DOI: https://doi.org/10.32782/2524-0072/D2026-86-238

УДК 657:004.056:338.24

ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМИ БУХГАЛТЕРСЬКОГО ОБЛІКУ: ВИКЛИКИ ЦИФРОВІЗАЦІЇ ТА ВІЙСЬКОВІ ЗАГРОЗИ

INFORMATION SECURITY OF ACCOUNTING SYSTEMS: THE CHALLENGES OF DIGITALISATION AND MILITARY THREATS

Литвиненко Володимир Сергійович
кандидат економічних наук, доцент,
Національний університет біоресурсів і природокористування України
ORCID: https://orcid.org/0000-0002-6495-0537

Lytvynenko Volodymyr
National University of Life and Environmental Sciences of Ukraine

У статті досліджено проблеми захисту інформації системи бухгалтерського обліку в умовах цифровізації та воєнного стану в Україні. Розглянуто актуальність безпеки бухгалтерських даних як джерела конфіденційної та бізнесової інформації. Виокремлено ключові кіберзагрози, включаючи вірусні атаки, хмарні вразливості та загрози цілеспрямованих кібератак в умовах збройного конфлікту. Проаналізовано ризики використання бухгалтерського програмного забезпечення, розробленого в країні-агресорі, та запропоновано рекомендації, які сприятимуть пришвидшенню переходу на вітчизняні й міжнародні прикладні програмні рішення. Запропоновано практичні рекомендації щодо резервного копіювання, управління доступом, шифрування даних, мережевої сегментації, антивірусного захисту та підвищення цифрової компетентності працівників бухгалтерської служби.

Ключові слова: облік, інформаційна безпека, цифровізація, воєнні ризики, бухгалтерське програмне забезпечення, хмарні технології, система, управління.

This article examines the theoretical and practical aspects of ensuring the information security of accounting systems in the context of the digitalisation of the economy and military threats in Ukraine. It is argued that the modern accounting system operates in an environment characterised by the active use of digital technologies, cloud services, automated information systems and remote data exchange, which enhances the efficiency of accounting processes but simultaneously creates new risks of loss, distortion or unauthorised access to accounting information. It is established that accounting information is a strategic resource of an enterprise, containing financial, managerial and commercial data, and therefore requires comprehensive protection during its generation, processing, storage and transmission. The main cyber threats affecting the functioning of the accounting system have been analysed, in particular malware, phishing attacks, data leaks, vulnerabilities in cloud infrastructure, breaches of access to information resources, and targeted cyberattacks on critical information infrastructure facilities under martial law. Particular attention is paid to the risks associated with the use of accounting software linked to the aggressor country, which poses additional threats to the information and economic security of enterprises. The need for business entities to switch to domestic and international software products that meet modern cybersecurity and information security requirements is emphasised. This article systematises the components of accounting information security, including technical, organisational, legal and human resources measures. It offers practical recommendations on the use of data encryption, data backup, multi-level access control, network segmentation, anti-virus protection and the enhancement of digital literacy among accounting staff. The research findings can be used by enterprises to improve their accounting information protection systems and enhance information security in the context of the digital transformation of the economy.

Keywords: accounting, information security, digitalisation, military threats, accounting software, cloud technologies, system, management.

Постановка проблеми. В умовах поглиблення процесів цифровізації та викликів воєнного стану питання захисту облікової інформації має критичне значення для стабільного функціонування бізнесу та наповнення державного бюджету. Система бухгалтерського обліку підприємства акумулює масиви чутливих даних – від інформації про активи, зобов'язання та фінансові результати до персональних даних працівників та контрагентів. Компрометація таких відомостей здатна завдати підприємству матеріальних збитків, зашкодити діловій репутації, стати підставою для юридичної відповідальності та навіть підвищити ризики обороноздатності країни.

Зростаюча залежність підприємств від цифрових інструментів обліку, використання хмарних сервісів та інтегрованих ERP-систем суттєво розширює можливості для кібератак. Бухгалтерський облік є інформаційною основою управління підприємством. Відповідно до Закону України «Про бухгалтерський облік та фінансову звітність в Україні» облік забезпечує відображення в грошовому вимірі усіх господарських операцій і формує повну та достовірну інформацію про майновий та фінансовий стан суб'єкта господарювання [14]. Саме ця інформація становить основу для прийняття управлінських рішень, укладання угод, залучення інвестицій та взаємодії з кредиторами.

З огляду на свій зміст, облікова інформація має подвійну сутність: з одного боку, вона є обов'язковою для офіційного розкриття у встановлених законодавством формах фінансової звітності; з іншого – значна її частина є комерційною таємницею підприємства, яка не підлягає розголошенню і має ретельно охоронятися. Зокрема, конфіденційний характер мають: інформація про заробітну плату та персональні дані співробітників, про постачальників і покупців, умови договорів, розміри дебіторської та кредиторської заборгованості, структуру витрат, а в умовах воєнного стану ще й місце розташування чутливих виробничих майданчиків. Такі дані можуть містити бухгалтерські документи про рух товарно-матеріальних цінностей, у яких вказані адреси доставки. Витік або спотворення таких даних може мати для підприємства критичні наслідки та підривати обороноздатність країни.

Посилення цифровізації бухгалтерського обліку відбувається у декількох вимірах: перехід до електронного документообігу; масштабне впровадження хмарних облікових рішень; інтеграція облікових систем із банківськими, митними та державними реєстрами, використання інструментів штучного інтелекту для обробки інформації. Кожен із цих напрямів підвищує ефективність обліку, знижує його трудомісткість, але одночасно формує нові загрози.

