-mail: yana.mankuta.suem@gmail.com;
Ірина Володимирівна Захарова,
канд. істор. наук, доцент,
ORCID 0000-0001-5482-4652
e-mail: zaharova.ira2308@gmail.com;
Євген Ігорович Терновий,
викладач,
ORCID 0009-0005-7172-8263
e-mail: evgenternovij@gmail.com
ПЗВО «Східноєвропейський університет імені Рауфа Аблязова», м. Черкаси

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ І КОРПОРАТИВНОЇ БЕЗПЕКИ В ІНТЕГРОВАНІЙ ЕКОСИСТЕМІ ЕКОНОМІКО-ПРАВОВОГО УПРАВЛІННЯ ПІДПРИЄМСТВАМИ ТА ІТ-КЛАСТЕРАМИ

Постановка проблеми. Цифровізація економіки, розширюючи можливості бізнесу, водночас стає критичним фактором конкурентоспроможності підприємств та створює нові виклики у сфері інформаційної безпеки. Стрімкий розвиток технологій зумовлює появу нових загроз для інформаційних ресурсів, що потребує вдосконалення механізмів ефективного управління підприємством[1].

В умовах воєнного стану в Україні питання захисту інформації набувають стратегічного значення. Обмеженість ресурсів, масовий перехід до дистанційного формату роботи та необхідність адаптації бізнес-процесів зумовлюють потребу у впровадженні надійних цифрових інструментів для забезпечення ефективного управління підприємствами. Сучасні суб'єкти господарювання стикаються з широким спектром загроз: несанкціонований доступ до конфіденційних даних може призвести до втрати комерційної таємниці, витоку службової кореспонденції, порушення цілісності інформаційних систем або фальсифікації документації. Відтак, ключовим завданням технологій захисту є запобігання втраті, підробці або несанкціонованому знищенню даних, що є критично важливим для стабільності всієї системи управління [1].

Особливістю сучасних інформаційних систем є територіальна розподіленість компонентів, інтенсивний обмін інформацією між ними, широкий спектр способів представлення, зберігання та передачі даних, а також одночасна участь у процесах обробки інформації великої кількості користувачів із різними правами доступу.

Цифрова трансформація охоплює всі рівні діяльності підприємств – від операційного управління до стратегічного планування та розбудови фінансової архітектури. Сучасні інформаційні технології кардинально змінюють парадигму прийняття рішень, забезпечуючи гнучку адаптацію до мінливого зовнішнього середовища та раціоналізацію використання ресурсів. Наприклад, розвиток фінансового сектору безпосередньо залежить від функціонування електронних платіжних систем, мобільного банкінгу та цифрових платформ управління капіталом, які не лише прискорюють проведення господарських операцій, а й підвищують загальну прозорість та ефективність фінансових потоків [2].

Проте значна частина підприємств не повною мірою усвідомлює потенційні переваги впровадження комплексних систем захисту інформації та потребу в інтеграції технологічних рішень із механізмами правового регулювання. Відтак постає необхідність розробки науково обґрунтованих підходів до побудови систем інформаційної безпеки, які б гармонізували специфіку бізнес-процесів, законодавчі вимоги та економічну доцільність відповідних інвестицій [3].

[1] Манькута Я. М., Циба А. М., Біліценко І. О. Детермінанти фінансового інжинірингу підприємства: цифрові технології бізнес-управління та системи аналізу даних в бізнес-моделюванні. *Вісник Східноєвропейського університету економіки і менеджменту. Сер.: Економіка і менеджмент*. 2025. № 1 (33). С. 238–252

Таким чином, постановка проблеми полягає у дослідженні технологій інформаційного забезпечення та безпеки як ключових детермінант ефективного економіко-правового управління підприємствами в умовах цифрової трансформації економіки.

Екосистемний підхід передбачає розгляд інформаційного забезпечення та безпеки не як окремих технічних інструментів, а як взаємопов'язаних складників цифрової інфраструктури, інтегрованих у бізнес-процеси, правові механізми та організаційні структури. Така екосистема базується на динамічній взаємодії технологічних, юридичних та економічних факторів, синергія яких формує захищене інформаційне середовище підприємства.

Аналіз останніх досліджень та публікацій. Проблематика інформаційної безпеки підприємств перебуває у центрі уваги численних вітчизняних та зарубіжних науковців. Питання цифровізації управління бізнес-процесами розглядали Л. Мельник, О. Карінцева, Л. Калініченко, М. Харченко та С. Тарасенко [4], а також Г. Долга й О. Хитрова [5], які дослідили вплив цифрових технологій на ефективність менеджменту та визначили ключові тенденції трансформації бізнесу.

Фундаментальні засади криптографічного захисту інформації закладені у працях А. Шаміра, Р. Рівеста та Л. Адлемана [6] (авторів алгоритму RSA); принципи побудови захищених систем сформульовані О. Керкгоффом[1], а практичні аспекти застосування криптографії у корпоративних мережах детально вивчені Б. Шнайєром[2]. Технічні методи захисту та роль бізнес-аналітики в обробці даних для прийняття управлінських рішень обґрунтували Х. Чен, Р. Чанг та В. Сторі [7].

Значний внесок в адаптацію міжнародних практик до українських реалій зробили вітчизняні дослідники: О. Щедріна[3], Н. Гончаренко[4], Н. Кащена, Р. Остапенко, В. Велієва [8], О. Буркін[5], Л. Вербівська та О. Буринська [9].

Нормативну базу формують міжнародні стандарти серії ISO/IEC 27000 та публікації NIST[6], які гармонізовані в Україні через систему ДСТУ[7]. Методологію моделювання систем захисту розвивали О. Марбан, Г. Маріскал, Х. Сеговія [10], Д. Дакіч, Д. Стефанович [11] та М. Янс [12].

Основою нормативно-правового регулювання інформаційної безпеки та захисту даних в Україні є закони «Про інформацію»[8], «Про Національну програму інформатизації»[9], «Про захист інформації в інформаційно-комунікаційних системах»[10], «Про основні засади забезпечення кібербезпеки України»[11], «Про електронну ідентифікацію та електронні довірчі послуги»[12], «Про державну таємницю»[13]. Саме ці нормативні акти закладають правовий фундамент для розробки цілісної екосистеми економіко-правового управління безпекою підприємства, що в умовах еволюції кіберзагроз набуває пріоритетного значення. Відтак, в умовах стрімкої еволюції кіберзагроз, розробка цілісної екосистеми економіко-правового управління безпекою підприємства набуває пріоритетного значення.

Виділення невирішених раніше частин загальної проблеми. Попри ґрунтовні теоретичні напрацювання щодо впровадження технологій захисту інформації та систем бізнес-аналітики, низка концептуальних питань залишається недостатньо висвітленою.

По-перше, відсутні комплексні моделі, які б забезпечували синергію технологічних засобів захисту з економіко-правовими векторами управління.

[1] Kerckhoffs A. La cryptographie militaire. *Journal des sciences militaires*. 1883. Vol. IX. P. 5–38, 161–191.

[2] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. John Wiley & Sons, 1996. 784 p.

[3] Щедріна О. І. Системний аналіз як інструмент прийняття управлінських рішень в бізнесі. *Моделювання та інформаційні системи в економіці*. 2020. № 99. С. 169-183.

[4] Гончаренко Н. Г. Роль комплексного системного аналізу в управлінні підприємством. *Економіка та суспільство*. 2017. № 12. С. 683-686.

[5] Буркін О. М. Аналіз форм і видів цифрових технологій та їх вплив на сучасне суспільство у динамічному ринковому середовищі. *Економіка і суспільство*. 2023. Вип. 51. С. 54-64.

[6] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO, 2022; ISO 8532:1995. Banking – Key management (retail). ISO, 1995; ISO 13888:2020. IT Security techniques – Non-repudiation. ISO, 2020; NIST Special Publication 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST, 2010. 131 p.

[7] ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT). Київ: ДП «УкрНДНЦ», 2016. 34 с.; ДСТУ 28147:2009. Інформаційні технології. Криптографічний захист інформації. Алгоритм криптографічного перетворення. Київ: Держспоживстандарт України, 2009. 13 с.

[8] Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12

[9] Про Національну програму інформатизації: Закон України від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20

[10] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (у редакції від 04.06.2020). URL: https://zakon.rada.gov.ua/laws/show/80/94-вр

[11] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

[12] Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19

[13] Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12

Більшість досліджень мають вузькоспеціалізований характер (суто технічний, організаційний або юридичний), тоді як сучасне середовище потребує цілісної парадигми, що інтегрує ці складові у єдиний функціональний контур. Екосистемний підхід вимагає розгляду безпеки як адаптивної системи, де IT-рішення (DLP, криптографічні шлюзи) синхронізовані з організаційними політиками та правовими нормами. Відсутність методології побудови таких самоорганізованих систем створює суттєву наукову прогалину.

