КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1209
УДК 004(4):005(4)

Капелюшна Тетяна Вікторівна
д-р. екон. н, доцент, професор кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0001-7490-6751
t.kapeliushna@duikt.edu.ua

Мужанова Тетяна Михайлівна
к. держ.упр., доцент, доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-7435-0287
muzanovat@gmail.com

Дьячук Олександр Станіславович
аспірант кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0006-5585-6393
realjewua@gmail.com

КОНЦЕПТ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЦИФРОВОГО СЕРЕДОВИЩА В ЕКОСИСТЕМІ ПІДПРИЄМСТВА

Анотація. У статті представлено концепт управління інформаційною безпекою та захисту цифрового середовища підприємства в межах загальної екосистеми «бізнесу за вимогою». Обґрунтовано перехід від сегментованого захисту до формування екосистеми безперебійного потоку інформації, що базується на когерентності взаємодії стейкголдерів. Проведено декомпозицію об'єктів захисту на основні (критичні дані, бізнес-процеси) та допоміжні (IT-інфраструктура, персонал, приміщення) активи. Особливу увагу приділено трансформації ролі штучного інтелекту в системі кіберзахисту, запропоновано механізм моніторингу вхідного трафіку на основі технології IDS-GAN та впровадження ШІ-агентів, які підлягають окремому аудиту та контролю. Концепт спрямований на інтеграцію внутрішньої системи управління безпекою із зовнішнім інституційним та регуляторним середовищем України, з відзначенням ролі Національного банку України у забезпеченні безпеки фінансових операцій через платформу MISP-NBU та дотримання стандартів серії ДСТУ ISO/IEC 27000. Встановлено взаємозв'язок між технічною спроможністю підприємства та вимогами НКЕК у сфері електронних комунікацій. Враховуючи ризики блекаутів, у моделі імплементовано модель C2M2 Міністерства енергетики України для оцінки кібербезпеки енергетичної складової бізнесу. Доведено, що ефективне управління цифровим середовищем вимагає багаторівневої структури контролю (від стратегічного до операційного) та обов'язкового криптографічного захисту каналів взаємодії. Отримані результати можуть слугувати методологічним підґрунтям для розробки комплексних програм кіберрезильєнтності, що забезпечують безперервність потоків інформації за умови синергії технологічних інновацій та нормативної відповідності, окрім того, можуть бути використані представниками IT-департаментів та спеціалістами з ризик-менеджменту для побудови адаптивних систем захисту в умовах невизначеності.

Ключові слова: безпека, інформаційна безпека, екосистема підприємства, захист цифрового середовища, управління безпекою підприємств, концепт управління інформаційною безпекою.

ВСТУП

Цифровізація та перехід до функціонування підприємств як «бізнесу за вимогою» (business-on-demand) актуалізують потребу у перегляді та доповненні усталених підходів до захисту інформаційного периметра підприємства для того, щоб забезпечувати його дієвість з врахуванням змін, що відбуваються в оточенні. Формування складних цифрових екосистем, що об'єднують внутрішні активи, хмарні сервіси

та розгалужені мережі постачальників, зумовлює необхідність перегляду стратегій кібербезпеки. Питання забезпечення безперебійного потоку інформації наразі розглядається не лише в технічній площині, а як складний процес досягнення когерентності між суб'єктами ІБ, технологічними рішеннями та потребує взаємодії із регуляторним середовищем.

Актуальність дослідження обумовлюється залежністю бізнес-процесів від стабільності енергопостачання та цілісності електронних комунікацій, що було підтверджено викликами енергетичної безпеки через постійні обстріли енергооб'єктів. Водночас інтеграція агентів штучного інтелекту в архітектуру управління безпекою створює нові вектори як для захисту, так і для виникнення специфічних загроз. У цьому контексті розробка цілісного концепту управління інформаційною безпекою, який поєднує внутрішній контроль підприємства із вимогами національних регуляторів (НБУ, НКЕК, Держспецзв'язку) та міжнародними стандартами ISO/IEC, стає нагальним завданням для захисту цифрового середовища підприємства при обміні інформацією та забезпечення безперервності бізнес-процесів.

Постановка проблеми. Глобалізація світових ринків, посилення співпраці між організаціями різних країн та активне використання електронних комунікацій створили умови до активного провадження електронного бізнесу, який наразі перестав бути просто технологічною перевагою, а перетворився на платформу, що забезпечує функціонування організацій в кіберпросторі. Стрімкий розвиток та доступність мобільних технологій пришвидшили цифровізацію ринку, водночас перенаправляючи питання безпеки у площину критичних щодо гарантування конфіденційності, цілісності, доступності даних та безперервності бізнес-процесів. Організації потребують захищеного середовища для інформаційних активів, оскільки будь-який кіберінцидент призводить до втрати довіри клієнтів (репутаційних ризиків) та інформаційних ризиків для підприємства.