Аналіз останніх досліджень і публікацій. Забезпечення інформаційної безпеки системи бухгалтерського обліку перебуває на перетині двох наукових дисциплін – бухгалтерського обліку та інформаційних технологій, що обумовлює міждисциплінарний характер досліджень у цьому напрямку.

Дослідження інформаційної безпеки даних бухгалтерського обліку здійснювали С. Василішин [6], П. Гайдуцький, Л. Гуцаленко [7], С. Дерев'янко [9], В. Жук [8], З.-М. Задорожний, Н. Іванова [9], О. Канцуров, В. Кицюк [10], С. Легенчук [11], Н. Лоханова, Т. Назаренко [11], В. Осмятченко, О. Петрук, Н. Правдюк [13], М. Проданчук, І. Царук [11], М. Яцко [9], А. Ясінська [20].

Як відзначили дослідники Жук В. М., Василішин С.І. та Нежид Ю.С., управління підприємством потребує функціонально дієвої та раціонально організованої системи бухгалтерського обліку, яка забезпечує своєчасне виявлення та оцінку ризиків, формування достовірної інформації для ухвалення управлінських рішень. Вона є не лише інструментом фіксації шкоди та збитків, а й механізмом планування відновлення, оптимізації ресурсів та підвищення стійкості підприємств до військових викликів і загроз» [8, с. 16]. Варто відзначити, що забезпечення стійкості й безпеки потребує і сама система бухгалтерського обліку в умовах цифрової економіки.

Будь-яке підприємство є складною економічною системою, а його діяльність підпорядковується законам функціонування і розвитку складних систем. Облікова система має бути належним чином організована і адаптована до внутрішнього та зовнішнього середовища [7, с. 31], а також захищеною від стороннього втручання.

Теоретико-методичні засади обліково-аналітичного забезпечення в системі ризиків та загроз економічної безпеки аграрних підприємств України досліджені в монографії С.І. Василішина. Автор відзначив, що однією з важливих передумов інституційного забезпечення економічної безпеки є належне функціонування інституту бухгалтерського обліку. У міру зростання ризиків економічної діяльності підприємств в умовах цифровіза-

ції змінюється обліково-аналітичне забезпечення управлінських процесів. У свою чергу це зумовлює трансформацію місії бухгалтерської професії, важливішими компонентами якої, крім реєстрації фактів господарського життя, стало гарантування економічної безпеки підприємства [6, с. 310-312].

Іванова Н.А., Яцко М.В. та Дерев'янко С.І. здійнили оцінку ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ та встановили, що її ефективність визначається рівнем інтеграції ризик-орієнтованих, процесних і технологічних підходів у єдину адаптивну систему управління кіберризиками. Основними проблемами забезпечення безпеки у цій сфері є невизначеність розподілу відповідальності між користувачем і провайдером, обмежена прозорість обробки даних, асиметрія інформації щодо кіберзагроз, складність управління правами доступу і недостатня адаптивність контрольних механізмів у хмарному середовищі [9].

Розглядаючи архітектуру облікових систем, питання організації баз даних, захисту облікової інформації в середовищі автоматизованих систем, дослідники обґрунтовують тезу, що безпека облікової інформації є складовою загальної системи інформаційної безпеки підприємства та потребує комплексного підходу – технічного, організаційного та правового характеру.

Так Кицюк В. М. та Пупинін,О. С. вважають, що інформаційна безпека підприємства має ґрунтуватися на сукупності взаємопов'язаних принципів: законності – дотримання правових норм та міжнародних стандартів у сфері захисту інформації; права власності – гарантування прав суб'єктів на належну їм інформацію в межах, визначених законодавством; економічної доцільності – всебічний аналіз можливої економічної шкоди від порушення захисту інформації; комплексного підходу – створення єдиної цілісної системи фізичної, технічної та кадрової безпеки; безперервності – регулярне застосування превентивних заходів та аудитів на всіх етапах життєвого циклу інформації; єдиноначальності – персональна відповідальність керівників за стан захисту конфіденційної інформації. Реалізація зазначених принципів, на думку дослідників, забезпечує надійний захист інформації, знижує ризики порушення її конфіденційності, цілісності та доступності, а також сприяє стабільності фінансово-господарської діяльності підприємства [10, с. 106-107]. Зазначені принципи цілком стосуються і забезпечення безпеки облікової інформації.

Легенчук С. Ф., Царук І. М. та Назаренко Т. П. дослідили принципи захисту даних у системі обліку та вважають, що безпека облікових даних підприємства базується на тріаді фундаментальних принципів – цілісності даних, конфіденційності та доступності для всіх авторизованих користувачів. Цілісність бухгалтерських даних передбачає унеможливлення несанкціонованого створення, зміни або знищення облікової інформації шляхом розмежування прав доступу користувачів у бухгалтерських інформаційних системах. Конфіденційність бухгалтерської інформації характеризує здатність підприємства захищати облікову інформацію від суб'єктів, що не мають повноважень на її перегляд, та реалізується через розмежування прав між користувачами на різних рівнях функціонування системи. Доступність бухгалтерських даних означає забезпечення безперервної роботи бухгалтерської інформаційної системи з метою надання користувачам доступу до облікових даних у будь-який момент часу [11, с. 65-67].

На комплексному підході до захисту бухгалтерської інформації наголошує і Ясінська А.І.: «інформаційна безпека є складним процесом, який повинен включати в себе різноманітні заходи та дії, і доцільним є застосування системно-комплексного підходу з точки зору організаційних, технічних і правових заходів» [20, с. 332].