По-друге, потребують глибшої адаптації міжнародні стандарти безпеки до специфіки українського бізнес-ландшафту, що функціонує в умовах воєнного стану, обмеженості ресурсів та особливих регуляторних вимог.

По-третє, гострою залишається проблема технологічного консерватизму та низької обізнаності малого й середнього бізнесу щодо необхідності впровадження систем класу SIEM чи IDS/IPS[1]. Брак методичного інструментарію для вибору оптимальних технологій захисту, виходячи з економічної доцільності, ускладнює прийняття стратегічних управлінських рішень.

По-четверте, бракує галузево-орієнтованих критеріїв оцінки ефективності систем безпеки. Універсальні методики не дозволяють адекватно оцінити вартість інформаційних активів та специфічні ризики конкретних бізнес-моделей.

По-п'яте, недостатньо вивченим є потенціал інтеграції інноваційних технологій (блокчейн, штучний інтелект) у контур інформаційної безпеки для автоматизації реагування на інциденти.

Окремого вивчення потребує архітектура комплексного захисту потоків даних у системах документообігу, де політика безпеки, криптографія та моніторинг мають утворювати єдину екосистему протидії загрозам.

Метою статті є теоретичне обґрунтування екосистемного підходу до захисту інформаційних ресурсів підприємства та розробка концептуальних засад інтеграції технологій корпоративної безпеки в систему економіко-правового управління для забезпечення стійкості та конкурентоспроможності бізнесу в умовах цифрової трансформації.

Виклад основного матеріалу дослідження. В умовах використання автоматизованих інформаційних систем під безпекою розуміється стан захищеності інформаційної системи від внутрішніх і зовнішніх загроз. Показник захищеності являє собою характеристику засобів системи, що описується певною групою вимог, які варіюються за рівнем і глибиною залежно від класу захищеності.

Основними об'єктами системи інформаційної безпеки для організації є:

1) інформаційні ресурси з обмеженим доступом, що становлять комерційну, банківську таємницю або інші чутливі відносно випадкових і несанкціонованих дій і порушень безпеки ресурси;

2) інформаційні технології, регламенти і процедури збору, обробки, зберігання та передачі інформації;

3) інформаційна інфраструктура, що включає технічні та програмні засоби і системи обробки й аналізу інформації, канали інформаційного обміну і телекомунікації, системи і засоби захисту.

Множина потенційних загроз безпеки інформації за природою їх виникнення поділяється на два класи: природні (об'єктивні) і штучні (суб'єктивні). Природні загрози викликані впливами на інформаційну систему об'єктивних фізичних процесів техногенного характеру або стихійних природних явищ. Штучні загрози викликані діяльністю людини і можуть бути ненавмисними (помилки персоналу, збої обладнання через неправильну експлуатацію) або навмисними (цілеспрямовані атаки зловмисників).

Основні джерела загроз інформаційної безпеки наступні: ненавмисні порушення встановлених регламентів збору, обробки і передачі інформації користувачами; навмисні дії легально допущених до інформаційних ресурсів користувачів (у корисливих цілях, з примусу третіми особами, зі злим умислом); діяльність злочинних груп і формувань, політичних і економічних структур із добування інформації, нав'язування неправдивої інформації, порушення працездатності інформаційних систем; віддалене несанкціоноване втручання через канали підключення до зовнішніх мереж; помилки при розробці компонентів інформаційної системи, відмови і збої технічних засобів; аварії, стихійні лиха.

Найбільш важливими загрозами безпеці інформації є порушення функціональності компонентів системи, порушення цілісності інформаційних ресурсів та їх фальсифікація, порушення конфіденційності відомостей, що становлять комерційну таємницю.

Забезпечення безпеки інформації полягає у розв'язанні трьох взаємопов'язаних задач: конфіденційності, цілісності та доступності (тріада CIA – Confidentiality, Integrity, Availability). Задача забезпечення конфіденційності полягає у захисті інформації від ознайомлення з нею осіб, що не мають права доступу. Забезпечення цілісності передбачає захист від навмисної або ненавмисної зміни інформації особами, що не мають на це права. Забезпечення доступності означає надання користувачам

[1] Дудикевич В. Б., Опірський І. Р. Аналіз моделей захисту інформації в інформаційних мережах держави. *Системи обробки інформації*. 2016. № 4. С. 86-89; Потій О. В., Горбенко Ю. І., Замула О. А. та ін. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки. *Системи управління, навігації та зв'язку*. 2017. № 3 (43). С. 102-110.

всієї наявної інформації відповідно до встановлених для них прав.

Для оцінки реального стану безпеки інформаційної системи застосовується система показників та ієрархія класів безпеки. Рівні захисту або рівні вразливості інформаційних систем класифікуються за шістьма рівнями (рис. 1):

1) фізичний рівень визначає ефективність захисту технічних елементів (сервери, робочі станції, мережеве обладнання, лінії зв'язку);

2) технологічний рівень відображає захист апаратно-програмних процедур (операційні системи, СУБД, прикладне ПЗ);

3) логічний рівень характеризує адекватність логічних основ механізму безпеки та організації зберігання інформації;

4) людський рівень відображає кваліфікованість персоналу на стадіях проектування та експлуатації;

5) законодавчий рівень визначає комплекс законодавчих і нормативно-правових актів;

6) організаційний рівень передбачає комплекс організаційних заходів, що регламентують процеси експлуатації системи [6].

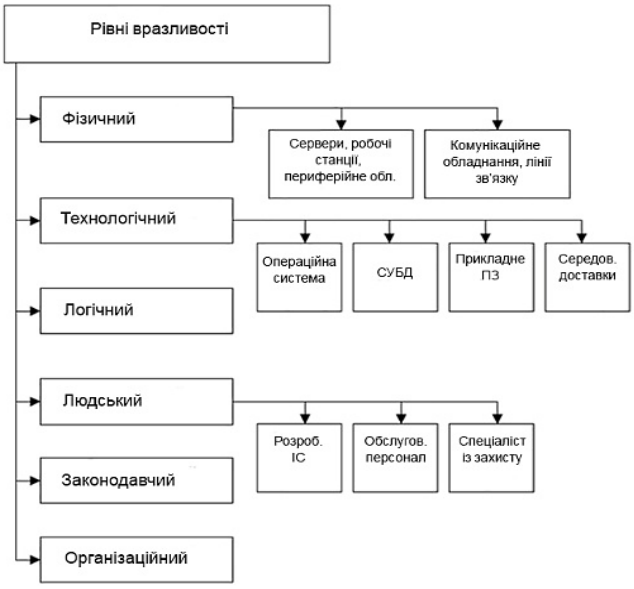

Рис. 1. **Рівні вразливості інформації**
Джерело: побудовано авторами за [6]

Основою формального опису системи захисту традиційно вважається модель системи захисту з повним перекриттям, в якій розглядається взаємодія області загроз, захищаємої області та системи захисту[1]. Таким чином маємо три множини: $T = t_i$ – множина загроз безпеки, $O = o_i$ – множина ресурсів захищеної системи, $M = m_k$ – множина механізмів безпеки інформаційної системи.

Елементи цих множин знаходяться між собою в певних відносинах, що власне і утворюють систему захисту. Для опису системи захисту зазвичай використовується графова модель. Множина відносин «загроза-об'єкт» утворює дводольний граф (T, O). Мета захисту полягає в тому, щоб перекрити всі можливі ребра в графі. Це досягається введенням третього набору M, в результаті чого виходить тридольний граф (T, M, O). Розвиток моделі передбачає введення ще двох елементів V – набору вразливих місць, який визначається підмножиною декартового добутку $\mathrm{T} * \mathrm{O}$: $v_r =< t_i, o_j >$, B – набору бар'єрів, який визначається декартовим добутком $\mathrm{V} * \mathrm{M}$: $b_l = < t_i, o_j, m_k >$.

В результаті отримуємо систему, що складається з п'яти елементів $< \mathrm{T}, M, O, V, B >$ і описує систему захисту з урахуванням наявності вразливостей (рис. 2).