Проблемою для господарюючих суб'єктів залишається їх вразливість, підприємства електронного бізнесу (e-business) чутливі до безпекових ризиків через постійну потребу використання інформаційно-комунікаційних технологій (ІКТ). Багато компаній зазнають збитків з причин відсутності комплексної системи управління інформаційною безпекою (СУІБ/ISMS) або базового процесного підходу до управління безпекою. Бізнес-середовище під дією екзистенційних загроз характеризується невизначеністю та важкопрогнозованістю щодо майбутнього функціонування. Окрім того, організації зазнають кібератак та перебувають під тиском інформаційної деформації щодо майбутніх подій. Зважаючи на зміни, які обумовлені активним переходом підприємств у цифрову площину провадження бізнесу, а саме: використання хмарних обчислень, мобільність персоналу, використання ШІ-агентів, автоматизація бізнес-процесів, ІКТ-аутсорсинг, виникають цифрові ризики, які важко визначити заздалегідь. Також варто враховувати складність екосистеми організацій, що функціонують у кіберпросторі через цифрову пов'язаність суб'єктів і даних, що створює середовище, де вразливість одного партнера загрожує всьому ланцюгу взаємодії (ланцюг постачання), мережі. Тому управління безпекою підприємства має ґрунтуватися не суто на традиційних підходах щодо забезпечення безперервності бізнесу, а включати до захисту активів – інформаційні ресурси, а також забезпечувати захист цифрового поля взаємодії з оточенням (стейкголдерами) в екосистемі підприємства. Адже, в іншому випадку, підприємства будуть нерезильєнтними, не матимуть запасу міцності та алгоритмів для швидкого відновлення, не встигатимуть зреагувати на момент виникнення загрози й нестимуть збитки.

Аналіз останніх досліджень та публікацій. Аналіз наукових робіт свідчить, що проблематика управління інформаційною безпекою підприємств є об'єктом вивчення не тільки фахівців та експертів з кібербезпеки, а й економістів, юристів та спеціалістів з державного управління. Міждисциплінарна зацікавленість науковців та практиків щодо забезпечення кібербезпеки та захисту інформації обумовлена інтеграцією цифрових активів у бізнес-процеси та правове поле держави.

Економічний та управлінський аспекти забезпечення кіберстійкості висвітлено у працях М. А. Мащенко та Є. М. Іполітова [1]. Автори наголошують, що впровадження міжнародних стандартів, зокрема ISO/IEC 27001:2022, у поєднанні зі стратегічно орієнтованою системою захисту, дозволяє підприємствам сформувати системний підхід до управління ризиками. Підкреслюють, що чітке визначення стратегічних цілей є ключовим для зниження загроз і посилення захисту інформаційних систем. Питання організаційно-управлінських механізмів ІБ розглядаються авторами І. Крамаренко, І. Іртищевою, С. Білоусовою, С. Іртищевим в контексті сталого розвитку та цифрової трансформації економіки України. Основна увага приділяється процесам встановлення цілей та аудиту ефективності заходів ІБ, як невід'ємної складової загального менеджменту підприємства [2].

Особливості функціонування систем ІБ в умовах воєнного стану та кризового управління досліджуються у працях К. Озарко та С. Копитко [3], а також П. Гриценка [4]. Основний акцент у роботах – важливість системного підходу, що об'єднує персонал, бізнес-процеси та комплексні інформаційні системи (апаратне та програмне забезпечення). Головною метою таких систем визначено

підтримку безперервності бізнес-процесів, що є критичним для виживання підприємств у невизначеному середовищі.

Корпоративний сектор та управління цифровими ризиками аналізують вчені О. Сороківська, Т. Кужда та Н. Кіналь [5], ними запропонована п'ятикомпонентна модель (структура, технології, ризики, дані, аудит), спрямована на мінімізацію кіберзагроз через призму сталого розвитку. У своїй праці О. Плесюк [6] виокремлює управління цифровими ризиками (digital risk management) як функціональний напрям менеджменту, пропонуючи синергію внутрішніх безпекових підрозділів із зовнішніми IT-консультантами.

Правовий аспект та виклики, пов'язані з новими технологіями, знаходяться у фокусі уваги К. Резворовича та Ю. Толмачової [7]. Автори порушують питання балансу між технологічним прогресом (зокрема ШІ) та відповідальністю, розглядаючи цифрові ризики й права людини, що підтверджує взаємозв'язок управління ІБ та юридичною відповідальністю.

Технологічна та методологічна основа класифікації ризиків представлена у роботах науковців В. Степанова [8], а також Ю. Костюк, П. Складанного, Б. Бебешка, К. Хорольської, С. Рзаєвої, М. Ворохоба [9], якими ґрунтовно розглядаються комплексні системи захисту інформації, методологія якісного та кількісного оцінювання інформаційних ризиків, математичний апарат для розв'язання прикладних задач у кібербезпеці та прийняття управлінських рішень.

У своїй праці В. Болек, А. Романова, Ф. Корцек [10] на основі даних, отриманих за результатами опитування, яке було проведено серед представників 91 підприємства електронної комерції на словацькому ринку (переважно мікропідприємства – 73,63%), стверджують, що немає статистично значущої кореляції між часткою витрат на ІБ у загальних витратах та рівнем захищеності підприємства. Це пояснюється тим, що високого рівня безпеки можна досягти не лише високовартісними технічними засобами, а й безкоштовними організаційними заходами (розробка політик, навчання персоналу).

Таким чином, за результатами огляду наукових праць, присвячених інформаційній безпеці, її можна визначити як складну екосистему, де технічні засоби контролю діють у синергії з економічними стратегіями та правовими нормами, що дозволить досягти високого рівня безпеки. З поміж тим, екосистема бізнесу «за вимогою» потребує формування нових підходів, концептів управління інформаційною безпекою та захисту цифрового середовища підприємства при взаємодії з оточенням (стейкголдерами) в процесі передачі даних.

Мета статті. Дослідити цифрове середовище в екосистемі підприємства та сформувати концепт його захисту задля забезпечення безперебійного потоку інформації в організації.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Традиційне управління безпекою в е-бізнесі забезпечується через контроль ізольованих доменів, таких як: технологічний рівень (спеціалізоване апаратне та програмне забезпечення); організаційний рівень (політики, процедури та навчання персоналу); стратегічний/законодавчий рівень (відповідність стандартам і правовим нормам). За доменами сформувалася парадигма управління інформаційною безпекою, яка не ставиться під сумнів, може тільки доповнюватися й збагачуватися через варіативність умов функціонування підприємств, в якій головним активом виступає – інформаційний.