Штучний інтелект є не лише каталізатором трансформаційних процесів у бухгалтерському обліку, а й джерелом ризиків для безпеки інформації. За дослідженням Правдюк Н. Л. і Правдюк М. В., технічне забезпечення впровадження штучного інтелекту й гарантування безпеки, а також конфіденційності бухгалтерських даних потребує реалізації низки заходів: шифрування даних, контроль доступу до системи штучного інтелекту й бухгалтерської інформації, аудит заходів безпеки, дотримання нормативних вимог і стандартів захисту даних [13, с. 78-79].

Законодавче та нормативне забезпечення кібербезпеки в Україні формує відповідне правове поле для захисту облікової інформації. Закон України «Про основні засади забезпечення кібербезпеки України» визначає об'єкти кіберзахисту, повноваження Команди реагування на комп'ютерні надзвичайні події України – CERT-UA та встановлює зобов'язання операторів критичної інфраструктури щодо

захисту інформаційних систем [17]. Відповідно до Стратегії кібербезпеки України пріоритетами є стійкість кіберінфраструктури, розвиток потенціалу кіберзахисту та міжнародне співробітництво у сфері кібербезпеки [19]. Ці заходи у повній мірі повинні стосуватися і захисту інформаційних систем обліку та управління підприємством.

Захист персональних даних, що обробляються в системах бухгалтерського обліку, регламентується Законом України «Про захист персональних даних» [15]. Порушення вимог цього закону тягне за собою адміністративну та кримінальну відповідальність, що робить відповідну складову облікової безпеки не тільки технічною, але й правовою проблемою.

Питання забезпечення безпеки облікових інформаційних систем знайшли відображення у роботах М. Ромні та П. Штейнбарта. Автори виокремлюють безпеку інформаційних систем бухгалтерського обліку (AIS) як самостійний розділ і розглядають її крізь призму концепції CIA-тріади (Confidentiality – конфіденційність, Integrity – цілісність, Availability – доступність). Ромні та Штейнбарт систематизують загрози обліковим системам за такими категоріями: природні та техногенні катастрофи, ненавмисні помилки людини, навмисні злочинні дії (хакінг, шкідливе ПЗ, витоки даних). Особливу увагу автори приділили контролю безпеки: превентивному (шифрування, автентифікація, навчання персоналу), детективному (системи виявлення вторгнень, журнали аудиту) та коригувальному (плани відновлення після інцидентів) [5]. Ця концептуальна схема зберігає свою актуальність і для умов воєнного часу.

Питання управління кіберризиками досліджуються також у межах системи COBIT (Control Objectives for Information and Related Technology), розробленої асоціацією ISACA. Ця система встановлює цілі контролю для інформаційних технологій, у тому числі для облікових інформаційних систем. Концепція COBIT 2019 визначає управлінські та операційні домени безпеки, що забезпечують відповідну основу для аналізу ризиків AIS [2]. Загальна теорія управління інформаційною безпекою підприємства ґрунтується на Концепції внутрішнього контролю (COSO) та стандарті ISO/IEC 27001:2022 [3], який встановлює вимоги до системи управління інформаційною безпекою (ISMS). Фреймворк NIST Cybersecurity Framework [4] систематизує функції безпеки у п’яти доменах: Identify (ідентифікація), Protect (захист), Detect (виявлення), Respond (реагування), Recover (відновлення). Ця модель набуває особливого значення для умов збройного конфлікту, де функція «Recover» (відновлення після деструктивних атак) стає критично важливою.

Загалом, аналіз наукових праць засвідчує, що проблеми захисту облікової інформації досліджувалися переважно в контексті загальних питань автоматизації обліку та побудови інформаційних систем. Досліджень, безпосередньо зосереджених на безпеці облікових даних в умовах воєнного конфлікту, недостатньо, що підтверджує актуальність і наукову новизну обраної теми.

Метою статті є дослідження сучасних загроз безпеці облікової інформації в умовах цифровізації та воєнного стану, а також формування комплексу рекомендацій щодо зниження відповідних ризиків.

Виклад основного матеріалу дослідження. Цифровізація бухгалтерського обліку є об’єктивним і незворотним процесом, що суттєво підвищує ефективність облікової роботи, водночас формуючи нові кластери ризиків. Виходячи з цього, все більшого значення набуває функція захисту облікової інформації, яка покликана забезпечити цілісність і конфіденційність даних про діяльність підприємства [12].

За даними Команди реагування на комп’ютерні надзвичайні події України (CERT-UA), фішингові атаки залишаються найпоширенішим початковим вектором проникнення до корпоративних мереж [1]. Бухгалтери є особливо привабливою ціллю для фішингових атак: вони мають широкий доступ до фінансової інформації, регулярно отримують електронні листи від банків, контрагентів і державних органів, а також здійснюють платіжні операції. Компрометація облікового запису бухгалтера через фішинг є стартовою точкою для розширення несанкціонованого доступу до всієї облікової системи підприємства.

Широке впровадження хмарних сервісів для ведення бухгалтерського обліку (хмарні облікові та ERP-системи, SaaS-рішення для обліку тощо) принесло значну користь, особливо на початку повномасштабного вторгнення. Водночас це означає, що критична фінансова інформація підприємства зберігається поза межами фізичної інфраструктури самого підприємства. Ключові ризики хмарного зберігання облікової інформації включають наступні:

– дані можуть фізично зберігатися на серверах у будь-якій країні світу, що підвищує ризик перехоплення даних з боку іноземних спецслужб або хакерських угруповань;

– проблеми з доступом до інформації в умовах відключення електрики, пошкодження ліній зв'язку, перебоїв з доступом до інтернету в умовах воєнного часу;

– порушення роботи хмарного сервісу (через технічні збої, кібератаки на постачальника або його банкрутство) може призвести до втрати доступу до облікових даних;

– зберігання даних різних клієнтів на спільній серверній інфраструктурі породжує ризик «перетікання» інформації між клієнтами у разі неналежного логічного розмежування;

– нерідко провайдери хмарних облікових рішень не шифрують резервні копії даних, що є критичною вразливістю;

– сполучення хмарних облікових систем із банківськими API, державними реєстрами та CRM-системами збільшує кількість точок потенційного несанкціонованого доступу.