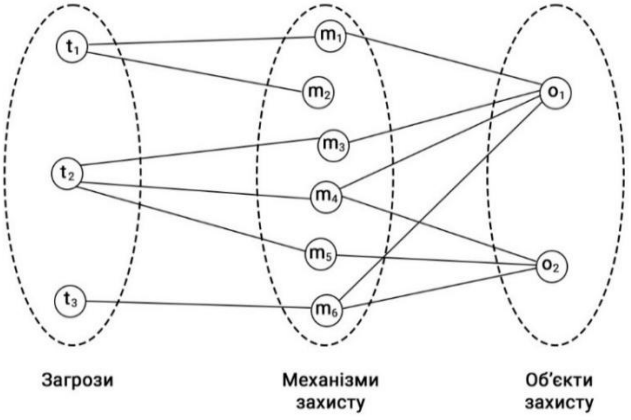

Рис. 2. **Модель системи захисту з повним перекриттям**
Джерело: побудовано авторами за (Дудикевич В. Б., Опірський І. Р. Аналіз моделей захисту інформації в інформаційних мережах держави. *Системи обробки інформації*. 2016. № 4. С. 86–89)

В системі з повним перекриттям для будь-якої вразливості існує бар'єр, що її усуває. Іншими словами, в подібній системі для всіх можливих загроз безпеки існують механізми захисту, що перешкоджають здійсненню цих загроз. Дана умова є першим фактором, що визначає захищеність інформаційної системи. Другим фактором вважається міцність і надійність механізмів захисту.

Тому в якості характеристик елемента набору бар'єрів $b_l =< t_i, o_j, m_k >$ може розглядатися набір $< P_l, L_l, R_l >$, де P_l – ймовірність появи загрози, L_l – величина збитку при вдалому здійсненні загрози щодо об'єктів, які захищаються (рівень серйозності загрози), а R_l – ступінь опірності механізму захисту, що характеризується ймовірністю його подолання.

[1] Дудикевич В. Б., Опірський І. Р. Аналіз моделей захисту інформації в інформаційних мережах держави. *Системи обробки інформації*. 2016. № 4. С. 86–89.

Надійність бар'єру $b_l =< t_i, o_j, m_k >$ характеризується величиною залишкового ризику $Risk_l$, пов'язаного з можливістю створення іншої загрози t_i щодо об'єкта інформаційної системи o_j при використанні механізму захисту m_k. Ця величина визначається за формулою: $Risk_l = P_k * L_k * (1 - R_k)$.

Для знаходження приблизної величини захищеності S можна використовувати наступну формулу: $S = 1/Risk_0$, де $Risk_0$ є сумою всіх залишкових ризиків $(0 < [P_k, L_k] < 1), (0 \leq R_k < 1)$.

Сумарна величина залишкових ризиків характеризує приблизну сукупну вразливість системи захисту, а захищеність визначається як величина, зворотна вразливості. При відсутності в системі бар'єрів b_k, що перекривають виявлені вразливості, ступінь опірності механізму захисту R_k приймається рівною нулю.

Така математична модель дозволяє кількісно оцінити ефективність системи захисту та обґрунтувати управлінські рішення щодо вибору оптимального набору засобів захисту з урахуванням балансу між витратами на безпеку та можливими збитками від реалізації загроз.

Організаційною основою для створення системи захисту є розроблена на підприємстві політика безпеки – комплекс превентивних мір по захисту конфіденційних даних і інформаційних процесів, що включає вимоги до персоналу, менеджерів та технічних служб. Політика безпеки має враховувати сучасний стан і найближчі перспективи розвитку інформаційних технологій підприємства, цілі, завдання та правові основи їх експлуатації.

Одним із ефективних засобів забезпечення безпеки інформаційних об'єктів є використання системи управління інформаційною безпекою (СУІБ), в основу якої покладено модель PDCA: планування (Plan) – етап розроблення системи управління безпекою, оцінювання ризиків і підбір заходів; дія (Do) – етап реалізації і впровадження обраних заходів; перевірка (Check) – етап оцінювання ефективності та продуктивності системи, який переважно виконується внутрішніми аудиторами; удосконалення (Act) – виконання коригуючих дій[1].

Політика інформаційної безпеки підприємства повинна визначати систему поглядів на проблему забезпечення безпеки інформації і являти собою систематизований виклад цілей і завдань захисту, що є методологічною основою для прийняття управлінських рішень, координації діяльності структурних підрозділів та розробки пропозицій щодо вдосконалення правового, нормативного, технічного та організаційного забезпечення безпеки.

Правове регулювання інформаційної безпеки в Україні, що базується на адаптації вимог європейського регламенту GDPR (General Data Protection Regulation) та міжнародних стандартів до національного законодавства, створює основу для формування комплексної системи інформаційного забезпечення та безпеки в екосистемі управління підприємством. Міжнародні стандарти у сфері інформаційної безпеки представлені сімейством ISO/IEC 27000, зокрема: ISO/IEC 27001 – вимоги до систем управління інформаційною безпекою; ISO/IEC 27002 – настанови щодо практичної реалізації заходів безпеки; ISO/IEC 27005 – управління ризиками інформаційної безпеки.

У межах екосистемного підходу політика інформаційної безпеки трансформується в інтегруючий механізм, що забезпечує синергію технологічних, організаційних та правових компонентів. Вона визначає не лише регламенти використання технологій, а й протоколи їхньої взаємодії та алгоритми адаптації екосистеми до динамічного ландшафту загроз.

Також, визначаються політики доступу до ресурсів комп'ютерної системи окремо від загальної політики інформаційної безпеки. Існують три основні моделі розмежування доступу (табл. 1):

1) дискреційна політика (DAC – Discretionary Access Control);

2) мандатна політика (MAC – Mandatory Access Control);

3) рольова політика (RBAC – Role Based Access Control).

Таблиця 1. **Порівняльна характеристика моделей розмежування доступу**

Характеристика	DAC	MAC	RBAC
Гнучкість	Висока	Низька	Висока
Складність адміністрування	Висока	Середня	Низька
Відповідність законодавству	Обмежена	Повна	Часткова
Масштабованість	Низька	Середня	Висока
Використання	Малі підприємства	Державні установи	Корпорації

Джерело: сформовано авторами за [13]

Вибір моделі розмежування доступу залежить від специфіки бізнесу, вимог законодавства та масштабу інформаційної системи. Для більшості комерційних підприємств оптимальним є впровадження рольової моделі з елементами дискреційного контролю для гнучкого управління правами доступу. RBAC є найбільш економічно ефективною для середнього бізнесу, оскільки знижує витрати на адміністрування.

При розгляді структури системи інформаційної безпеки можливим є виділення підсистем забезпечення: правового, організаційного, інформаційного,

[1] Sokovic M., Pavletic D., Pipan K. Quality improvement methodologies - PDCA cycle, RADAR matrix, DMAIC and DFSS. *Journal of Achievements in Materials and Manufacturing Engineering*. 2010. Vol. 43 (1). P. 476-483.

технічного (апаратного), програмного, математичного та нормативно-методичного. Технічним захистом називають діяльність, спрямовану на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Вся сукупність технічних засобів поділяється на апаратні і фізичні. Апаратні засоби – це пристрої, що вбудовуються безпосередньо в обчислювальну техніку або сполучаються з нею по стандартному інтерфейсу (мережеві фільтри, генератори шуму, скануючі радіоприймачі). Фізичні засоби реалізуються у вигляді автономних пристроїв та систем і включають різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об'єкти інфраструктури.

На сьогоднішній день найбільш поширеними класами технологій захисту інформації підприємства є наступні (табл. 2):

Таблиця 2. **Класифікація засобів захисту інформації**

Категорія	Призначення	Переваги	Недоліки	Приклади
DLP-системи	Захист від витоків	Комплексний контроль каналів	Висока вартість	Symantec DLP, Falcongaze
Міжмережеві екрани	Фільтрація трафіку	Швидкість обробки	Потребує налаштування	Cisco ASA, ZoneAlarm
VPN-шлюзи	Шифрування каналів	Захист даних у транзиті	Зниження швидкості	F5 BIG-IP, Pulse Secure OpenVPN, WireGuard
SIEM	Моніторинг подій	Централізоване управління	Складність впровадження	Splunk, IBM QRadar
IDS/IPS	Виявлення атак	Проактивний захист	Хибні спрацювання	Snort, Suricata
IAM	Управління доступом	Автоматизація процесів	Інтеграційні складнощі	Microsoft AD, Okta

Джерело: сформовано авторами за [14]

1. Системи захисту від витоків конфіденційної інформації (DLP – Data Loss Prevention). DLP-системи є розподіленими програмно-апаратними комплексами, що дозволяють у режимі реального часу проводити моніторинг і блокування вхідних і вихідних повідомлень співробітників, відправлення файлів на зовнішні носії та веб-ресурси. Існує декілька загальноприйнятих розшифровок терміну DLP: Data Loss Prevention, Data Leak Prevention або Data Leakage Protection. DLP-системи розрізняють за способом виявлення витоку даних: Data-in-Use – на робочому місці користувача; Data-in-Motion – у мережі компанії; Data-at-Rest – на серверах і робочих станціях компанії.