Інформаційні активи представляють собою не просто повідомлення й знання у вигляді накопиченої інформації, структурованих або неструктурованих даних, а цінний актив – фактор виробництва, який визнано на рівні із традиційними (земля, праця, капітал, підприємницькі здібності).

Згідно із нормативно-правовим документом (Методикою оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж), інформаційні активи можуть бути на будь-якому носії й представлятися як у цифровій, так і не цифровій формі: бізнес-дані, інтелектуальна власність, інформація про клієнтів, контракти, договори, журнали безпеки, метадані, оперативні дані, фінансові дані, інформація про безпеку та журнали керування подіями, файли конфігурації [11].

Інформаційний актив, який має нематеріальний характер й представляє цінність для підприємства називається гудвіл – накопичені нематеріальні активи підприємства, що включають його найменування, репутацію, ділові зв'язки (у тому числі клієнтуру), товарні знаки тощо; власність фірми («власність» має досить широке тлумачення й охоплює цілу низку економічних інтересів (активів) – як матеріальних, так і нематеріальних) [12]. Тобто йдеться про активи, які формують сприйняття компанії загалом, стекголдерами, в якому важливу роль відіграє захист персональних даних, інтелектуальної власності, бізнес-зв'язків через інфокомунікаційні платформи. У продовження питання когерентності взаємодії бізнес-партнерів у кіберпросторі, потребує уваги питання надання послуг ІКТ і їх безпеки. Послугам електронних комунікацій характерні нематеріальність та невідчутність (послуга не має фізичної форми,

її неможливо попередньо осягнути, протестувати чи оцінити до моменту отримання; не передбачає переходу права власності, а лише реалізацію права користування).

Провіши аналіз останніх публікацій, у яких досліджуються питання інформаційної безпеки, можна зробити висновок, що зростає кількість статей в періодичних виданнях правничого та економічного напрямів, що пояснюється актуальністю ІБ у всіх сферах через активну цифровізацію суспільства та бізнес-процесів, активним провадженням діяльності в кіберпросторі. Послуги сфери електронних комунікацій формують надійну основу (за умови їх безпечного та якісного надання) для провадження електронного бізнесу, забезпечуючи безперервність бізнес-процесів. Їх специфіка визначається поєднанням класичних характеристик послуг із новими властивостями, зумовленими цифровим середовищем. Передусім, послуги електронних комунікацій характеризуються цифровою природою корисного ефекту, який реалізується через створення, обробку, передачу та зберігання інформації. Споживча цінність таких послуг формується не лише в момент їх надання, а й у процесі подальшого використання інформаційних ресурсів.

Важливою особливістю є технологічна опосередкованість та інфраструктурна залежність, так як надання послуг здійснюється через складні інформаційно-комунікаційні системи (мережі зв'язку, серверні потужності, програмні платформи), що забезпечують їх масштабованість, доступність та автоматизацію.

Послуги електронних комунікацій, зберігаючи загальну нематеріальність, набувають ознак часткової матеріалізації через прив'язку до інформаційних носіїв, технічної інфраструктури та програмних продуктів. Водночас економічна цінність концентрується не в матеріальних елементах, а в інформації як стратегічному ресурсі. Це зумовлює переорієнтацію управлінських підходів із матеріальних активів на інформаційні активи, про зазначалося вище.

Крім того, відбувається трансформація таких класичних характеристик, як незбережуваність та варіативність, оскільки результати надання послуг можуть зберігатися у вигляді даних, а їх якість визначається алгоритмами та програмним забезпеченням, що забезпечує одночасно стандартизацію та персоналізацію сервісів.

За таких умов особливої актуальності набуває проблема захисту послуг електронних комунікацій, оскільки їх функціонування безпосередньо залежить від стану інформаційних активів і рівня їх захищеності. Вразливість цифрового середовища до кіберзагроз (несанкціонований доступ, витік даних, порушення цілісності та доступності інформації) створює ризики не лише для окремих операцій, але й для безперервності діяльності підприємства в цілому.

Отже, інструментом забезпечення стійкості електронного бізнесу виступає управління інформаційною безпекою підприємства, яке передбачає системний, процесно-орієнтований підхід до ідентифікації, оцінювання та мінімізації ризиків. Впровадження системи управління інформаційною безпекою (ISMS) дозволяє:

- забезпечити конфіденційність, цілісність і доступність інформаційних ресурсів;
- мінімізувати наслідки кіберінцидентів та запобігати їх виникненню;
- підтримувати довіру клієнтів і партнерів;
- гарантувати безперервність надання електронних послуг;
- оптимізувати витрати на безпеку шляхом концентрації ресурсів на критично важливих активах.

Таким чином, послуги сфери електронних комунікацій характеризуються гібридною природою, поєднуючи нематеріальність із цифровою інфраструктурною датацентричністю. Це об'єктивно зумовлює необхідність інтеграції механізмів управління інформаційною безпекою у всі етапи їх створення та надання, що є передумовою ефективного функціонування підприємства в умовах цифровізації бізнес-процесів, які посилюються за умов невизначеності.