Особливу небезпеку для облікових систем становлять деструктивні шкідливі програми класу wiper (знищувачі даних). Найбільш показовим прецедентом стала атака вірусу NotPetya (інша назва – Petya.A) у червні 2017 року, яка набула найбільшого масштабу саме в Україні. Вірус, що маскувався під програму-вимагач класу ransomware, поширився через механізм оновлення популярного в Україні програмного забезпечення (ПЗ) для ведення бухгалтерського обліку та подання звітності. На відміну від класичного ransomware, NotPetya не передбачав жодного механізму відновлення навіть після сплати «викупу» – це свідчило про деструктивну, а не корисливу мету атаки.

Масштаб збитків виявився колосальним: атака паралізувала IT-системи Укренерго, Нової пошти, Укртелекому, низки банків, Чорнобильської АЕС (автоматичні радіаційні монітори перейшли в ручний режим), а також Кабінету Міністрів України. Для бізнесу результатом стала повна або часткова втрата баз даних бухгалтерського обліку [18].

Прецедент NotPetya виявив системні вразливості в ланцюгу постачань програмного забезпечення, що ставить питання безпеки облікового ПЗ та механізмів його оновлення в центр захисту облікової інформації.

Таблиця 1

Заходи протидії ризикам інформаційної безпеки облікових систем в умовах воєнного стану

№ з.п.	Група ризику	Заходи протидії ризику
1.	Дезінформація та маніпуляції з обліковими записами	Посилений контроль за розмежуванням прав доступу та двоособове підтвердження критичних операцій; регулярна звірка даних між підсистемами.
2.	Вимушена зміна місця ведення обліку та евакуація	Завчасна міграція до хмарних облікових рішень; документування порядку дій при евакуації; надання ключовому персоналу дистанційного доступу до систем.
3.	Цілеспрямовані кібератаки на бізнес-інфраструктуру	Впровадження комплексних рішень класу EDR (Endpoint Detection and Response), використання MFA (багатофакторної автентифікації) для доступу до облікових систем, регулярна перевірка реєстрів підозрілих процесів.
4.	Фізичне знищення серверної інфраструктури	Обов'язкове хмарне резервне копіювання з реплікацією на серверах у безпечних регіонах або закордоном; документування конфігурації облікової системи для швидкого розгортання на новому обладнанні.
5.	Відключення електропостачання та інтернет-з'єднання	Застосування безперебійних джерел живлення; налаштування механізмів коректного завершення роботи баз даних; використання транзакційних систем управління БД (СУБД) з функціями відновлення після збоїв (WAL – Write-Ahead Logging).
6.	Ризик компрометації облікових даних через VPN та дистанційний доступ	Використання сучасних протоколів VPN (WireGuard, OpenVPN) з MFA; регулярний аудит облікових записів дистанційних користувачів; обмеження доступу за географічними ознаками

Джерело: сформовано автором

Збройний конфлікт з російською федерацією сформував принципово новий контекст для управління безпекою облікових інформаційних систем. У таблиці 1 представлено основні групи ризиків та відповідні їм заходи протидії.

Окремої уваги заслуговує питання забезпечення безперервності ведення бухгалтерського обліку як в умовах бойових дій, так і у разі кіберінцидентів. Для цього доцільно розробити та затвердити на підприємстві план забезпечення безперервності бізнесу та план відновлення після катастроф, які повинні охоплювати окрему процедуру відновлення облікових систем і баз даних. Відповідно до стандарту ISO/IEC 27001 [3], план відновлення має визначати максимально допустимий час та допустиму точку відновлення даних для облікових систем.

До початку повномасштабного вторгнення значна частина підприємств в Україні використовувала облікове програмне забезпечення, розроблене компаніями, що мають зв'язки з російською федерацією. Найбільш поширеним таким рішенням була система «1С:Підприємство» (розробник – АТ «1С»), яка, за різними оцінками, до 2022 р. охоплювала від 30 до 80% ринку корпоративного облікового ПЗ в Україні. У таблиці 2 відображені основні ризики використання таких програмних рішень для інформаційної безпеки підприємства.

Незважаючи на очевидні ризики, багато підприємств змушені використовувати неліцензійне програмне забезпечення, а перехід з «1С» та подібних програм на альтернативні рішення залишається повільним. Водночас не можливо не відмітити, що програмні рішення для ведення бухгалтерського обліку в Україні стали більш різноманітними та доступними:

– Українські рішення: «Master: Бухгалтерія» (розробник – компанія IT-Enterprise , Україна), «Дебет Плюс» (ТОВ «КТ-менеджмент», Україна), «FlyDoc» та інші.

– Міжнародні рішення: SAP Business One та SAP S/4HANA (SAP SE, Німеччина), Microsoft Dynamics 365 Business Central (Microsoft, США).

Водночас на нашу думку, доцільно запровадити ряд заходів для полегшення та пришвидшення переходу на ці програмні рішення (Рис. 1).

На основі проведеного дослідження запропоновано комплекс методичних засобів реалізації функції безпеки облікової інформації, що об'єднує технічні, організаційні, правові та кадрові заходи (Рис. 2).