Сучасна DLP-система складається з великого числа модулів різного призначення: база даних для зберігання інформації про інциденти, модулі аналізу інформації, агенти для робочих станцій, модулі контролю мережевого трафіку.

2. Міжмережеві екрани (брандмауери, Firewall). Брандмауер – це комплекс апаратних і програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів на різних рівнях моделі OSI відповідно до заданих правил.

3. Криптографічні шлюзи (VPN). Віртуальна приватна мережа (VPN) – це логічна мережа, створювана поверх іншої мережі, найчастіше Інтернет. Всі дані, що передаються між вузлами VPN, шифруються, створюючи захищений тунель обміну інформацією.

4. Системи виявлення й запобігання вторгнень (IPS/IDS). Системи IDS/IPS – це комплекси програмних або апаратних засобів, які виявляють факти і запобігають спробам несанкціонованого доступу в корпоративну систему.

5. SIEM-системи (Security Information and Event Management) .SIEM-системи призначені для управління інформаційною безпекою організації в цілому і управління подіями з різних джерел. Джерелами даних служать IDS/IPS, журнали серверів, комутатори, маршрутизатори, DLP-системи, антивірусні платформи.

6. Системи управління обліковими записами (IAM – Identity and Access Management). IAM-системи дозволяють автоматизувати управління обліковими даними і ролями користувачів, виробляти аудит доступу, обробляти електронні заявки на отримання доступу.

В екосистемі економіко-правового управління впровадження зазначених технологій (зокрема DLP та SIEM-систем) виконує функцію комплаєнс-контролю. Це дозволяє підприємству не лише мінімізувати економічні ризики від витоку комерційної таємниці, а й сформувати надійну юридичну доказову базу у разі внутрішніх чи зовнішніх правових спорів, забезпечуючи відповідність діяльності вимогам Закону України «Про захист персональних даних» та міжнародним стандартам безпеки.

Спектр застосування DLP-систем обмежується запобіганням витоків від користувачів. Вони не можуть забезпечити захист при транспортуванні інформації за межі контрольованої зони для цього використовуються криптографічні методи.

Криптографія – це сукупність методів перетворення даних, спрямованих на приховання їх інформаційного змісту. Криптографічна система захисту інформації являє собою сукупність криптографічних алгоритмів, протоколів і процедур формування, розподілу, передачі й використання криптографічних ключів.

Під шифруванням розуміється процес перетворення відкритої інформації в зашифровану або процес зворотного перетворення (дешифрування). Оригінальне повідомлення називається відкритим текстом, шифроване – шифротекстом. Ключ – це конк-

ретний секретний стан певних параметрів алгоритму криптографічного перетворення даних, що забезпечує вибір тільки одного варіанта перетворення з усіх можливих.

За методом обробки відкритого тексту шифрування поділяється на блочне та потокове. Блочне шифрування передбачає обробку тексту блоками фіксованої довжини (наприклад, 64 або 128 біт). При потоковому методі шифрування елементів відкритого тексту здійснюється послідовно, одне за одним.

Криптосистеми можна поділити на два класи:

1. Симетричні криптосистеми (з одним ключем). У симетричних системах ключі шифрування і розшифрування співпадають ($k_1 = k_2 = k$), обидва ключі є закритими. Принцип роботи: створюється ключ, файл разом з ключем пропускається через програму шифрування, результат пересилається адресатові. Ключ передається окремо через захищений канал. Переваги: висока швидкість шифрування, простота реалізації. Недоліки: складність роботи з секретними ключами при наявності множини віддалених абонентів, необхідність створення і зберігання окремого ключа для кожного абонента.

Популярні алгоритми симетричного шифрування: AES (Rijndael) – ключ 128-256 біт, стандарт США; ГОСТ 28147-89 (ДСТУ 28147:2009) – ключ 256 біт, український стандарт; 3DES – ключ 168 біт, стандарт ANSI X9.52; Blowfish – ключ до 448 біт; TwoFish – ключ 128-256 біт.

2. Асиметричні криптосистеми (з відкритим ключем). У несиметричних системах використовуються два ключі: відкритий для зашифрування і закритий для розшифрування. Не існує алгоритмів прийнятної обчислювальної складності для визначення секретного ключа за відомим відкритим. Принцип роботи: абонент А генерує пару взаємопов'язаних ключів, секретний залишає у себе, відкритий публікує. Абонент В зашифровує повідомлення відкритим ключем А і передає шифртекст. Абонент А розшифровує за допомогою секретного ключа. Переваги: відсутність необхідності передачі секретного ключа, спрощення організації криптозахисту. Недоліки: значна обчислювальна складність порівняно з симетричними алгоритмами, відсутність математично строгого доведення стійкості. Популярні алгоритми асиметричного шифрування: RSA – ключ 1024-4096+ біт, найпоширеніший; ECC (Elliptic Curve Cryptography) – ключ 256-521 біт, ефективніший за RSA; ElGamal – заснований на дискретному логарифмуванні.

Для захисту інформації від модифікації використовуються хеш-функції та електронний підпис (ЕП). Хеш-функція H(M) – це складнозворотне перетворення даних, що застосовується до повідомлення довільної довжини M і повертає значення фіксованої довжини h. Властивості односпрямованих хеш-функцій: знаючи M, легко обчислити h; знаючи h, важко визначити M; важко знайти M', для якого H(M) = H(M',).

Популярні хеш-функції: MD5 (128 біт), SHA-1 (160 біт), SHA-256 (256 біт), ГОСТ 34.311-95, RIPEMD-160.

Електронний цифровий підпис (ЕЦП) формується наступним чином: обчислюється хеш-функція повідомлення; хеш-значення шифрується таємним ключем відправника; результат додається до повідомлення як цифровий підпис.

Ефективність захисту систем залежить від безпечного розподілу ключів:

1. Метод базових/сеансових ключів (ISO 8532) – використовується ієрархія ключів: майстер-ключ для шифрування ключів і сеансовий ключ для шифрування даних.

2. Метод відкритих ключів (ISO 13888) – може використовуватися для розподілу ключів як симетричного, так і асиметричного шифрування через сертифікаційні центри.

Найнадійніший спосіб розповсюдження відкритих ключів – через сертифікаційні центри, що зберігають цифрові сертифікати. Цифровий сертифікат – це електронний ідентифікатор, що підтверджує справжність особи користувача і містить інформацію про відкритий ключ.

Для генерації ключової інформації застосовуються методи (у порядку зростання якості): програмна генерація на основі часу і дій користувача; програмна генерація з використанням якісного генератора псевдовипадкових послідовностей; апаратна генерація з використанням якісного генератора; апаратна генерація на основі фізичних генераторів шуму.

Класифікація програмних генераторів псевдовипадкових послідовностей представлена на рис. 3.

Для перевірки якості генератора використовується керівний документ NIST Special Pub 800-22, що рекомендує частотні тести, перевірку накопичених сум, спектральний аналіз, універсальний тест Маурера, ентропійний тест тощо.

Для використання криптографічних методів на підприємстві необхідно розробити політику використання криптографічних засобів, яка визначає: методику використання криптографічних засобів; принципи управління ключами; ролі та обов'язки відповідальних осіб; відповідний рівень криптографічного захисту для різних даних; заходи забезпечення ефективності впровадження.

Пропонується розглянути практичне застосування технології інформаційного забезпечення та безпеки в екосистемі економіко-правового управління підприємств на прикладі комплексної системи захисту інформації, яка повинна органічно поєднувати організаційні, технічні та криптографічні методи в єдину функціональну систему. Для формалізації та опису такої системи доцільно використовувати методологію функціонального моделювання бізнес-процесів IDEF0.