Інтеграція бізнес-процесів представляє собою системно організований процес об'єднання функціональних, інформаційних, технологічних та організаційних компонентів діяльності підприємства в єдину узгоджену архітектуру, що забезпечує безперервний обмін даними, синхронізацію операцій та досягнення стратегічних цілей бізнесу. Сучасна інтеграція охоплює не лише внутрішні процеси (ERP, CRM, фінанси, логістика), але й зовнішні взаємодії з партнерами, клієнтами та постачальниками, формуючи концепцію «бізнесу за вимогою» (on-demand business). Бізнес за вимогою є моделлю цифрової комерції, що базується на архітектурі миттєвого доступу до ресурсів, товарів та сервісів через інтегровані цифрові платформи, а також реалізує стратегічну синергію між незалежними контрагентами та кінцевими споживачами, забезпечуючи проведення транзакції у режимі реального часу та мінімізацію часу на її реалізацію [13]. В Директиві Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу йдеться про питання активного розвитку інтернет-платформ й приведено наступне: «З огляду на виникнення

інноваційних технологій і нових бізнес-моделей очікується поява на внутрішньому ринку нових моделей послуг і розгортання хмарних обчислень у відповідь на розвиток потреб споживачів» [14].

Отже, постає потреба у побудові моделі, що передбачає створення єдиного інформаційного простору, у якому дані, процеси та користувачі функціонують як взаємопов'язана система.

Повертаючись до питання активів, доцільно їх групувати за стандартом ISO 27002:2022 на [15]:

– допоміжні (апаратне забезпечення, програмне забезпечення, мережа, персонал (керівники, працівники, підрядники)), сайти;
– основні (інформація та бізнес-процеси).

В останній редакції міжнародного стандарту ISO/IEC 27001:2022 відображено суттєві зміни у підходах до управління інформаційною безпекою, зумовлені розвитком цифрових технологій, інтеграцією бізнес-процесів та зростанням загроз у невизначеному середовищі функціонування підприємств. Структурна трансформація доменів безпеки відбулася через перегрупування 114 контрольних заходів, що спрощує їх застосування та відображає системний характер управління безпекою.

Контролі за стандартом поділяються на домени [15]:

– люди (people) охоплює аспекти, пов'язані з поведінкою, компетенціями та відповідальністю персоналу (політики конфіденційності, безпека віддаленої роботи, підвищення обізнаності з кібербезпеки);
– організаційний (organizational) включає управлінські та процесні аспекти (політики інформаційної безпеки; управління ризиками; безпека у хмарних сервісах; забезпечення безперервності бізнесу);
– технологічний (technological) охоплює технічні механізми захисту (автентифікація та контроль доступу, запобігання витоку даних, моніторинг активності, безпечна розробка програмного забезпечення);
– фізичний (physical) розглядає питання фізичного захисту (контроль доступу до приміщень, захист носіїв інформації, моніторинг фізичної безпеки).

Серед 11 контролів, що з'явилися в стандарті – готовність ІКТ для забезпечення неперервності бізнесу (5.30), згідно якого організації повинні створювати план неперервності ІКТ для забезпечення операційної стійкості.

Основні підходи до управління інформаціною безпекою підприємств, зважаючи на об'єкти захисту, наступні (таблиця 1):

– техноцентричний підхід, в межах якого основна увага приділялася захисту саме технічній складовій – IT-інфраструктурі, технічним заходам (мережевий захист, антивірусні системи, контроль доступу), а управління має реактивний характер;
– процесно-орієнтований (ISMS), що передбачає інтеграцію безпеки у бізнес-процеси підприємства, а управління інформаційною безпекою здійснюється на основі стандартизованих підходів, ризик-менеджменту та циклу безперервного вдосконалення (PDCA);
– ризик-орієнтований підхід змістив акцент із суцільного захисту всіх активів на ідентифікацію та пріоритезацію критичних активів, що дозволило оптимізувати витрати на безпеку та підвищити ефективність управлінських рішень;
– людиноцентричний підхід, що враховує поведінкові аспекти, рівень обізнаності персоналу та ризики соціальної інженерії, персонал розглядається не лише як джерело загроз, але і як активний елемент системи безпеки;
– комплексний підхід поєднує найкращі практики з кожного підходу;
– екосистемний підхід базується на концепціях Zero Trust та кіберстійкості (cyber resilience), поява якого обумовлена властивістю теперішньої складної цифрової екосистеми, яка охоплює хмарні сервіси, мобільні пристрої, IoT та розподілені середовища.

Таблиця 1

Підходи до управління інформаційною безпекою підприємств за об'єктами захисту

Об'єкти захисту (фокус)	Підхід	Суть
Люди	людиноцентричний підхід	персонал розглядається як основний елемент системи безпеки та одночасно як потенційне джерело ризиків
Бізнес-процеси	процесно-орієнтований підхід	безпека інтегрується у всі бізнес-процеси, відображає процесно-орієнтовану та ризик-орієнтовану парадигми (ISMS)

Продовження таблиці 1

Активи	ризик-орієнтований підхід	ідентифікація та пріоритезація критичних активів
IT-інфраструкутра	техноцентричний підхід	захист цифрового середовища
Люди; бізнес-процеси; активи; IT-інфраструктура	комплексний підхід	захист за пріоритеними напрямами з кожного вищепереліченого підходу (персонал, бізнес-процес, ризик, актив, IT-інфраструктура)
Цифрова екосистема	екосистемний підхід	екосистема управління ризиками, кіберстійкість (cyber resilience) розподілених середовищ у цифровій екосистемі
Процесні активи (бізнес-процеси; інтеграційні сценарії; автоматизовані ланцюги прийняття рішень)	агентно-орієнтований (Agentic AI)	забезпечення цілісності, довіри та стійкості цифрових процесів в екосистемі

Цифрові трансформації в суспільстві та бізнесі зумовили потребу включення у підходи взаємоінтегрованості систем та процесів, формування цифрових екосистем, забезпечення їх безпечного і безперервного фінкціонування.