Функція захисту інформації бухгалтерського обліку передбачає шифрування усіх даних бухгалтерського обліку як у стані збе-

Таблиця 2

Ризики використання програмного забезпечення країни-агресора

№ з.п.	Ризик	Характеристика ризику в умовах воєнного стану
1.	Ризик наявності шпигунського функціоналу	Програмне забезпечення, розроблене в країні-агресорі, теоретично може містити прихований функціонал для передачі даних або дистанційного управління системою. Верифікація вихідного коду закритого ПЗ є неможливою для кінцевого користувача.
2.	Правові ризики	Відповідно до Указу Президента України та рішень РНБО про санкції щодо фізичних та юридичних осіб рф, використання ПЗ від підсанкційних російських компаній може кваліфікуватися як порушення законодавства про санкції. Особливо критичним даний ризик є для суб'єктів державного та оборонного секторів.
3.	Відсутність офіційної підтримки та оновлень	З моменту введення санкцій та добровільного виходу ряду зарубіжних компаній з ринку, легальне оновлення «1С» та подібного програмного забезпечення в Україні стало неможливим. Відсутність патчів безпеки означає, що вразливості, виявлені з 2022 р., залишаються не закритими, а робота з програмами стала не лише більш ризиковою, але й складною.
4.	Ризик цільового деактивування	Відмічені випадки дистанційного деактивування ПЗ на підприємствах в окупованих регіонах та, навпаки, продовження його роботи в інтересах окупаційних адміністрацій. Це свідчить про наявність механізмів дистанційного управління програмним продуктом.

Джерело: сформовано автором

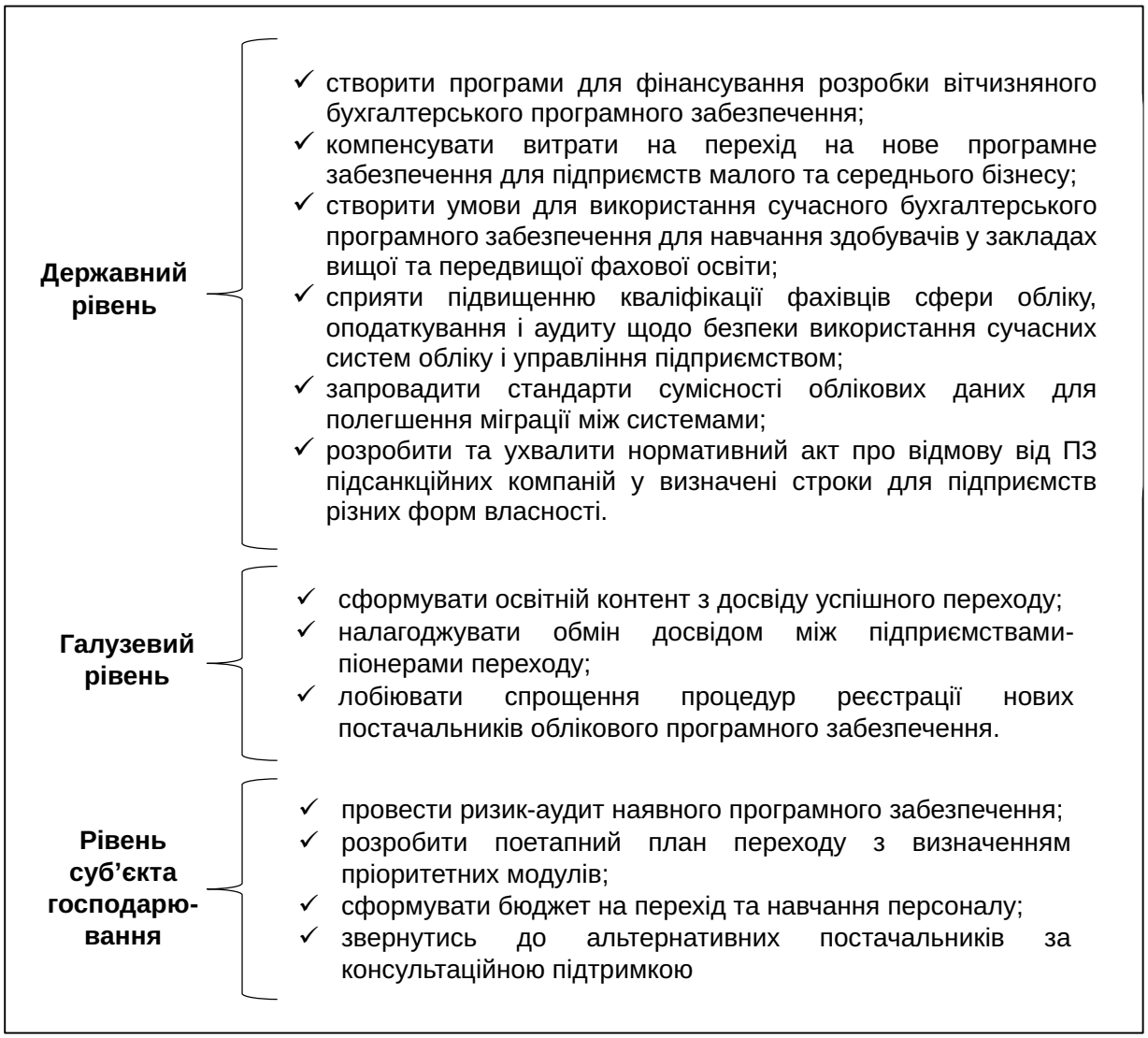

Рис. 1. Заходи стимулювання переходу підприємств на сучасні облікові програмні рішення

Джерело: сформовано автором

рігання, так і під час передачі, а кожен користувач облікової системи повинен мати лише той рівень доступу, який необхідний для виконання його функцій.