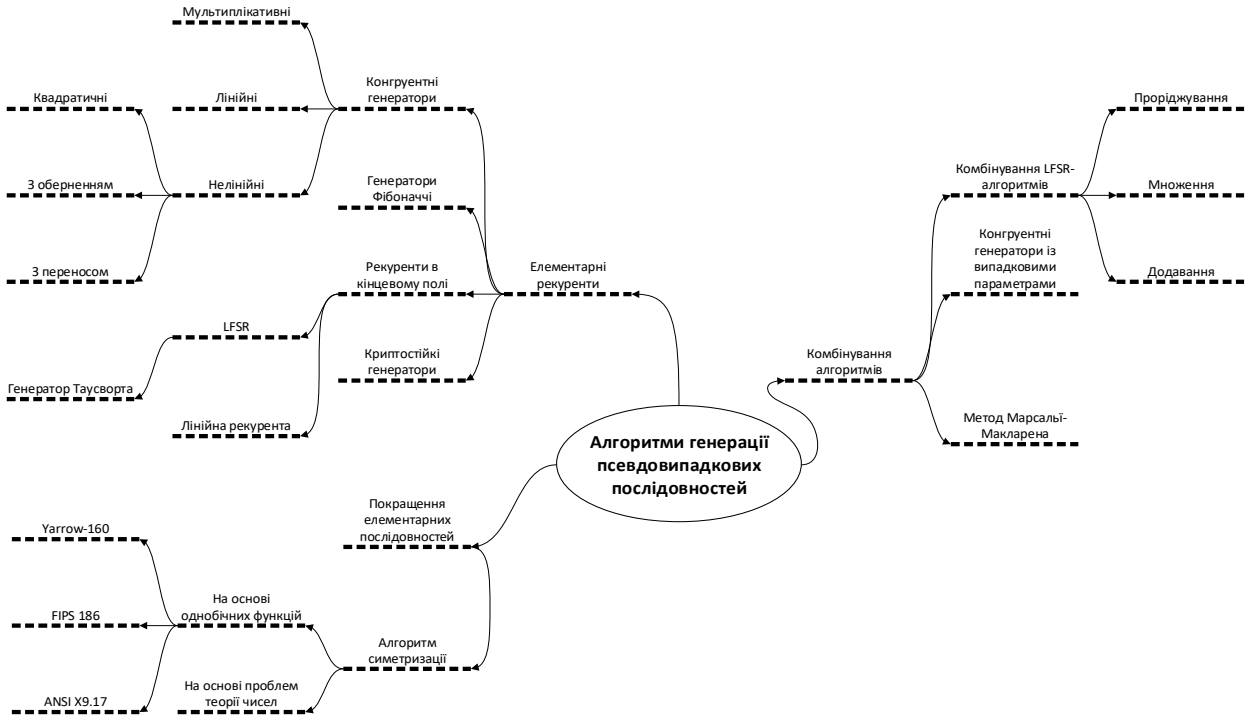

Рис. 3. **Класифікація програмних генераторів псевдовипадкових послідовностей**
Джерело: власна розробка авторів

Модель комплексної системи захисту інформаційних потоків автоматизованої системи документообігу на прикладі підприємства, що надає транспортно-експедиторські послуги.

Контекстна діаграма (рис. 4) представляє систему захисту даних як єдиний функціональний блок з визначенням основних входів, виходів, засобів управління та механізмів.

Діаграма декомпозиції (рис. 5) деталізує функціональний блок захисту даних до чотирьох основних функцій:

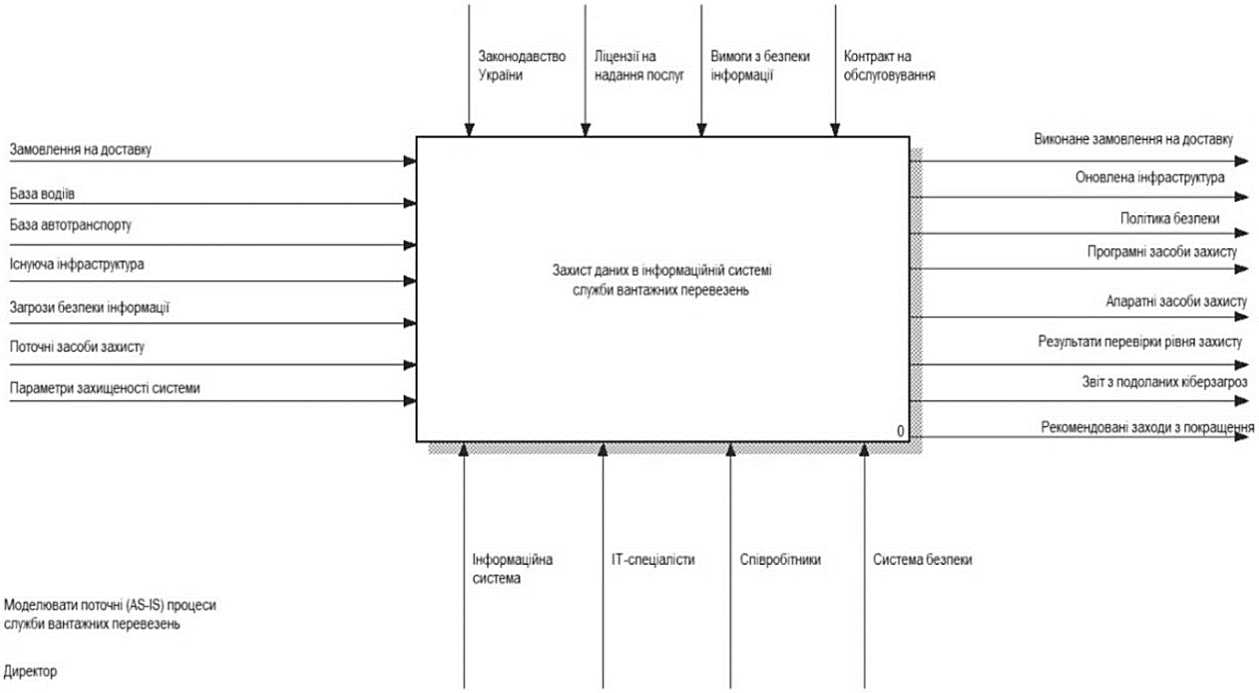

Рис. 4. **Контекстна діаграма «Захист даних в інформаційній системі підприємства» в нотації IDEF0**
Джерело: сформовано авторами за [13]

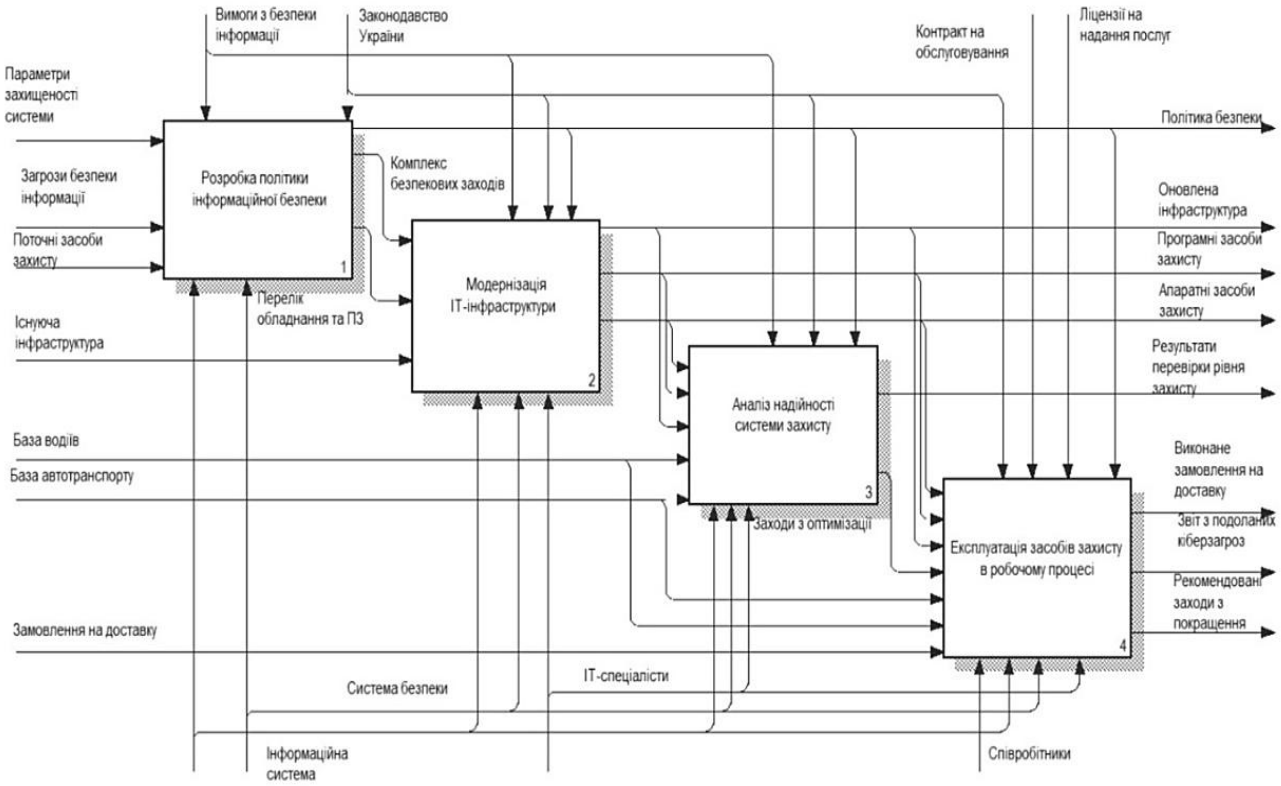

Рис. 5. **Діаграма декомпозиції «Захист даних в інформаційній системі підприємства» в нотації IDEF0**
Джерело: сформовано авторами за [13]

Функція «Розробка політики інформаційної безпеки» складається з чотирьох функціональних блоків – аналізу інформаційних загроз, визначення прав та рівнів доступу для користувачів системи, перевірки поточного стану захищеності наявної IT-інфраструктури та розробки заходів для покращення захисту інформації.