Зважаючи на активне використання та впровадженням інструментів ШІ, зокрема переходом від допоміжних інтелектуальних систем до автономних агентів (Agentic AI), здатних самостійно приймати рішення та взаємодіяти з цифровим середовищем, формується агентно-орієнтований концепт управління інформаційною безпекою, ознаками якого є:

- розширення об’єкта захисту до автономних агентів, моделей та алгоритмів;
- поява нових класів ризиків (маніпуляції моделями, атаки на промпти, викривлення даних);
- перехід від контролю доступу до управління взаємодіями між агентами, системами та даними;
- необхідність забезпечення прозорості, підзвітності та пояснюваності рішень ШІ;
- інтеграція криптографічного захисту та принципів Zero Trust у взаємодію агентів у гібридних середовищах.

Таким чином, інформаційна безпека трансформується з функції захисту ресурсів у систему управління поведінкою цифрових суб’єктів та взаємодіями в динамічних екосистемах, що вказує на можливість використання агентно-орієнтованого (захист агентів, управління взаємодіями) підходу до управління інформаційною безпекою підприємств.

Формування екосистеми безперебійного потоку інформації в бізнесі «за вимогою» передбачає когерентність між суб’єктами взаємодії (стейкголдерами) задля забезпечення захисту цифрового середовища (зовнішнього та внутрішнього) при обміні інформацією. Управління інформаційною безпекою в екосистемі підприємства передбачає формування нового погляду щодо захисту інформації в частині формування каналів взаємодії та включення до об’єктів захисту (дані, користувачі, системи) агентів ШІ. Екосистема представляє собою взаємодію між стейкголдерами, які не обмежуються лише їх внутрішніми взаємозв’язками, а передбачається комунікація із регуляторами з питань кібербезпеки та захисту інформації у сферах, де використовуються електронні комунікації.

Підприємства користуються платіжними послугами, відповідно, взаємодіють із банками та іншими об’єктами, що здійснюють діяльність на фінансових ринках. Безпекові питання, у тому числі кібербезпеки, щодо проведення платіжних операцій, банківських послуг, фінпослуг регулює Національний банк України [16]. НБУ надає доступ до спеціалізованого сайту MISP-NBU Центру кіберзахисту (Malware Information Sharing Platform of the National Bank of Ukraine), що побудований на базі платформи з відкритим програмним кодом MISP, а також призначений для організації доступу банків до системи збору, обробки, зберігання і обміну інформацією загального організаційного та технічного характеру в режимі реального часу з урахуванням вимог конфіденційності. Окрім того, банки при розробці політики інформаційної безпеки керуються Національними стандартами України з питань інформаційної безпеки: ДСТУ ISO/IEC 27000:2019 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів»; ДСТУ ISO/IEC 27001:2022 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»; ДСТУ ISO/IEC 27002:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки»; ДСТУ ISO/IEC 27010:2018 «Інформаційні технології. Методи захисту. Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій» [17].

Питання контролю безпеки електронних комунікаційних послуг провадить Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (НКЕК) [18].

Державний центр кіберзахисту (ДЦКЗ), а також CERT-UA (Команда реагування на комп'ютерні надзвичайні події України) забезпечують технічний захист функціонування системи та націлені на раннє попередження вразливостей.

Електричні мережі, без яких надання електронних комунікаційних послуг важко уявити (підтвердженням є блекаути впродовж зими), контролює Міністерство енергетики, керуючись моделлю C2M2 спроможності кібербезпеки електричних мереж для оцінки вдосконалення програм з кібербезпеки та зміцнення експлуатаційної здібності.

Ліцензування діяльності у галузі криптографічного захисту інформації (КЗІ) здійснює Держслужба спецзв'язку та захисту інформації.

Згадані регулятори формують зовнішнє середовище в екосистемі потоку інформації на підприємствах, провадять контроль інформаційної безпеки організацій, дотримуючись комплаєнсу в межах сфери своєї діяльності.

Внутрішня екосистема забезпечення безперебійного потоку інформації на підприємствах представлена за блоками: активи, стейкголдери та цифрові канали взаємодії, постачальники послуг та технологічна база, інформація як вхідний трафік та інтелектуальний моніторинг, рівні управління та система контролів за вертикаллю управління, контроль поведінки ШІ-агентів.

Отже, загальний концепт захисту цифрового середовища в екосистемі забезпечення безперебійного потоку інформації на підприємстві, що формує взаємовідносини із стейкхолдерами за принципом бізнес за вимогою, включає внутрішнє та зовнішнє оточення та обмін інформацією між ними (рисунок 1).

1. Активи. Інформаційні активи представлені категоріями основні та допоміжні. Основні активи включають критичні дані та бізнес-процеси підприємства, є об'єктами формування вартості, оскільки забезпечують функціонування та конкурентоспроможність організації. Допоміжні активи охоплюють інфраструктурну складову – системи (апаратне та програмне забезпечення, мережеві ресурси), користувачів (людський капітал) та виробничі приміщення. Зв'язок між ними реалізується через інструменти та технології управління доступом, що підкреслює роль фізичного та логічного захисту периметра.

2. Стейкголдери та цифрові канали взаємодії. Взаємодія зі стекголдерами здійснюється через цифрові канали, які підлягають обов'язковому криптографічному захисту. Це забезпечує цілісність, конфіденційність та автентичність даних, що передаються у відкритих та закритих мережевих середовищах, нівелюючи ризики перехоплення або несанкціонованої модифікації інформації.

Захист вибудовуватиметься за контролями доступу до корпоративної мережі, контролем поведінки як користувачів, так і ШІ-агентів; захистом промтів, логікою прийняття рішень й запобігання маніпуляціям.