Висновки. Проведене дослідження засвідчило, що безпека облікової інформації є комплексною проблемою, яка потребує системного вирішення на технічному, організаційному, правовому та кадровому рівнях. Інформація системи бухгалтерського обліку концентрує дані про усі аспекти фінансово-господарської діяльності підприємства, включаючи комерційну таємницю, персональні дані співробітників та відомості про контрагентів. В умовах цифровізації ця інформація стала вразливою до широкого спектру кіберзагроз.

Важливою складовою реалізації функції інформаційної безпеки бухгалтерського обліку є розробка та впровадження політики інформаційної безпеки підприємства, яка визначає: класифікацію облікових даних за ступенем конфіденційності, правила доступу до облікових систем, порядок обробки та зберігання чутливих фінансових даних, відповідальність посадових осіб тощо.

Регулярне навчання персоналу щодо розпізнавання фішингових листів та правил роботи з конфіденційними даними сприятиме зростанню рівня інформаційної безпеки. Розподіл функцій має передбачати, що особи, які вводять первинні документи до системи, не повинні мати права на їх затвердження, а особи, що адмініструють облікову систему, не повинні мати можливості змінювати облікові дані.

Використання облікового програмного забезпечення, розробленого в російській

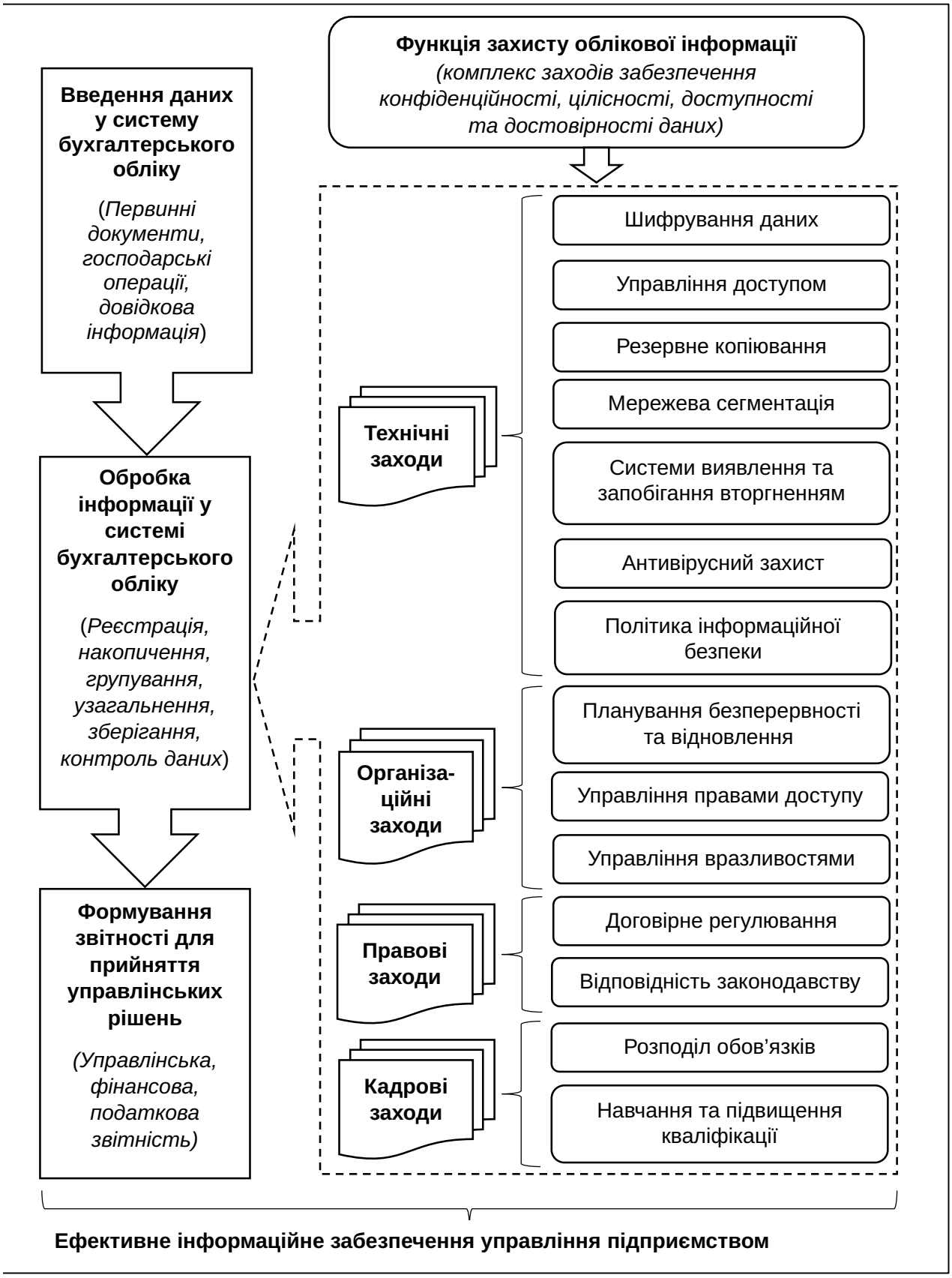

Рис. 2. Реалізація функції захисту облікової інформації в управлінні підприємством

Джерело: сформовано автором

федерації, є неприйнятним ризиком в умовах збройного конфлікту з країною-розробником. Перехід на українські та міжнародні альтернативи є нагальним завданням, прискоренню якого має сприяти державна підтримка, стандартизація форматів даних для полегшення міграції та розвиток ринку фахівців із альтернативних рішень.