Функція «Модернізація IT-інфраструктури» отримує на вході відомості про існуючу інфраструктуру, перелік обладнання та ПЗ, які необхідно придбати, а також розроблений комплекс безпекових заходів, на виходах формуються апаратні та програмні засоби захисту і оновлена інфраструктура. Складовими елементами даної моделі є наступні роботи: закупка апаратних засобів захисту, оновлення наявного програмного забезпечення, закупка та встановлення програмних засобів захисту, конфігурування сформованої системи безпеки.

Функція «Аналіз надійності системи захисту» складається з наступних робіт: виявлення можливих ризиків безпеки в даній конфігурації системи, проведення імітаційного моделювання кібератаки, обрахунок числових параметрів захищеності системи та розробка заходів з подальшого покращення ефективності захисту.

Функція «Експлуатація засобів захисту в робочому процесі» складається з наступних робіт: реєстрації замовлень та побудови маршрутів, обслуговування доставки та комунікації з водіями, виконання доставки і закриття замовлення, а також підсумкового аналізу ефективності виконання Дана модель може бути адаптована для різних типів підприємств шляхом зміни специфічних входів та виходів при збереженні загальної структури функціональних блоків.

Для оцінки ефективності комплексної системи захисту інформації пропонується використовувати математичну модель, що враховує ймовірність реалізації загроз на різних рівнях інформаційної системи.

Для інформаційних систем з багаторівневою архітектурою ймовірність збереження захищеності визначається за формулою [15]:

$$P(E,M) = \Pi_{i=1}^{L}\left(\Pi_{j=1}^{N}\left(1-E_{ij}\right) + \sum_{j=1}^{N}\left[E_{ij}\Pi_{k=1}^{j-1}\left(1-E_{jk}\right) * \left(\sum_{k=1}^{j} M_{jk} * \Pi_{l=k+1}^{j}\left(1-M_{ij}\right)\right)\right]\right),$$

де L – кількість потенційних загроз інформації, яка опрацьовується в ІС; N – кількість рівнів стека протоколів; M_{ij} – змінна, значення якої визначає факт наявності/відсутності механізму захисту від i-ї загрози на протоколі j-го рівня; E_{ij} – показник ефективності реалізації i-ї загрози на протоколі j-го рівня.

Показник ефективності реалізації загрози E_{ij} визначається як показник оцінки ризику, пов'язаний з реалізацією цієї загрози:

$$E_{ij} = Q_{ij}R_{ij},$$

ISSN 1817-3772

де Q_{ij} – показник, що характеризує відносний внесок, який характеризується i-ю загрозою інформації, реалізованою на протоколі j-го рівня стека протоколів ІС; R_{ij} – показник, що характеризує статистичну ймовірність реалізації i-ї загрози інформації на протоколі j-го рівня системи.

Для перевірки наявності/відсутності автокореляції залишків використовується критерій Дарбіна-Уотсона [15]:

$$DU = \frac{\sum_{k=2}^{N}(d_k - d_{k-1})^2}{\sum_{k=1}^{N} d_k^2}$$

де $d_k = \bar{Y} - Y_k$ – різниця середнього і фактичного значення (залишок) на інтервалі в N точок, для яких відоме значення Y_k.

Якщо значення DU близьке до 2 – автокореляція залишків відсутня, якщо близьке до 0 або до 4 – присутня.

Для перевірки гіпотези про нормальний розподіл ряду використовується правило Романовського, згідно з яким гіпотеза про нормальний розподіл незалежних випадкових величин приймається у разі виконання нерівності:

$$\frac{\chi^2 - r}{\sqrt{2r}} < 3$$

де r – кількість ступенів свободи розподілу, що дорівнює різниці між кількістю класів розбиття усієї кількості спостережень і чіткістю накладених зв'язків (для нормального закону розподілу – дорівнює 3).

Значення χ^2-критерію обчислюється за формулою

$$\chi^2 = \sum_{i=1}^{k} \frac{(m_i - nP_i^*)^2}{nP_i^*}$$

де k – кількість точок розбиття усієї кількості спостережень на класи; m_i – кількість значень випадкової величини в i-му класі; n – кількість спостережень; P_i^* – теоретична ймовірність потрапляння випадкової величини в i-й клас відповідно до вибраного закону розподілу.

Сумарне відносне відхилення реальних значень від середнього оцінюється за формулою [15]:

$$\delta = \sum_{k=1}^{N} \left| \frac{\bar{Y} - Y_k}{\bar{Y}} \right| * 100\%$$

де Y – середнє значення відносних частот спроб реалізації загроз інформації; Y_k – k-те спостережне значення; N – кількість спостережень.

Для оцінки інформаційної безпеки також використовують методи рентабельності витрат на здійснення заходів щодо захисту інформації. Вибір оптимального набору засобів захисту пов'язаний з мінімізацією сумарних витрат W, що складаються з витрат C на створення засобів захисту і можливих витрат N в результаті успішного здійснення загроз:

$$W = C + N \rightarrow min$$

Даний підхід дозволяє обґрунтувати економічну доцільність інвестицій у кожен конкретний механізм захисту, порівнюючи витрати на його впровадження з потенційними збитками від реалізації загроз, які він перекриває. Наприклад, якщо впровадження DLP-системи коштує \$50,000, а потенційні збитки від витоку інформації становлять \$500,000, то інвестиція є економічно виправданою (табл. 3).

Таблиця 3. **Критерії оцінки ефективності систем захисту інформації**

Критерій	Метод оцінки	Переваги	Недоліки	Застосування
Рівень захищеності S	Математична модель	Кількісна оцінка	Складність розрахунків	Технічні системи
Залишковий ризик Risk	Імовірнісний аналіз	Врахування невизначеності	Потребує статистики	Оцінка загроз
Рентабельність W	Економічний аналіз	Обґрунтування інвестицій	Складність оцінки збитків	Управлінські рішення
Критерій χ^2	Статистичний тест	Перевірка гіпотез	Вимагає великої вибірки	Аналіз інцидентів
Відхилення δ	Порівняльний аналіз	Простота обчислень	Не враховує розподіл	Моніторинг системи

Джерело: сформовано авторами за [14]

На практиці рекомендується використовувати комбінацію формальних (математичних) та неформальних (експертних) методів оцінки. Формальні методи дозволяють отримати кількісні показники захищеності, тоді як експертні оцінки враховують специфічні особливості організації, які важко формалізувати.

Для малих та середніх підприємств доцільно використовувати спрощені методики оцінки, що базуються на класифікаційних підходах: визначення рівня критичності інформації (низький, середній, високий); класифікація потенційних порушників за кваліфікацією; оцінка поточних засобів захисту за функціональністю; визначення класу захищеності системи згідно з державними стандартами.

Результати оцінки ефективності системи захисту повинні регулярно переглядатися (не рідше одного разу на рік або після значних змін в інформаційній системі) для забезпечення актуальності прийнятих рішень щодо захисту інформації.

Висновки. У результаті проведеного дослідження сформульовано наступні теоретичні та практичні висновки:

1. Обґрунтовано екосистемний підхід до інформаційного забезпечення та безпеки підприємства. Доведено, що в умовах цифровізації захист даних слід розглядати не як ізольований технічний захід, а як динамічну екосистему, що інтегрує технічні засоби, правові норми, організаційні політики та економічні стимули. Така система характеризується

здатністю до адаптації та синергетичною взаємодією компонентів, що є детермінантою ефективного економіко-правового управління.

2. Визначено концептуальні засади захисту інформації, що базуються на тріаді CIA (конфіденційність, цілісність, доступність). Встановлено, що організаційним фундаментом безпеки є корпоративна політика, яка має гармонізувати вимоги національного законодавства (зокрема законів «Про захист інформації в інформаційно-комунікаційних системах» та «Про захист персональних даних») із міжнародними стандартами серії ISO/IEC 27000.

3. Систематизовано інструментарій комплексного захисту, який включає технічні методи (DLP, SIEM, IDS/IPS, VPN-шлюзи) та криптографічні алгоритми (AES, RSA, ECC). Доведено, що лише комбінація симетричного та асиметричного шифрування у поєднанні з жорстким розмежуванням доступу (моделі DAC, MAC, RBAC) дозволяє мінімізувати ризики витоку комерційної таємниці та фальсифікації документів.