3. Постачальники послуг та технологічна база охоплює постачальників електронних комунікацій, операторів системи передачі (ОСП) та системи розподілу (ОСР). Їхня роль інтегрована в загальну екосистему як зовнішнє джерело апаратного та програмного забезпечення. Безпека підприємства безпосередньо залежить від надійності ланцюга постачання, що вимагає впровадження жорстких протоколів перевірки відповідності технічних засобів та програм (ERM, CRM-системи, API-інтерфейси, мобільні додатки) вимогам кіберзахисту систем.

4. Інформація як вхідний трафік та інтелектуальний моніторинг – складова динамічного захисту інформації як вхідного трафіку, якою передбачається впровадження механізмів безперервного моніторингу за допомогою агентів ШІ (AI), зокрема, технології IDS-GAN (Intrusion Detection System на основі Generative Adversarial Networks), що дозволяє виявляти аномалії в трафіку шляхом генерації та аналізу сценаріїв атак, забезпечуючи проактивне реагування на загрози.

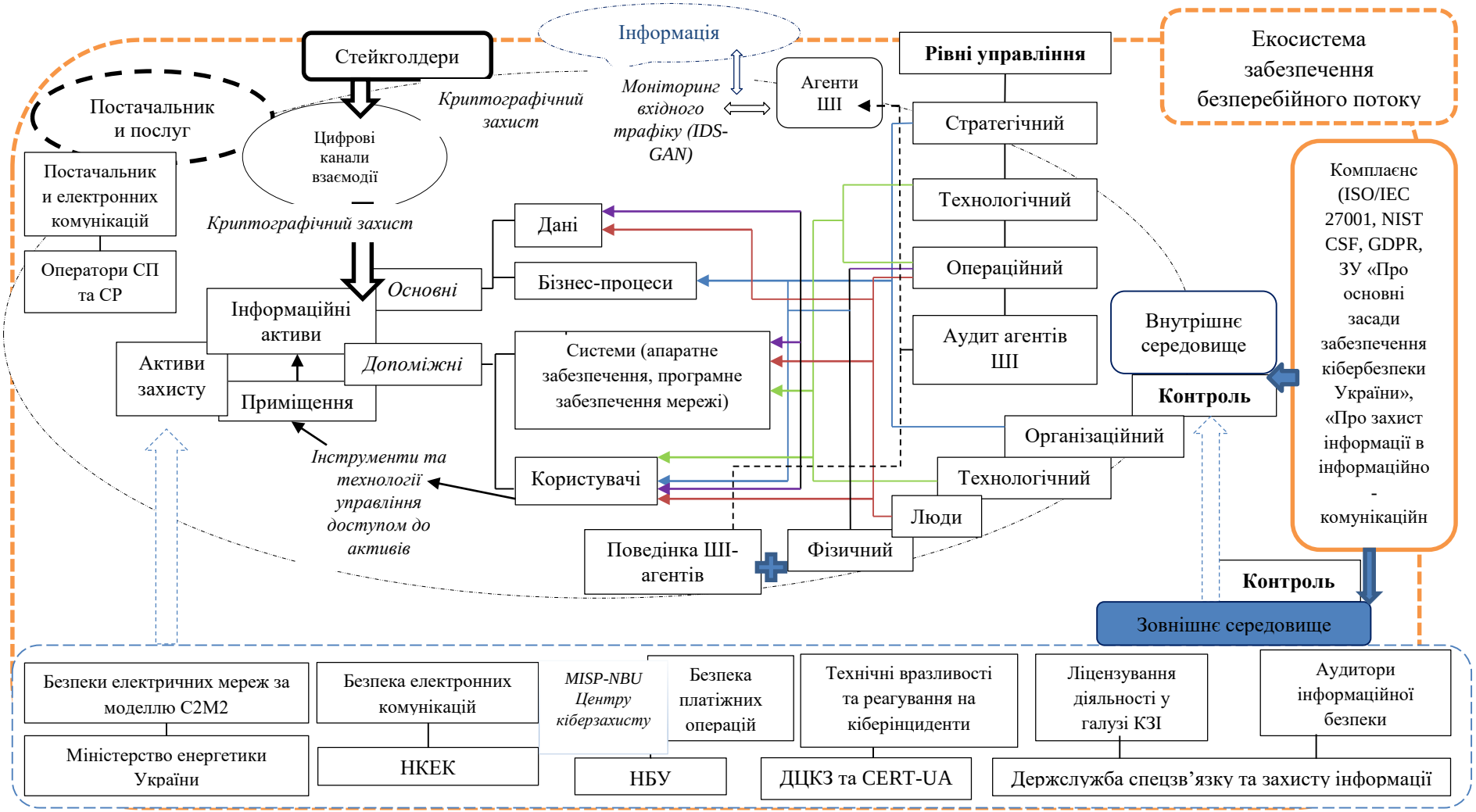

Рис. 1. Концепт захисту цифрового середовища в екосистемі забезпечення безперебійного потоку інформації на підприємств

5. Рівні управління та система контролів за вертикаллю управління:
- стратегічний рівень – для визначення цілей та політик безпеки;
- технологічний – вибір та впровадження засобів захисту;
- операційний – перманентне адміністрування та реагування на інциденти;
- аудит агентів ШІ – спеціалізований рівень контролю за діями автономних систем захисту.

Слід зауважити, що задачі за рівнями управління тісно корелюють із блоком контролів, який розподілений за векторами впливу на організаційний, технологічний, людський (робота з персоналом) та фізичний. Такий взаємозв'язок забезпечує цілісність системи захисту (Defense-in-Depth).

6. Контроль поведінки ШІ-агентів доповнює підходи до управління безпекою в частині включення до контуру безпеки контролю за поведінкою ШІ-агентів. Як зазначалося раніше, автономні системи стають частиною захисної екосистеми, тож потребують верифікації їхньої діяльності, що можна реалізувати шляхом аналізу прийнятих ШІ-рішень щодо фільтрації трафіку, використання криптографічних протоколів для захисту внутрішніх каналів обміну даними між агентами, постійного зворотного зв'язку між результатами моніторингу (IDS-GAN) та блоком аудиту.