Подальші дослідження можуть бути спрямовані на розробку галузевих методичних рекомендацій із захисту облікової інформації для підприємств різних секторів економіки, а також дослідження ефективності використання інструментів штучного інтелекту для виявлення кіберзагроз в облікових інформаційних системах та засобів боротьби з ними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. CERT-UA. Офіційний сайт Команди реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua (дата звернення: 12.05.2026).

2. ISACA. COBIT 2019 Framework: Introduction and Methodology. Rolling Meadows: ISACA, 2018. 100 с. URL: https://rms.koenig-solutions.com/Sync_data/Trainer/QMS/1827-2022414376-Cobit2019.pdf (дата звернення: 12.05.2026).

3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 2022. 23 p. https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf (дата звернення: 12.05.2026).

4. NIST. Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). Version 1.1. National Institute of Standards and Technology. Gaithersburg, MD: NIST, 2018. 55 p. URL: https://doi.org/10.6028/NIST.CSWP.04162018 (дата звернення: 12.05.2026).

5. Romney M. B., Steinbart P. J. Accounting Information Systems. 14th ed. Harlow: Pearson, 2018. 752 p.

6. Василішин С.І. Обліково-аналітичне забезпечення в системі ризиків та загроз економічної безпеки аграрних підприємств України: монографія. Харків. нац. аграр. ун-т ім. В.В. Докучаєва. Харків: ТОВ «Друкарня Мадрид», 2020. 419 с.

7. Гуцаленко Л. В. Адаптивна система обліку і контролю результатів діяльності сільськогосподарських підприємств: монографія. К.: ННЦ ІАЕ. 2010. 372 с.

8. Жук В. М., Василішин С.І., Нежид Ю.С. Обліково-інформаційне забезпечення управління агропідприємствами в умовах надзвичайних ситуацій та повоєнних викликів. *Ефективна економіка*. 2025. № 10. DOI: http://doi.org/10.32702/2307-2105.2025.10.14 (дата звернення: 12.05.2026).

9. Іванова Н.А., Яцко М.В., Дерев'янко С.І. Оцінка ефективності системи внутрішнього контролю кібербезпеки хмарних облікових платформ. *Актуальні питання економічних наук*. 2026. № 21. DOI: https://doi.org/10.5281/zenodo.19478268 (дата звернення: 12.05.2026).

10. Кицюк В.М., Пупинін О.С. Інформаційна безпека підприємства: теоретичний аспект. *Сучасний захист інформації*. 2024. № 2 (58). С. 103–108. DOI: https://doi.org/10.31673/2409-7292.2024.020012 (дата звернення: 12.05.2026).

11. Легенчук С. Ф., Царук І. М., Назаренко Т.П. Принципи захисту даних у системі обліку: управлінські аспекти. *Економіка, управління та адміністрування.* 2021. № 2 (96). С. 61–69. DOI: https://doi.org/10.26642/ema-2021-2(96)-61-69 (дата звернення: 12.05.2026).

12. Литвиненко В.С. Функції бухгалтерського обліку в умовах цифрової трансформації управління підприємством. *Цифрова економіка та економічна безпека.* 2026. № 2(23). С. 393-400. URL: https://dees.iei.od.ua/index.php/journal/article/view/1032 (дата звернення: 20.05.2026).

13. Правдюк Н.Л., Правдюк М.В. Штучний інтелект як каталізатор трансформаційних процесів у бухгалтерському обліку. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*. 2024. № 1 (67). С.69-83. URL: https://socrates.vsau.org/repository/getfile.php/36727.pdf (дата звернення: 15.05.2026).

14. Про бухгалтерський облік та фінансову звітність в Україні: Закон України від 16.07.1999 № 996-XIV. URL: https://zakon.rada.gov.ua/laws/show/996-14 (дата звернення: 12.05.2026).

15. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 15.05.2026).

16. Про інформацію: Закон України від 02.10.1992 №2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 12.05.2026).

17. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.05.2026).

18. Рік після атаки вірусу Petya: що змінилося в кібербезпеці України https://www.radiosvoboda.org/a/29336511.html (дата звернення: 15.05.2026).

19. Стратегія кібербезпеки України: Рішення РНБО від 14.05.2021: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 12.05.2026).

20. Ясінська А.І. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство*. 2023. № 56. С. 331–336. DOI: https://doi.org/10.32782/2524-0072/2023-56-118 (дата звернення: 12.05.2026).

REFERENCES:

1. CERT-UA (2026) Ofitsiinyi sait Komandy reahuvannia na kompiuterni nadzvychaini podii Ukrainy [Official website of the Computer Emergency Response Team of Ukraine]. Available at: https://cert.gov.ua (accessed May 12, 2026).

2. ISACA (2018) COBIT 2019 Framework: Introduction and Methodology. Rolling Meadows: ISACA, 100 p. Available at: https://rms.koenig-solutions.com/Sync_data/Trainer/QMS/1827-2022414376-Cobit2019.pdf (accessed May 12, 2026).

3. ISO/IEC 27001:2022 (2022) Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: ISO, 23 p. Available at: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf (accessed May 12, 2026).

4. NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology, 55 p. Available at: https://doi.org/10.6028/NIST.CSWP.04162018 (accessed May 12, 2026).