4. Розроблено інтегровану модель системи захисту на основі методології IDEF0. Модель охоплює повний цикл управління безпекою: від проектування політики та модернізації інфраструктури до безперервного моніторингу й експлуатації засобів захисту. Це дозволяє підприємствам адаптувати безпековий контур під конкретні бізнес-процеси та автоматизувати документообіг.

5. Запропоновано математичний та економічний інструментарій оцінки ефективності побудованої системи захисту інформації.. Розроблена модель обчислення ймовірності збереження захищеності та показників залишкового ризику надає менеджменту об’єктивні дані для прийняття управлінських рішень. Визначений економічний критерій мінімізації сумарних витрат дозволяє кількісно обґрунтувати доцільність інвестицій у безпеку, забезпечуючи баланс між вартістю активів та витратами на їх захист.

6. Встановлено, що сталий розвиток підприємства в умовах еволюції кіберзагроз можливий лише за умови впровадження циклічного підходу (PDCA), що забезпечує безперервне вдосконалення системи безпеки. Комплексна інтеграція технологій захисту в загальну стратегію менеджменту не лише забезпечує правову відповідність, а й стає вагомим чинником підвищення конкурентоспроможності підприємства на цифровому ринку.

Перспективи подальших досліджень. Подальший розвиток екосистемного підходу до інформаційного забезпечення та безпеки є стратегічно важливим для трансформації систем управління підприємствами. Пріоритетними напрямами майбутніх розвідок є**:** інтеграція технологій Інтернету речей (IoT) та нейронних мереж у цифрову інфраструктуру бізнесу для підвищення її адаптивності; розробка гібридних моделей прогнозування кіберзагроз та інтелектуальної оптимізації процесів економіко-правового менеджменту; дослідження механізмів автоматизованого комплаєнсу, що дозволять системам безпеки в режимі реального часу підлаштовуватися під динамічні зміни в законодавчому полі. Це дозволить трансформувати систему безпеки підприємства з реактивної моделі у проактивну самонавчальну екосистему.

ЛІТЕРАТУРА

1. Скочиляс-Павлів О. Правові механізми забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*. 2024. Т. 11, № 2 (42). С. 151-158. https://doi.org/10.23939/law2024.42.151

2. Мандич С. М. Інформаційна безпека як складова організаційно-правового захисту аграрного бізнесу. *Український журнал прикладної економіки та техніки*. 2024. Т. 9, № 3. С. 397-401. https://doi.org/10.36887/2415-8453-2024-3-71

3. Кицюк В. М., Пупинін О. С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації*. 2024. № 2 (58). С. 103-108. https://doi.org/10.31673/2409-7292.2024.020012

4. Мельник Л., Карінцева О., Калініченко Л., Харченко М., Тарасенко С. Цифрова трансформація бізнес-процесів в Україні: кращі практики вітчизняного бізнесу та сучасні виклики. *Mechanism of an Economic Regulation*. 2024. № 2 (104). С. 54-60. https://doi.org/10.32782/mer.2024.104.07

5. Долга Г., Хитрова О. Розвиток і тенденції цифровізації управління бізнес-процесами. *Сталий розвиток економіки*. 2024. № 2 (49). С. 141-145. https://doi.org/10.32782/2308-1988/2024-49-22

6. Rivest R. L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*. 1978. Vol. 21, No. 2. P. 120-126. https://doi.org/10.1145/359340.359342

7. Chen H., Chiang R. H. L., Storey V. C. Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*. 2012. Vol. 36, No. 4. P. 1165-1188. https://doi.org/10.2307/41703503

8. Кащена Н., Остапенко Р., Велієва В. Бізнес-аналітика як інструмент обробки даних. *Економіка та суспільство*. 2024. № 62. https://doi.org/10.32782/2524-0072/2024-62-14

9. Вербівська Л., Буринська О. Використання цифрових технологій у підприємницькій діяльності. *Економіка та суспільство*. 2024. № 61. https://doi.org/10.32782/2524-0072/2024-61-84

10. Marban O., Mariscal G., Segovia J. A Data Mining & Knowledge Discovery process model. *Data Mining and Knowledge Discovery in Real Life Applications*. 2009. Vol. 18 (1). P. 1-13. https://doi.org/10.5772/6438

11. Dakic D., Stefanovic D., Cosic I. et al. Business process mining application: a literature review. *Annals of DAAAM & Proceedings*. 2018. Vol. 29. P. 866-875. https://doi.org/10.2507/29th.daaam.proceedings.125

12. Jans M., Van Der Werf J. M., Lybaert N. et al. Business process mining application for internal transaction fraud mitigation. *Expert Systems with Applications*. 2011. Vol. 38 (10). P. 13351-13359. https://doi.org/10.1016/j.eswa.2011.04.159

13. Молодецька-Гринчук К. В. The model of decision making support system for detection and assessment of the state information security threat of social networking services. *Український науковий журнал інформаційної безпеки.* 2017. Т. 23, № 2. С. 136-144. https://doi.org/10.18372/2225-5036.23.11803

14. Тишик І. Підходи щодо вдосконалення систем моніторингу кіберзагроз у корпоративних мережах. *Кібербезпека: освіта, наука, техніка.* 2025. № 1 (29). С. 548-558. https://doi.org/10.28925/2663-4023.2025.29.903

15. Литвинов В. В., Казимир В. В., Стеценко І. В. Моделювання та аналіз безпеки розподілених інформаційних систем: монографія. Чернігів: ЧНТУ, 2016. 254 с.

16. Гуцалюк О. М. Аналіз стану кадрового забезпечення сфери охорони здоров'я України у період реформування. *Вісник економічної науки України.* 2019. № 2 (37). С. 110-114. https://doi.org/10.37405/1729-7206.2019.2(37).110-114

17. Гуцалюк О. М., Бондар Ю. А. Безпековий менеджмент авіаційного транспорту в контексті сталого розвитку національної економіки. *Управління економікою: теорія та практика. Чумаченківські читання*. 2020. С. 82-94. https://doi.org/10.37405/2221-1187.2020.82-94

18. Гуцалюк О. М., Бондар Ю. А. Управління стратегічним розвитком транспортної інфраструктури національної економіки. *Науковий вісник Івано-Франківського національного технічного університету нафти і газу. Серія: Економіка та управління в нафтовій і газовій промисловості*. 2021. № 1 (23). С. 98-107. https://doi.org/10.31471/2409-0948-2021-1(23)-98-107

19. Гуцалюк О. М., Бондар Ю. А., Цатурян Р. О. Особливості формування системи реінжинірингу бізнес-процесів підприємств з використанням цифрових технологій. *Економічний вісник Донбасу*. 2023. № 2 (72). С. 40-47. https://doi.org/10.12958/1817-3772-2023-2(72)-40-47

20. Гуцалюк О. М., Бондар Ю. А., Коцюрба О. Ю., Пітел Н. С. Управління розвитком інноваційно-проєктної діяльності освітніх закладів в умовах взаємодії, конкурентоспроможності та забезпеченні їх фінансово-економічної безпеки. *Вісник економічної науки України*. 2023. № 2 (45). С. 90-96. https://doi.org/10.37405/1729-7206.2023.2(45).90-96

21. Hutsaliuk O., Bondar Iu., Boiko O., Bakum I. Approaches to the strategic management of the development of medical treatment facilities. *Intellectualization of logistics and Supply Chain Management*. 2024. Vol. 27. P. 7-18. https://doi.org/10.46783/smart-scm/2024-27-1

Надійшла до редакції 12.02.2026
Прийнята до друку 06.04.2026
Опублікована 30.05.2026

REFERENCES

1. Skochylyas-Pavliv, O. (2024). Legal mechanisms for ensuring information security in Ukraine. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika». Seriia: Yurydychni nauky*, *11*(2), 151-158. https://doi.org/10.23939/law2024.42.151 [in Ukrainian].

2. Mandych, S. M. (2024). Information security as a component of organizational and legal protection of agrarian business. *Ukrainskyi zhurnal prykladnoi ekonomiky ta tekhniky*, *9*(3), 397-401. https://doi.org/10.36887/2415-8453-2024-3-71 [in Ukrainian].

3. Kytsiuk, V. M., & Pupynin, O. S. (2024). Information security of an enterprise: theoretical aspect. *Suchasnyi zakhyst informatsii*, *2*, 103-108. https://doi.org/10.31673/2409-7292.2024.020012 [in Ukrainian].

4. Melnyk, L., Karintseva, O., Kalinichenko, L., Kharchenko, M., & Tarasenko, S. (2024). Digital transformation of business processes in Ukraine: best practices of domestic business and modern challenges. *Mechanism of an Economic Regulation*, *2*, 54-60. https://doi.org/10.32782/mer.2024.104.07 [in Ukrainian].