ВИСНОВКИ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

За результатами проведеного дослідження сформовано концепт управління інформаційною безпекою підприємства як дворівневої екосистеми, що інтегрує внутрішні технологічні цикли з вимогами зовнішнього регуляторного середовища, а також:

1. Доведено, що в умовах моделі «бізнесу за вимогою» безпека інформаційних потоків досягається не лише через ізоляцію активів, а шляхом забезпечення когерентності між усіма суб'єктами екосистеми. Це вимагає впровадження наскрізного криптографічного захисту цифрових каналів взаємодії та безперервного моніторингу вхідного трафіку.

2. Аргументовано доцільність включення штучного інтелекту у концепт як активного суб'єкта захисту (використання технологій IDS-GAN дозволяє перейти від реактивного до проактивного виявлення аномалій, а включення ШІ-агентів до переліку об'єктів контролю мінімізує ризики, пов'язані з автономністю інтелектуальних систем).

3. Встановлено, що стійкість підприємства безпосередньо залежить від глибини його інтеграції в національну інфраструктуру кібербезпеки. Використання інструментів MISP-NBU, дотримання стандартів ISO/IEC 27001/27002 та врахування галузевих моделей спроможності (C2M2 для енергетики) створюють необхідний базис для забезпечення безперебійності бізнес-процесів.

4. Сформована ієрархія (від стратегічного планування до аудиту ШІ-агентів) забезпечує детермінованість процесів контролю, де кожен рівень управління відповідає за конкретний вектор захисту (організаційний, технологічний, людський або фізичний).

Представлений концепт має перспективи для подальших наукових розробок та прикладних впроваджень, зокрема, розробці алгоритмів етичного та безпекового аудиту ШІ; створенні формалізованих методик моніторингу поведінки автономних агентів для запобігання вторгненню та несанкціонованим змінам у політиках безпеки, ініційованих самим штучним інтелектом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mashchenko, M., & Ippolitov, Y. (2024). Formation of an enterprise information security enhancement strategy. *Entrepreneurship, Trade and Exchange Activities, 2*. https://doi.org/10.32782/2524-0072/2024-70-147
2. Kramarenko, I., Irtyshcheva, I., Bilousova, S., Irtyshchev, O., & Harahulia, A. (2024). Organizational and managerial mechanisms for ensuring information security of entrepreneurial activity in the context of digital transformation of Ukraine's economy. *Entrepreneurship and Innovation, 32*, 246-252. https://doi.org/10.32782/2415-3583/32.38
3. Ozarko, K. S., & Kopytko, S. B. (2023). Features of the functional approach to enterprise information security management under crisis conditions. *Bulletin of Economic Science of Ukraine, 1*(44), 45-49.
4. Hrytsenko, P. (2025). Information security at a state enterprise under martial law and organizational methods of its implementation. *Dictum Factum, 1*(17), 298-306. https://doi.org/10.32703/2663-6352/2025-1-17-298-306
5. Sorokivska, O., Kuzhda, T., & Kinal, N. (2025). Digital risks and information security of the corporate sector. *Herald of Khmelnytskyi National University. Economic Sciences, 342*(3(1)), 95-105. https://doi.org/10.31891/2307-5740-2025-342-3(1)-14

6. Plesiuk, O. (2025). Digital risks in enterprise development management. *Bulletin of Sumy National Agrarian University*, *3*(103), 65-70. https://doi.org/10.32782/bsnau.2025.3.10
7. Rezvorovych, K., & Tolmachova, Y. (2025). Digital risks for human rights: Artificial intelligence between progress and irresponsibility. *Scientific Bulletin of Dnipro State University of Internal Affairs*, *3*(136), 76-86.
8. Stepanov, V. (2024). Digitalization and digital security risks. *Bulletin of the National University of Civil Protection of Ukraine. Series: Public Administration*, *1*, 55-61.
9. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Security of information and communication systems*. Borys Grinchenko Kyiv Metropolitan University.
10. Bolek, V., Romanová, A., & Korček, F. (2023). The information security management systems in e-business. *Journal of Global Information Management*, 1-29. https://doi.org/10.4018/jgim.316833
11. Ministry of Energy of Ukraine. (2024). *Methodology for assessing the cybersecurity state of electrical networks and cybersecurity practices of electrical networks* (Order No. 285). https://zakon.rada.gov.ua/laws/show/z1278-24
12. Reznikova, V., & Kravets, I. (2019). Classification of goods: Economic and legal aspect. *Economics and Law*, *2*(53). https://doi.org/10.15407/econlaw.2019.02.025
13. Council of the European Union. (n.d.). *EU rules on platform work*. https://www.consilium.europa.eu/en/policies/platform-work-eu/#economy
14. Verkhovna Rada of Ukraine. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2)*. https://zakon.rada.gov.ua/laws/show/9a3_001-22
15. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en:term:3.1.20
16. National Bank of Ukraine. (n.d.). *Authorization of payment market participants*. https://bank.gov.ua/ua/supervision/payment-services
17. TASKOMBANK. (2025). *Information security policy*. https://tascombank.ua/files/Polityka_informatsiinoi_bezpeky-2025.pdf
18. National Commission for the State Regulation of Electronic Communications, Radiofrequency Spectrum and Postal Services. (n.d.). *Regulatory activities*. https://nkek.gov.ua/diialnist/rehuliatorna-diialnist

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Tetiana Kapeliushna
Doctor of Economics, Associate Professor, Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-7490-6751
t.kapeliushna@duikt.edu.ua