5. Romney M. B., Steinbart P. J. (2018) Accounting Information Systems. 14th ed. Harlow: Pearson, 752 p.

6. Vasylishyn S. I. (2020) Oblikovo-analitychne zabezpechennia v systemi ryzykiv ta zahroz ekonomichnoi bezpeky ahrarnykh pidpryiemstv Ukrainy: monohrafiia [Accounting and analytical support in the system of risks and threats to the economic security of agricultural enterprises of Ukraine: monograph]. Kharkiv: TOV «Drukarnia Madryd», 419 p. (in Ukrainian)

7. Hutsalenko L. V. (2010) Adaptyvna systema obliku i kontroliu rezultativ diialnosti silskohospodarskykh pidpryiemstv: monohrafiia [Adaptive system of accounting and control of agricultural enterprises performance results: monograph]. Kyiv: NNTs IAE, 372 p. (in Ukrainian)

8. Zhuk V. M., Vasylyshyn S. I., Nezhyd Yu. S. (2025) Oblikovo-informatsiine zabezpechennia upravlinnia ahropidpryiemstvamy v umovakh nadzvychainykh sytuatsii ta povoiennykh vyklykiv [Accounting and information support for the management of agricultural enterprises under emergency situations and post-war challenges]. Efektyvna ekonomika, no. 10. Available at: http://doi.org/10.32702/2307-2105.2025.10.14 (accessed May 12, 2026).

9. Ivanova N. A., Yatsko M. V., Derevianko S. I. (2026) Otsinka efektyvnosti systemy vnutrishnoho kontroliu kiberbezpeky khmarnykh oblikovykh platform [Assessment of the effectiveness of the internal cybersecurity control system of cloud accounting platforms]. *Aktualni pytannia ekonomichnykh nauk,* no. 21. Available at: https://doi.org/10.5281/zenodo.19478268 (accessed May 12, 2026).

10. Kytsiuk V. M., Pupynin O. S. (2024) Informatsiina bezpeka pidpryiemstva: teoretychnyi aspekt [Information security of the enterprise: theoretical aspect]. Suchasnyi zakhyst informatsii, no. 2(58), pp. 103–108. Available at: https://doi.org/10.31673/2409-7292.2024.020012 (accessed May 12, 2026).

11.Lehenchuk S. F., Tsaruk I. M., Nazarenko T. P. (2021) Pryntsypy zakhystu danykh u systemi obliku: upravlinski aspekty [Principles of data protection in the accounting system: managerial aspects]. *Ekonomika, upravlinnia ta administruvannia*, no. 2(96), pp. 61–69. Available at: https://doi.org/10.26642/ema-2021-2(96)-61-69 (accessed May 12, 2026).

12. 12. Lytvynenko V. S. (2026) Funktsii bukhhalterskoho obliku v umovakh tsyfrovoi transformatsii upravlinnia pidpryiemstvom [Functions of accounting in the conditions of digital transformation of enterprise management]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, no. 2(23), pp. 393-400. Available at: https://dees.iei.od.ua/index.php/journal/article/view/1032 (accessed May 20, 2026).

13. Pravdiuk N. L., Pravdiuk M. V. (2024) Shtuchnyi intelekt yak katalizator transformatsiinykh protsesiv u bukhhalterskomu obliku [Artificial intelligence as a catalyst for transformational processes in accounting]. *Ekonomika, finansy, menedzhment: aktualni pytannia nauky i praktyky*, no. 1(67), pp. 69–83. Available at: https://socrates.vsau.org/repository/getfile.php/36727.pdf (accessed May 15, 2026).

14. Pro bukhhalterskyi oblik ta finansovu zvitnist v Ukraini: Zakon Ukrainy vid 16.07.1999 №996-XIV [On Accounting and Financial Reporting in Ukraine: Law of Ukraine dated July 16, 1999 No. 996-XIV]. Available at: https://zakon.rada.gov.ua/laws/show/996-14 (accessed May 12, 2026).

15. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.2010 № 2297-VI [On Personal Data Protection: Law of Ukraine dated June 1, 2010 No. 2297-VI]. Available at: https://zakon.rada.gov.ua/laws/show/2297-17 (accessed May 15, 2026).

16. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 №2657-XII [On Information: Law of Ukraine dated October 2, 1992 No. 2657-XII]. Available at: https://zakon.rada.gov.ua/laws/show/2657-12 (accessed May 12, 2026).

17. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 №2163-VIII [On the Basic Principles of Cybersecurity of Ukraine: Law of Ukraine dated October 5, 2017 No. 2163-VIII]. Available at: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed May 12, 2026).

18. Rik pislia ataky virusu Petya: shcho zminylosia v kiberbezpetsi Ukrainy [A year after the Petya virus attack: what has changed in Ukraine's cybersecurity]. Available at: https://www.radiosvoboda.org/a/29336511.html (accessed May 15, 2026).

19. Stratehiia kiberbezpeky Ukrainy: Rishennia RNBO vid 14.05.2021: Ukaz Prezydenta Ukrainy vid 26.08.2021 №447/2021 [Cybersecurity Strategy of Ukraine: National Security and Defense Council Decision dated May 14, 2021: Decree of the President of Ukraine dated August 26, 2021 No. 447/2021]. Available at: https://zakon.rada.gov.ua/laws/show/447/2021 (accessed May 12, 2026).

20. Yasinska A. I. (2023) Informatsiina bezpeka pidpryiemstva: kontseptualni zasady efektyvnoho zakhystu informatsii [Information security of the enterprise: conceptual foundations of effective information protection]. *Ekonomika ta suspilstvo*, no. 56, pp. 331–336. Available at: https://doi.org/10.32-82/2524-0072/2023-56-118 (accessed May 12, 2026).

Дата надходження статті: 17.04.2026
Дата прийняття статті: 15.05.2026
Дата публікації статті: 27.05.2026