5. Dolha, H., & Khytrova, O. (2024). Development and trends in digitalization of business process management. *Stalyi rozvytok ekonomiky*, *2*, 141-145. https://doi.org/10.32782/2308-1988/2024-49-22 [in Ukrainian].

6. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126. https://doi.org/10.1145/359340.359342

7. Chen, H., Chiang, R. H. L., & Storey, V. C. (2012). Business intelligence and analytics: from big data to big impact. *MIS Quarterly*, *36*(4), 1165-1188. https://doi.org/10.2307/41703503

8. Kashena, N., Ostapenko, R., & Veliieva, V. (2024). Business analytics as a data processing tool. *Ekonomika ta suspilstvo*, *62*. https://doi.org/10.32782/2524-0072/2024-62-14 [in Ukrainian].

9. Verbivska, L., & Burynska, O. (2024). The use of digital technologies in entrepreneurial activity. *Ekonomika ta suspilstvo*, *61*. https://doi.org/10.32782/2524-0072/2024-61-84 [in Ukrainian].

10. Marban, O., Mariscal, G., & Segovia, J. (2009). A data mining & knowledge discovery process model. *Data Mining and Knowledge Discovery in Real Life Applications*, *18*(1), 1-13. https://doi.org/10.5772/6438

11. Dakic, D., Stefanovic, D., Cosic, I. et al. (2018). Business process mining application: a literature review. *Annals of DAAAM & Proceedings*, *29*, 866-875. https://doi.org/10.2507/29th.daaam.proceedings.125

12. Jans, M., Van Der Werf, J. M., Lybaert, N. et al. (2011). Business process mining application for internal transaction fraud mitigation. *Expert Systems with Applications*, *38*(10), 13351-13359. https://doi.org/10.1016/j.eswa.2011.04.159

13. Molodetska-Hrynchuk, K. V. (2017). The model of decision-making support system for detection and assessment of the state information security threat of social networking services. *Ukrainian Scientific Journal of Information Security*, *23*(2), 136-144. https://doi.org/10.18372/2225-5036.23.11803

14. Tyshyk, I. (2025). Approaches to improving cyber threat monitoring systems in corporate networks. *Kiberbezpeka: osvita, nauka, tekhnika*, *1*, 548-558. https://doi.org/10.28925/2663-4023.2025.29.903 [in Ukrainian].

15. Lytvynov, V. V., Kazymyr, V. V., & Stetsenko, I. V. (2016). *Modeling and analysis of security of distributed information systems* [Monograph]. Chernihiv National University of Technology [in Ukrainian].

16. Hutsaliuk, O. M. (2019). Analysis of the state of human resources in the healthcare sector of Ukraine during the reform period. *Visnyk ekonomichnoi nauky Ukrainy*, *2*(37), 110-114. https://doi.org/10.37405/1729-7206.2019.2(37).110-114 [in Ukrainian].

17. Hutsaliuk, O. M., & Bondar, Iu. A. (2020). Safety management of aviation transport in the context of sustainable development of the national economy. *Economic management: theory and practice. Chumachenko's Annals* [Collection of scientific works], 82-94. https://doi.org/10.37405/2221-1187.2020.82-94

18. Hutsaliuk, O. M., & Bondar, Iu. A. (2021). Management of strategic development of transport infrastructure of the national economy. *Scientific Bulletin of the Ivano-Frankivsk National Technical University of Oil and Gas. Series: Economics and management in the oil and gas industry, 1*(23), 98-107. https://doi.org/10.31471/2409-0948-2021-1(23)-98-107

19. Hutsaliuk, O. M., Bondar, Iu. A., & Tsaturyan, R. O. (2023). Features of the formation of a system for reengineering business processes of enterprises using digital technologies. *Economic Bulletin of Donbass, 2*(72), 40-47. https://doi.org/10.12958/1817-3772-2023-2(72)-40-47

20. Hutsaliuk, O. M., Bondar, Iu. A., Kotsiurb, A. Yu. & Pitel, N. S. (2023). Management of the development of innovative and project activities of educational institutions in the conditions of interaction, competitiveness and ensuring their financial and economic security. *Bulletin of Economic Science of Ukraine, 2*(45), 90-96. https://doi.org/10.37405/1729-7206.2023.2(45).90-96

21. Hutsaliuk, O. M., Bondar, Iu., Boiko, O. & Bakum, I. (2024). Approaches to the strategic management of the development of medical treatment facilities. *Intellectualization of logistics and Supply Chain Management, 27,* 7-18. https://doi.org/10.46783/smart-scm/2024-27-1

Received: 12.02.2026
Accepted: 06.04.2026
Published: 30.05.2026

Гуцалюк О. М., Манькута Я. М., Захарова І. В., Терновий Є. І. Технології інформаційного забезпечення і корпоративної безпеки в інтегрованій екосистемі економіко-правового управління підприємствами та ІТ-кластерами

У статті обґрунтовано екосистемний підхід до інформаційного забезпечення та безпеки підприємств як фундаментальної умови ефективного економіко-правового управління в умовах цифровізації. Акцентовано, що сучасні підприємства функціонують у середовищі високої динаміки цифрових трансформацій, зростання обсягів даних, активізації кіберзагроз і посилення нормативно-правових вимог, що зумовлює потребу у комплексному підході до захисту інформаційних ресурсів. Обґрунтовано, що інформаційна безпека має розглядатися не як суто технічна функція, а як стратегічний компонент системи управління, який впливає на стабільність бізнес-процесів, фінансову стійкість, репутацію та довіру зацікавлених сторін.

Визначено роль сучасних інформаційних технологій, зокрема DLP, SIEM, VPN, IDS/IPS, у забезпеченні тріади CIA (конфіденційність, цілісність, доступність), а також у своєчасному виявленні інцидентів, контролі доступу, моніторингу подій і попередженні витоків критичних даних. Показано, що ефективність технологічних рішень суттєво підвищується за умови їх узгодження з внутрішніми регламентами, політиками управління доступом та механізмами юридичної відповідальності в межах економіко-правового управління.

Розроблено інтегровану модель захисту інформаційних потоків на основі методології IDEF0, що поєднує технічні засоби із організаційними політиками, процедурами контролю та правовими нормами, забезпечуючи системність та керованість процесів безпеки. Запропоновано математичний інструментарій оцінки ймовірності захищеності інформації та економічний критерій мінімізації витрат, який дозволяє обґрунтовувати доцільність інвестицій у безпеку з урахуванням ризиків і потенційних втрат. Доведено, що інтеграція технологій захисту в загальну стратегію менеджменту сприяє комплаєнс-контролю, зниженню економічних і правових ризиків та підвищує конкурентоспроможність бізнесу в цифровому середовищі.

Ключові слова: інформаційна безпека, екосистемний підхід, корпоративний менеджмент, інтегровані системи управління, цифрова трансформація, тріада CIA, IDEF0, математичне моделювання, економічні ризики, ІТ-кластери.

Hutsaliuk O., Mankuta Ya., Zakharova I., Ternovyi Ye. Information support and corporate security technologies within the integrated ecosystem of economic and legal governance of enterprises and IT clusters

The article substantiates the ecosystem approach to information security and enterprise security as a fundamental condition for effective economic and legal management in the context of digitalization. It is emphasized that modern enterprises operate in an environment of high dynamics of digital transformations, growth in data volumes, intensification of cyber threats and strengthening of regulatory requirements, which determines the need for a comprehensive approach to the protection of information resources. It is substantiated that information security should be considered not as a purely technical function, but as a strategic component of the management system, which affects the stability of business processes, financial stability, reputation and trust of stakeholders.

The role of modern information technologies, in particular DLP, SIEM, VPN, IDS/IPS, in ensuring the CIA triad (confidentiality, integrity, availability), as well as in timely incident detection, access control, event monitoring and prevention of critical data leaks, is determined. It is shown that the effectiveness of technological solutions is significantly increased if they are coordinated with internal regulations, access control policies and legal liability mechanisms within the framework of economic and legal management.

An integrated model of information flow protection based on the IDEF0 methodology has been developed, which combines technical means with organizational policies, control procedures and legal norms, ensuring the systematicity and manageability of security processes. A mathematical tool for assessing the probability of information security and an economic criterion for minimizing costs have been proposed, which allows justifying the feasibility of investments in security taking into account risks and potential losses. It has been proven that the integration of security technologies into the overall management strategy contributes to compliance control, reducing economic and legal risks and increasing the competitiveness of business in the digital environment.

Keywords: information security, ecosystem approach, corporate management, integrated management systems, digital transformation, CIA triad, IDEF0, mathematical modeling, economic risks, IT clusters.