Tetiana Muzhanova
PhD in Public Administration, Associate Professor, Associate Professor of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-7435-0287
muzanovat@gmail.com

Oleksandr Diachuk
Postgraduate of the Department of Cybersecurity and Information Protection Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0006-5585-6393
realjewua@gmail.com

CONCEPT OF INFORMATION SECURITY MANAGEMENT OF THE DIGITAL ENVIRONMENT IN THE ENTERPRISE ECOSYSTEM

Abstract. The article presents a concept of information security management and protection of the enterprise's digital environment within the overall ecosystem of "on-demand business." The transition from segmented protection to the formation of an ecosystem of uninterrupted information flow based on the coherence of stakeholder interaction is substantiated. Within the proposed approach, a decomposition of protection objects is carried out, distinguishing between primary (critical data, business processes) and supporting (IT infrastructure, personnel, facilities) assets. Special attention is paid to the transformation of the role of artificial intelligence in the cybersecurity system; a mechanism for monitoring incoming traffic based on IDS-GAN technology and the implementation of AI agents subject to separate auditing and control are proposed. The concept is aimed at integrating the internal security management system with the external institutional and regulatory environment of Ukraine, highlighting the role of the National Bank of Ukraine in ensuring the security of financial transactions through the MISP-NBU platform and compliance with the DSTU ISO/IEC 27000 series standards. The relationship between the enterprise's technical capacity and the requirements of the National Commission for the State Regulation of Electronic Communications is established. Considering blackout risks, the model incorporates the C2M2 model of the Ministry of Energy of Ukraine to assess the cybersecurity of the energy component of business operations. It is demonstrated that effective management of the digital environment requires a multi-level control structure (from strategic to operational) and mandatory cryptographic protection of communication channels. The obtained results may serve as a methodological basis for developing comprehensive cyber resilience programs that ensure continuity of information flows through the synergy of technological innovations and regulatory compliance. In addition, they may be applied by IT departments and risk management specialists to build adaptive protection systems under conditions of high uncertainty.

Keywords: security, information security, enterprise ecosystem, digital environment protection, enterprise security management, concept of information security management.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Mashchenko, M., & Ippolitov, Y. (2024). Formation of an enterprise information security enhancement strategy. *Entrepreneurship, Trade and Exchange Activities, 2*. https://doi.org/10.32782/2524-0072/2024-70-147
2. Kramarenko, I., Irtyshcheva, I., Bilousova, S., Irtyshchev, O., & Harahulia, A. (2024). Organizational and managerial mechanisms for ensuring information security of entrepreneurial activity in the context of

digital transformation of Ukraine's economy. *Entrepreneurship and Innovation, 32*, 246-252. https://doi.org/10.32782/2415-3583/32.38

3. Ozarko, K. S., & Kopytko, S. B. (2023). Features of the functional approach to enterprise information security management under crisis conditions. *Bulletin of Economic Science of Ukraine, 1*(44), 45-49.
4. Hrytsenko, P. (2025). Information security at a state enterprise under martial law and organizational methods of its implementation. *Dictum Factum, 1*(17), 298-306. https://doi.org/10.32703/2663-6352/2025-1-17-298-306
5. Sorokivska, O., Kuzhda, T., & Kinal, N. (2025). Digital risks and information security of the corporate sector. *Herald of Khmelnytskyi National University. Economic Sciences, 342*(3(1)), 95-105. https://doi.org/10.31891/2307-5740-2025-342-3(1)-14
6. Plesiuk, O. (2025). Digital risks in enterprise development management. *Bulletin of Sumy National Agrarian University, 3*(103), 65-70. https://doi.org/10.32782/bsnau.2025.3.10
7. Rezvorovych, K., & Tolmachova, Y. (2025). Digital risks for human rights: Artificial intelligence between progress and irresponsibility. *Scientific Bulletin of Dnipro State University of Internal Affairs, 3*(136), 76-86.
8. Stepanov, V. (2024). Digitalization and digital security risks. *Bulletin of the National University of Civil Protection of Ukraine. Series: Public Administration, 1*, 55-61.
9. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Security of information and communication systems*. Borys Grinchenko Kyiv Metropolitan University.
10. Bolek, V., Romanová, A., & Korček, F. (2023). The information security management systems in e-business. *Journal of Global Information Management*, 1-29. https://doi.org/10.4018/jgim.316833
11. Ministry of Energy of Ukraine. (2024). *Methodology for assessing the cybersecurity state of electrical networks and cybersecurity practices of electrical networks* (Order No. 285). https://zakon.rada.gov.ua/laws/show/z1278-24
12. Reznikova, V., & Kravets, I. (2019). Classification of goods: Economic and legal aspect. *Economics and Law, 2*(53). https://doi.org/10.15407/econlaw.2019.02.025
13. Council of the European Union. (n.d.). *EU rules on platform work*. https://www.consilium.europa.eu/en/policies/platform-work-eu/#economy
14. Verkhovna Rada of Ukraine. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2)*. https://zakon.rada.gov.ua/laws/show/9a3_001-22
15. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27002:ed-3:v2:en:term:3.1.20
16. National Bank of Ukraine. (n.d.). *Authorization of payment market participants*. https://bank.gov.ua/ua/supervision/payment-services
17. TASKOMBANK. (2025). *Information security policy*. https://tascombank.ua/files/Polityka_informatsiinoi_bezpeky-2025.pdf
18. National Commission for the State Regulation of Electronic Communications, Radiofrequency Spectrum and Postal Services. (n.d.). *Regulatory activities*. https://nkek.gov.ua/diialnist/rehuliatorna-diialnist

Отримано редакцією журналу / Received: 05.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 25.06.26